SOTI.net
We Manage Mobility

SOTI Inc. | Email: sales @ soti.net | Web: www.soti.net | Tel: 1 888 624 9828 (Toll Free N. America) | Tel: +1 905 624 9828 (International)

Contents

Getting Started

To get started with MobiControl, we suggest that you familiarize yourself with the main MobiControl components *(See below.)* and then proceed to the "MobiControl Tutorial" topic on page 3. Once you have been through the tutorial, you should be ready to use MobiControl to manage your mobile field force.

MobiControl Components

The **MobiControl Manager** provides a centralized management console from which all aspects of the system can be monitored and controlled. The Manager can be installed on one or more desktop or notebook computers in your network. The manager communicates with the database and Deployment Servers. Please see the "MobiControl Manager Overview" topic on page 6.

The **MobiControl Deployment Server** communicates with mobile devices and executes the rules configured using MobiControl Manager. Deployment Servers also make real-time and historical information available to users through the tools provided in MobiControl Manager. Please see the "Deployment Server Overview" topic on page 382 for more information.

The **MobiControl Device Agent** is the MobiControl software which resides on mobile devices. Device Agents communicate with MobiControl Deployment Servers and are responsible for installing/uninstalling packages, as well as providing Deployment Servers with real-time information about the state of the device. Please see the "Device Agent" topic on page 276.

The **MobiControl Database** is used to store status and configuration information as well as the packages that are deployed to the devices. There are three versions of the MobiControl setup program: one that includes the old Microsoft SQL Server Desktop Engine (MSDE), one that includes the new Microsoft SQL Server 2005 Express Edition, and one that does not include a database server. MSDE is a free lightweight version of the Microsoft SQL Server 2000 database. Microsoft SQL Server 2005 Express Edition is a free lightweight version of the Microsoft SQL Server 2005 database. Please see the "Database" topic on page 462.

The **MobiControl Package Studio** is used to create packages of software or data that are to be deployed. Package Studio combines the files to be deployed, as well as installation instructions, into a single compressed package file. Please see the "MobiControl Package Studio" topic on page 413.

The **MobiControl Web Console** is a light support tool that can be accessed anywhere where Internet Explorer is installed. This feature uses HTTP to communicate back to your deployment server so you can view your devices in real time. Allowing you to remote control any online device, send a script, or even locate the device using our Location Services feature. Please see the Web Console page for more information.

MobiScan is used to create barcodes for devices to scan and have the MobiControl Device Agent installed automatically. Please see the MobiScan page for more information.

MobiControl Tutorial

The following sequence of steps will guide you through the basic features of MobiControl. MobiControl has several other features and capabilities that are not discussed in this tutorial. We recommend reading through the entire manual. The first two steps of this tutorial show you how to get your devices configured within MobiControl. Then, the remaining steps show you how to use MobiControl to perform various management operations.

1. Create device groups.

   Device groups allow administrators to organize groups of devices based on their location or function. For example, a particular installation may have devices that are used by sales staff and other devices that are used by warehouse staff. The administrator might create a group called "Sales Devices" to hold the sales devices, and a group called "Warehouse Devices" to hold the warehouse devices. By organizing devices into groups, administrators can quickly locate the device(s) in which they are interested. Please see the "Device Groups" topic on page 124 for detailed information.

2. Add devices.

   Before you can use MobiControl to manage your mobile devices, your devices need to be added to MobiControl and configured. To do this you need to create an add device rule. An add devices rule specifies the device group to which the devices are to be added. It also contains other parameters such as how often the device is to check for updates. Please see the "Add Devices" topic on page 127 for detailed information.

3. Deploy packages to devices.

   First, you need to create a deployment rule. A deployment rule specifies the packages that are to be deployed and the devices they are to be deployed to. Please see the "Deploying Packages to Devices" topic on page 358 for detailed information.

4. Use the MobiControl Help Desk.

   MobiControl includes a complete suite of help desk and remote control tools so you can provide real-time help and support to your mobile field force. The Help Desk suite of tools includes real-time remote control, remote explore tool, remote registry editor, remote task manager, remote scripting, remote DOS, remote screen and video capture,and remote printing. Please see the "Help Desk" topic on page 28 for detailed information.

5. Generate reports.

   MobiControl includes a set of preconfigured reports that provide administrators with detailed information about the operation of the system. Some of the reports included with the system are the rule execution report, device activity report and package report. Please see the "Generate Reports" topic on page 390 for detailed information.

MobiControl Security

MobiControl provides end-to-end enterprise scale security for the mobile devices and the mobile data across all endpoints. MobiControl's highly scalable and flexible multi-tiered security model is centrally managed and leverages industry standards to provide rules-based security across the mobile enterprise. All security policies are configured from the centralized MobiControl Manager console and all device security policies and subsequent updates are implemented over the air, making enterprise-wide policy changes and implementation a seamless and easily manageable process.

MobiControl's comprehensive security extends to all components that form the mobile enterprise, from the mobile devices being used in the field by the end user, to the Manager consoles being used by the remote help desk to support the field force, to the network over which corporate data flows to and from the mobile devices.

Mobile Device Security

MobiControl's on-device security policy enforcement protects mobile data and controls access to the device in both the connected and disconnected modes. All security policies are managed centrally and can be customized for individual devices or enforced at the group level. Security policies are distributed to the devices over-the-air (OTA) in a transparent and seamless manner. User authentication using Active Directory credentials allows the mobile devices to be authenticated on the network using the same credentials that the end users use for existing computers and workstations, eliminating the need for multiple passwords and allowing centrally-managed user authentication management.

Advanced data security features like automatic file encryption for the device and storage media allow securing the mobile data. In addition, time-based, fail-safe security policies can trigger various actions, for instance, a remote self-wipe, on-demand encryption of files, device lockdown, in response to events like unsuccessful user authentication, or failure to communicate with the server. Application run control features allow creating application black lists and white lists to prevent unauthorized applications from being installed and executed on the device. The device lockdown feature allows running the device in a kiosk mode with the capability to limit or restrict access to applications and device settings, such as Wi-Fi or power. Additionally, device features and communication ports (e.g. Bluetooth, infrared, camera, phone) can be disabled, restricted, or limited. Please see the "Device Security and Control" topic on page 183 for more details.

Data Communications Security

To ensure end-to-end security, by default MobiControl encrypts all communication between the MobiControl Manager and the Deployment Server using SSL. By default the Device Agent uses a proprietary algorithm for encrypted communication with the Deployment Server. For organizations that require standards based encryption for protecting data communication, SSL-based encryption can be enabled for communication between the Device Agent and the Deployment Server. This allows all communication and data flowing between the mobile devices, the MobiControl Deployment Server and the MobiControl Manager consoles to be encrypted using SSL certificates, for an extra layer of security. Multiple methods of distributing the certificates for encryption are available. Please see the "Communication and Connection Security" topic on page 411 for more details.

Manager Console User Security

MobiControl allows the implementation of tiered support teams by limiting access to the MobiControl Manager console and the functionality available to the support personnel. By providing the capability to disable certain operations and features for specific users or groups in an Active Directory or using local security, MobiControl provides multiple levels of access to the mobile enterprise in an environment where the business model requires role-based delegation of administration functions and tasks. For instance, a help desk environment where tier 1 has limited access to the powerful features available in MobiControl, and tier 2 has more control and access to an expanded set of functions. MobiControl's user security system allows users to authenticate with a user list created locally, or integrates with Active Directory using read-only communication (without modifying the directory schema) and the Windows security system to control user access to MobiControl. Please see the "Manager Console User Security" topic on page 409 for more details.

MobiControl Manager

MobiControl Manager is a centralized management console that allows users to monitor and control all aspects of system operations.

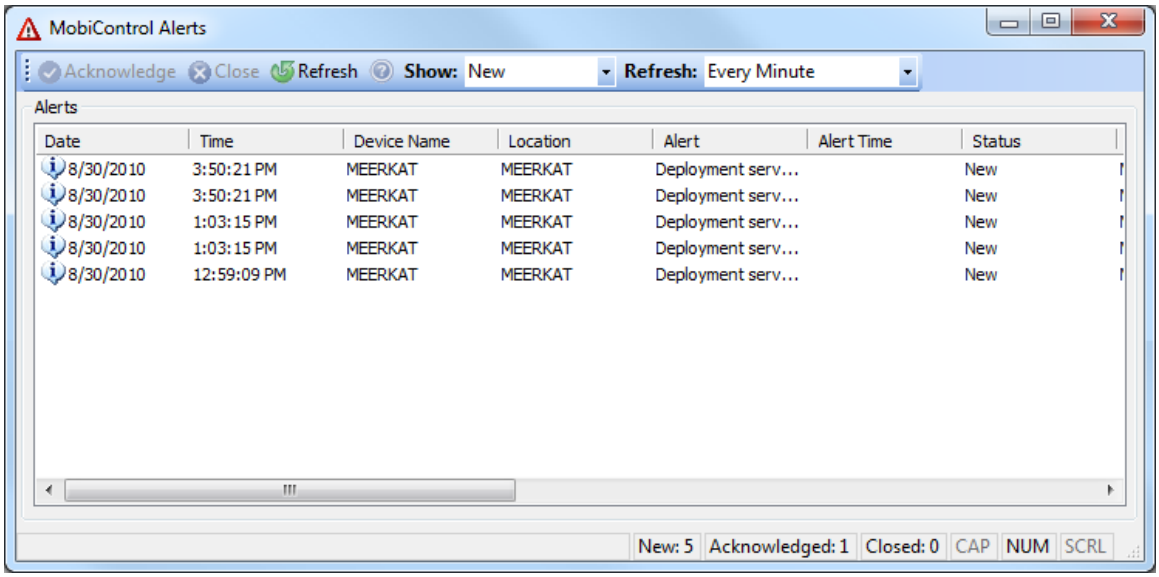
Start MobiControl Manager from the icon on your desktop, or click **Start,** select **Programs,** select **SOTI,** select **MobiControl,** and click on **MobiControl Manager.** Using MobiControl Manager, users can remotely install packages to devices, uninstall packages from devices, view the online status of devices, remote control devices, get inventory information about the packages installed on a device, generate reports, and more.

The MobiControl Manager user interface consists of five views. The views can be selected using the tabs at the bottom of the MobiControl Manager user interface.

- The **Devices view (tab)** allows users to view information about configured devices, for instance packages installed, device ID, and IP address. The Devices view (tab) also allows users to control and configure devices, for example, to remote control a device or to change a device's name.
- The **Rules view (tab)** allows users to view information about the configured rules. The Rules view (tab) also allows users to configure rules, for instance, create an add devices rule, a deployment rule, a file sync rule, an enable rule, or a disable rule.
- The **Packages view (tab)** allows users to view information about packages, for instance the packages currently configured or a list of devices onto which a certain package has been installed. The Packages view (tab) also allows users to configure package-related information, for example to add or delete packages.
- The **Deployment Servers view (tab)** allows users to view information about the configured Deployment Servers or to manage Deployment Servers, for example, enabling or disabling, shutting down, or viewing a list of devices connected to a Deployment Servers.
- The **Reports view (tab)** provides users with a set of reports containing detailed information about the operation of the system. Provided reports include: deployment rule execution summary report, device configuration rule execution summary report, and device activity report.

Alert Manager

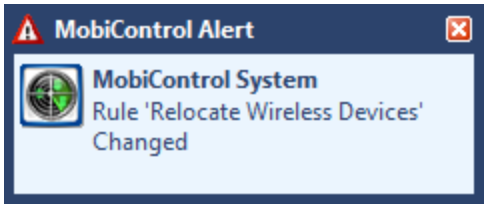
Once you have successfully created an Alert Rule the MobiControl Manager Alerts Manager window will start populating Alerts that have been generated by the rules created.



The Alerts Manager window will show information regarding your alerts. Alerts can be Acknowledged here by selecting the alert and clicking Acknowledge. Also Alerts can be closed from this window.

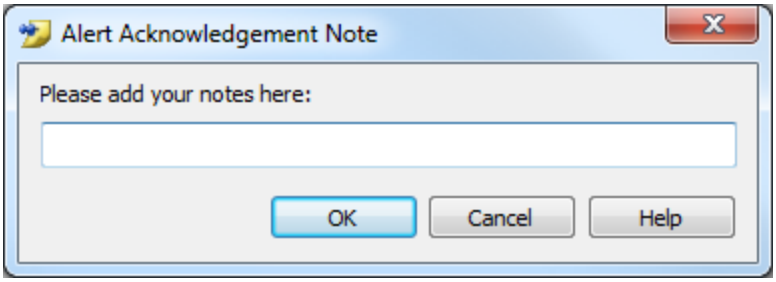
NOTE:

This Window can be launched by pressing CTRL+A

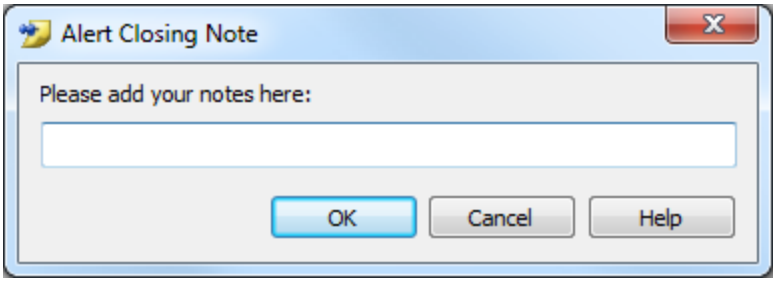


When you receive a new Alert, you will see a notification window appear in the bottom left of your screen. Clicking on this window will open the MobiControl Alerts Manager window.

To Acknowledge an Alert or Close an Alert, right click on the Alert in the list and select Close or Acknowledge. Alternatively you can select the Alert and click the Close or Acknowledge button. When Closing or Acknowledging an Alert you can enter a note about the alert. The note is then available in the Alert Manager.



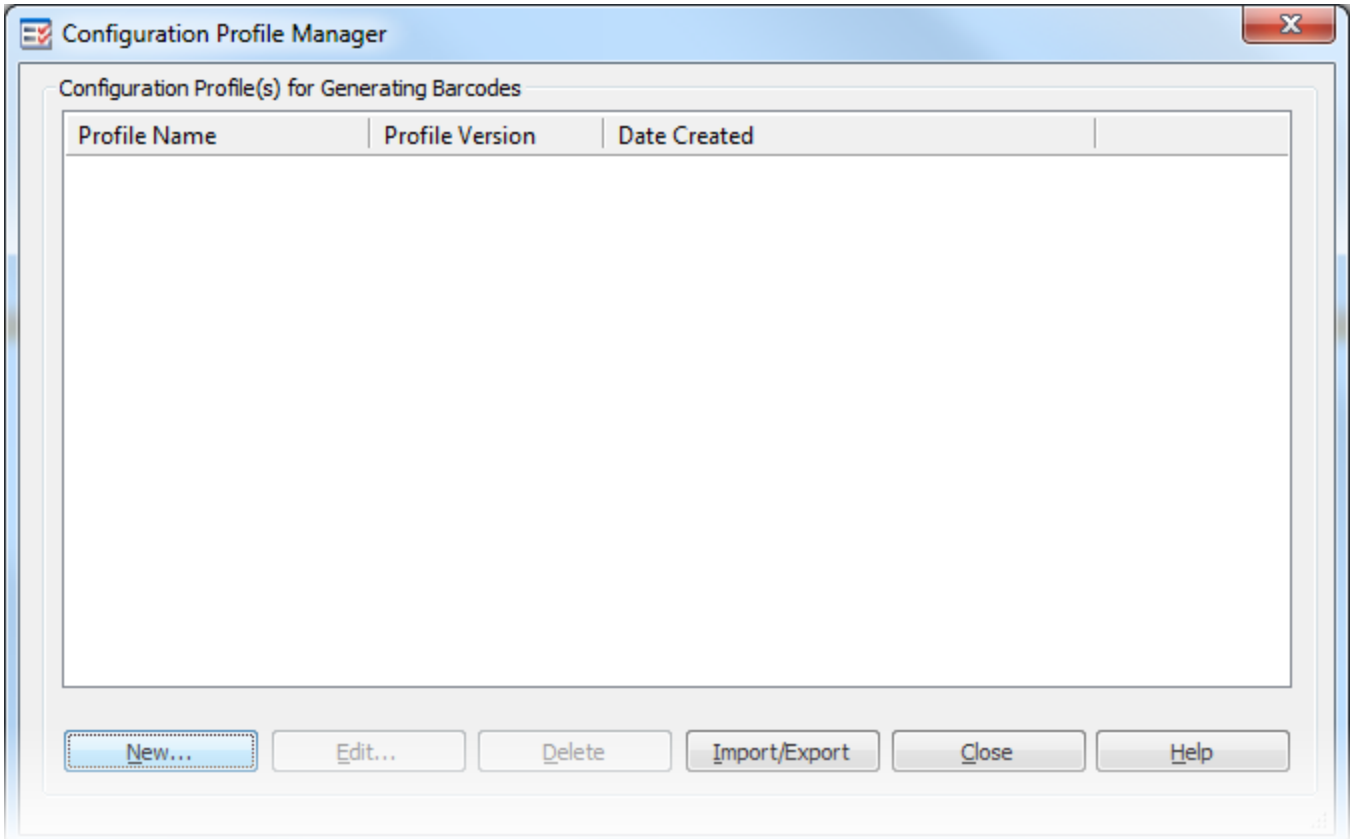
Acknowledge an Alert



Close an Alert

Configuration Profile Manager

Configuration Profile Manager is an interface that allows the user to create, edit and delete Configuration Profiles. The Profile includes initial configuration like Wireless ZeroConfig, Summit Wireless settings, Fusion settings, Devicescape Wireless settings, Static IP, Cellular connection (APN) settings and MobiControl Device Agent settings for Windows Mobile and Windows CE powered devices that will be managed by SOTI MobiControl Device Agent.



The Configuration Profile Manager displays a list of existing Profiles that have been created (the list will be empty if there is no Profile created as yet), and allows the user to create, edit and delete Profiles. Users can also import and export Profiles

To create a new Configuration Profile, click on the **New** button.

To edit an existing Profile, click on the **Edit** button.

NOTE:

When you edit an existing Profile, the existing version number will automatically be incremented by 1.

To delete an obsolete Profile, click on the **Delete** button.

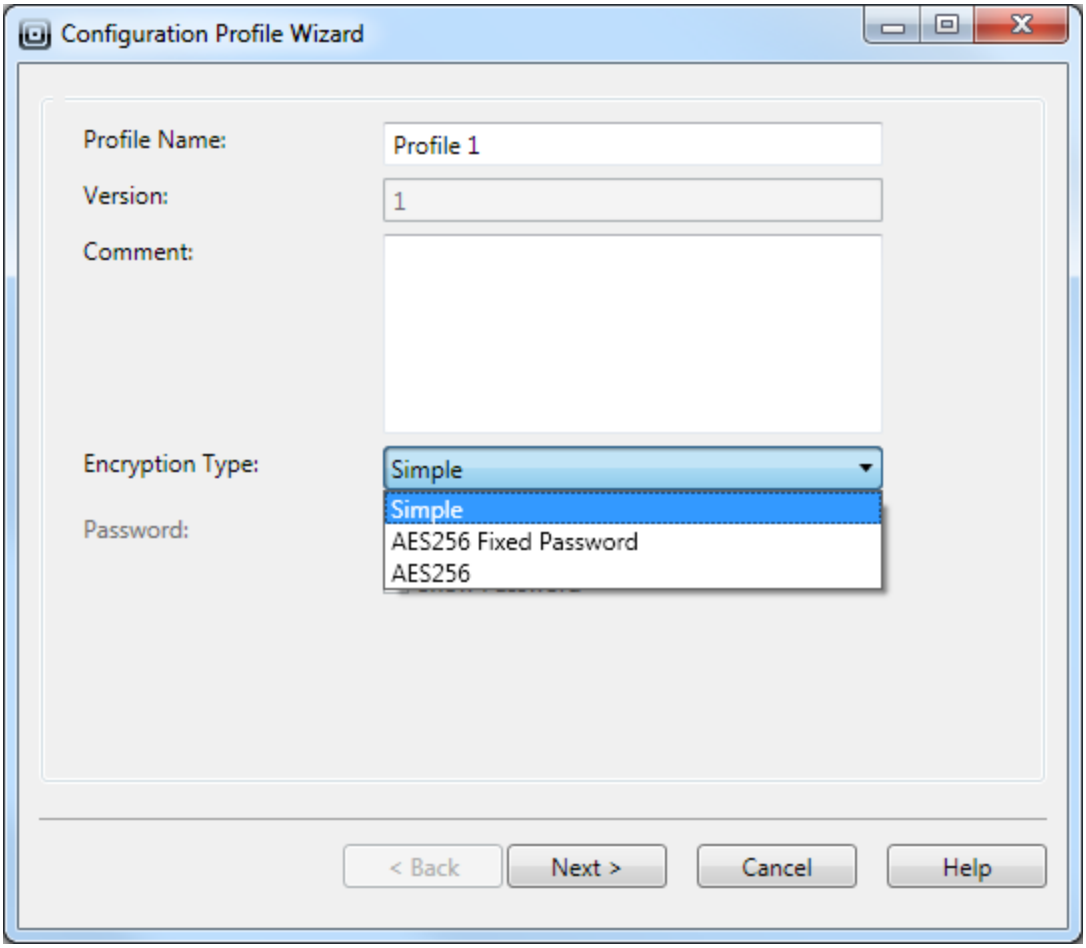
To import a Profile from file, click on the **Import/Export** button and then select **Import From file**

To export Profile to a file, click on the **Import/Export** button and then select **Export To file**

1. Creating a Configuration Profile.

The Configuration Profile Manager will allow you to create a Configuration Profile.

Click on **New** > **Create New** to create a new Configuration Profile: to create a new Configuration Profile:



Field Name	Description
Profile Name	Enter the name of the profile you want to create
Version	This field displays the current version number of the Configuration Profile.
Comment	Enter a description for this package. You can optionally leave this field blank.
Encryption Type	**Simple:** Simple encryption uses a SOTI algorithm to encrypt the data before generation the barcode. This option creates the smallest footprint for the barcode. It is the default option and recommended if enhanced security is not required. **AES256 Fixed Password:** Encrypts data with AES256 algorithm. This option uses a fixed password and the barcode will be able to read by ANY device having the MobiScan Agent. **AES256:**

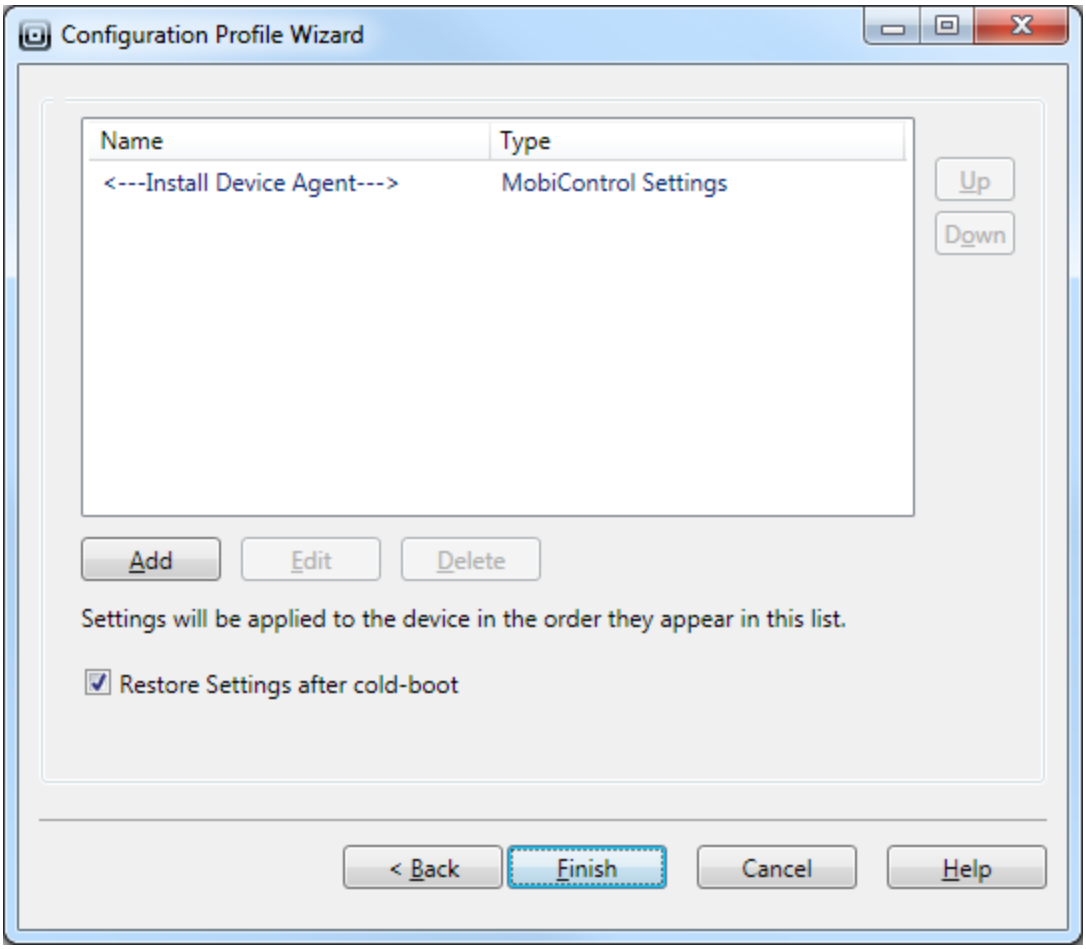
Field Name	Description
	Encrypts data with AES 256 algorithm. When using this option, you must enter password to generate the barcode. This password will then be required by the end user to configure the device.
Password	If **AES256** Encryption is used, enter a password to generate the barcode. This password will then be required by the end user to configure the device.

Click on **Next** to continue

2. Add settings to be included in your Configuration Profile

Click on **Add** to open "**Configure Settings**" page

Select your Settings Type



NOTE:

If the option "**Restore Settings after cold-boot" is checked, it** will make the Settings cold-boot persistent.

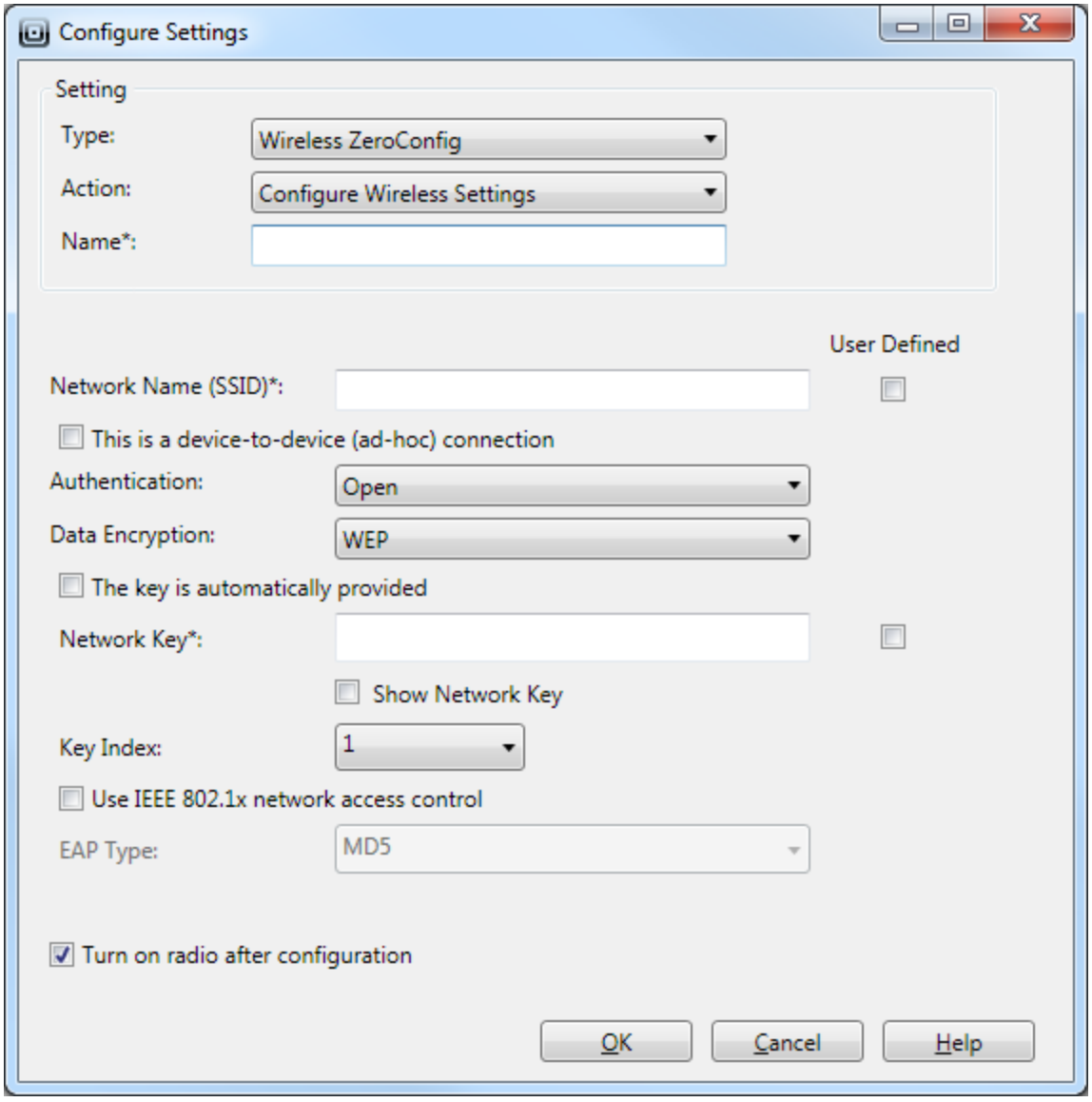
The most recently added profile is automatically set to Active/Default Profile. You may change the "Default Profile" by using the Up/Down arrows.

3. Configure Profile Settings.

Select one of the following Wireless Configuration Profiles.

Wireless ZeroConfig

Adds a wireless profile for Microsoft Wireless ZeroConfig.



Field Name	Description
Action	**Configure Wireless Settings**: This option will allow you to configure the settings for your Wireless ZeroConfig Profile **Turn on radio**: This option allows you to turn ON the WiFi radio. **Turn off radio**: This option allows you to turn OFF the WiFi radio.

Field Name	Description
Name	Enter the name for your Wireless ZeroConfig settings
Network Name (SSID)	Enter your Network name/Service Set Identifier (SSID) (Check the "**User Defined**" option to allow the user to enter or change this information)
This is a device-to-device (ad-hoc) connection	Check this option if you are configuring ad-hoc connection.
Authentication	Enter the Authentication type for your network. Options are Open, Shared, WPA, WPA-PSK, WPA2 and WPA2-PSK
Data Encryption	Enter the Data Encryption for your network. Options are Disabled, WEP, AES, TKIP
Network Key	Enter the Network Key for your network. (Check the"**User Defined**" option to allow the user to enter or change this information)
EAP Type	Specify your Extensible Authentication Protocol (EAP) method. You can choose from the following EAP types: MD5, PEAP and TLS.
Turn on radio after configuration	If this option is checked, it will turn ON the WiFi radio of the device after configuring Wireless ZeroConfig settings.

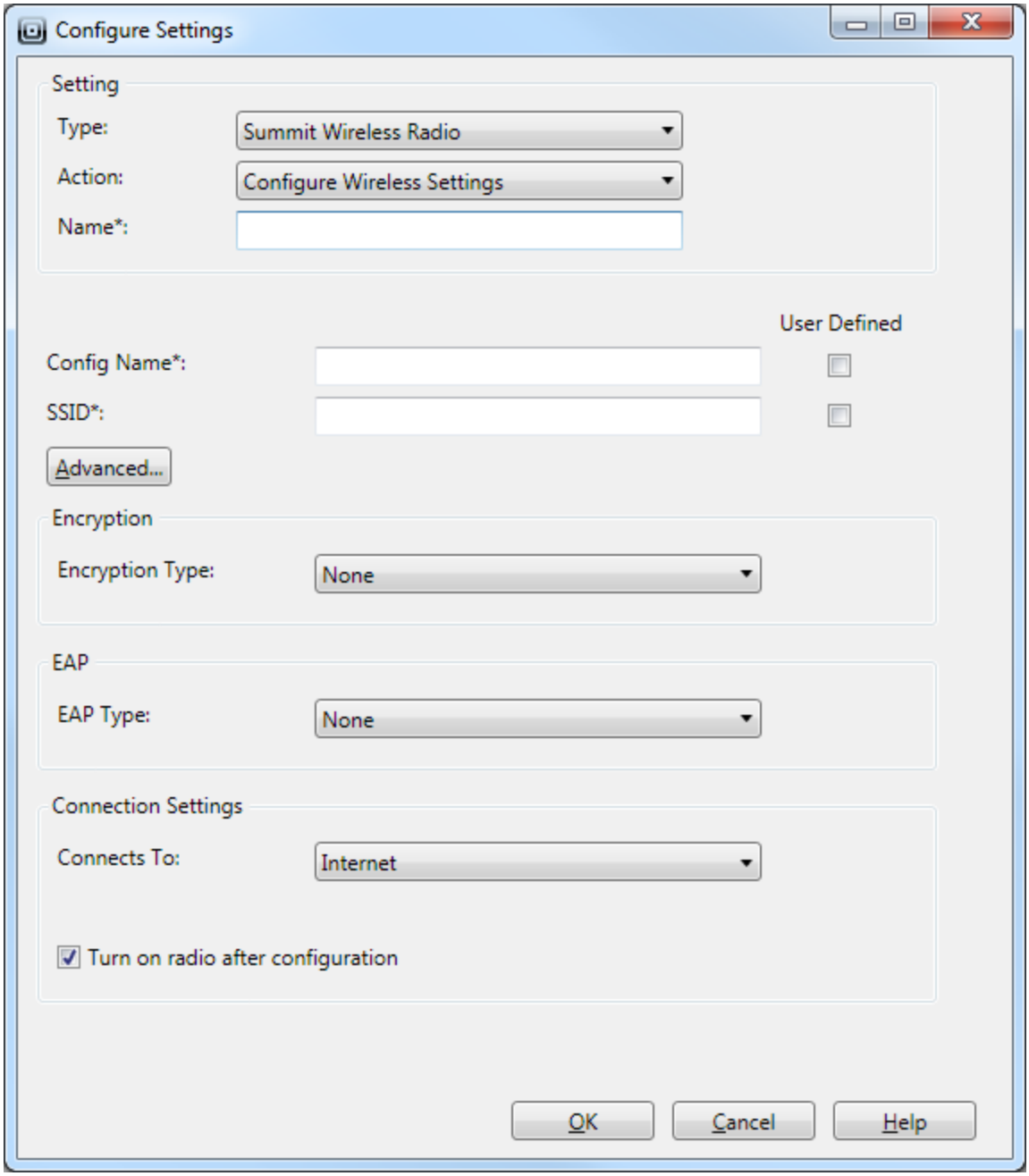
NOTE:

The following options are only applicable for WEP encryption:

- Check the option "**The Key is automatically provided**" if the network key for clients is automatically provided.
- Select the "**Key Index**" from the drop down menu, if applicable.
- Check the option "**User IEEE 802.1x network access control**" to use IEEE standard for port-based Network Access Control

Summit Wireless Radio

Enables the Summit Radio on the device and adds a Summit Wireless profile.

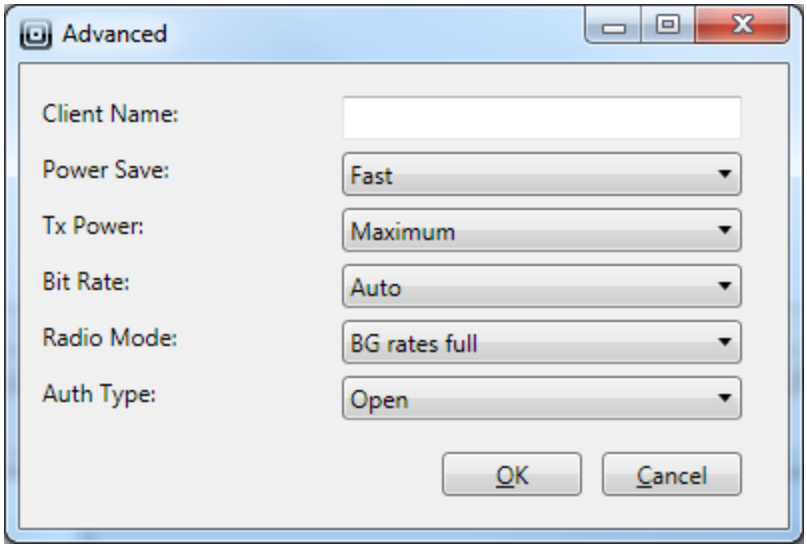


Field Name	Description
Action	**Configure Wireless Settings**: This option will allow you to configure the settings for your Summit Wireless Profile **Turn on radio**: This option allows you to turn ON the WiFi radio. **Turn off radio**: This option allows you to turn OFF the WiFi radio.
Name	Enter a name for your Summit Wireless settings
Config Name	Enter a name for your Summit Wireless Profile

Field Name	Description
	(Check the **"User Defined"** option to allow the user to enter or change this information)
SSID	Enter your Service Set Identifier (SSID) to which radio will connect (Check the **"User Defined"** option to allow the user to enter or change this information)
Encryption Type	Select the encryption type
EAP Type	Select your Extensible Authentication Protocol (EAP) type associated with the profile. You can choose from the following EAP types: LEAP, EAP-FAST, PEAP-MSCHAP, PEAP-GTC AND EAP-TLS.
Connects To	Select if this network connects to Internet or Work
Turn on radio after configuration	If this option is checked, it will turn ON the WiFi radio of the device after configuring Summit Wireless settings.

Advanced Settings:

This set of options allow the user to configure advanced settings for that Summit Wireless Profile.

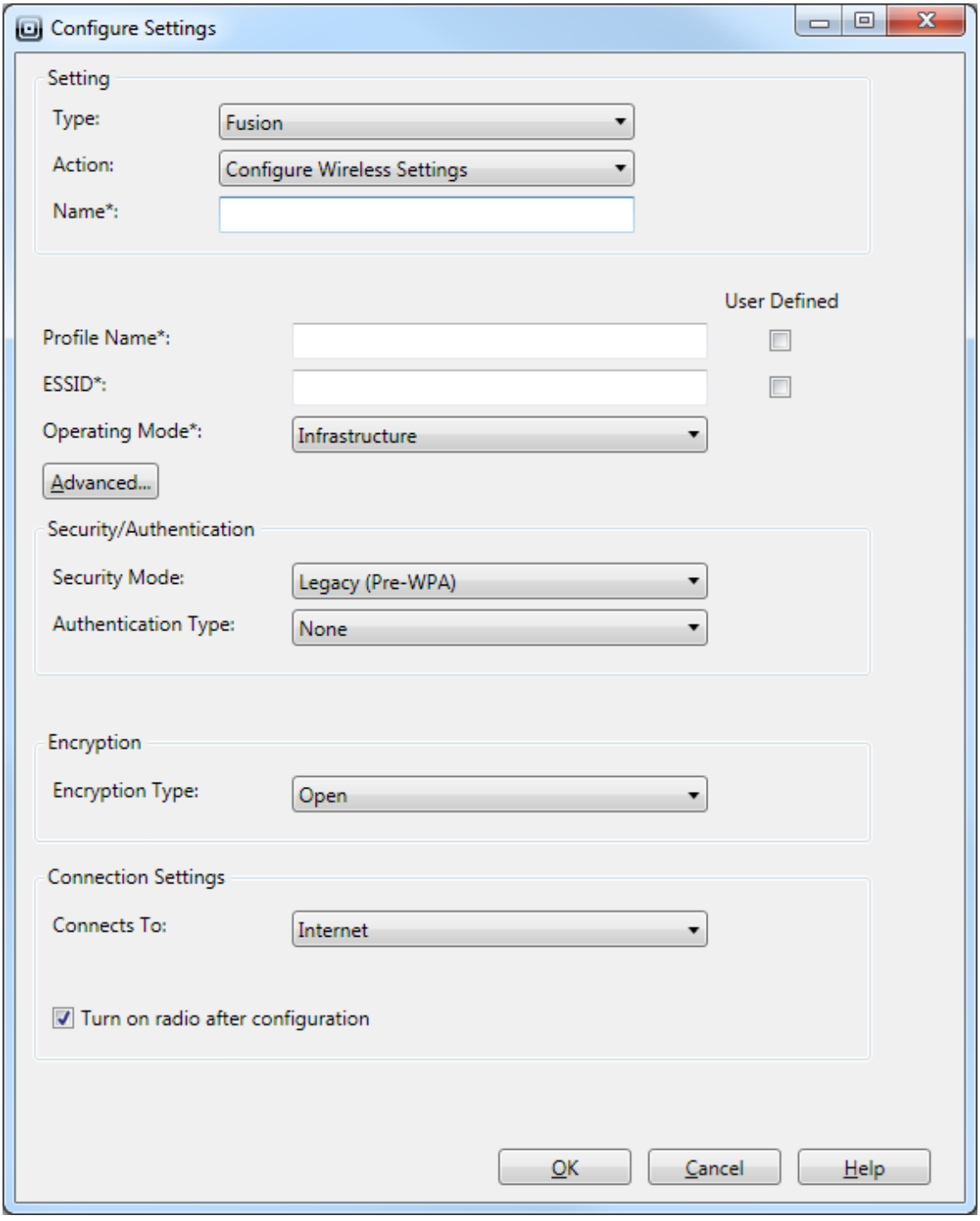


Field Name	Description
Client Name	Enter a name for client device used for Summit radio
Power Save	Select the Power Save value. CAM: Constantly awake mode, Maximum: Maximum power savings, Fast: Fast power save mode

Field Name	Description
Tx power	Select the Transmit Power.
Bit Rate	Select the Bit Rate used by radio when interacting with Access Point.
Radio Mode	Select the Radio Mode used when interacting with Access Point.
Auth Type	Select the authentication type used when associating with Access Point.

Fusion

Adds a wireless profile for Fusion.

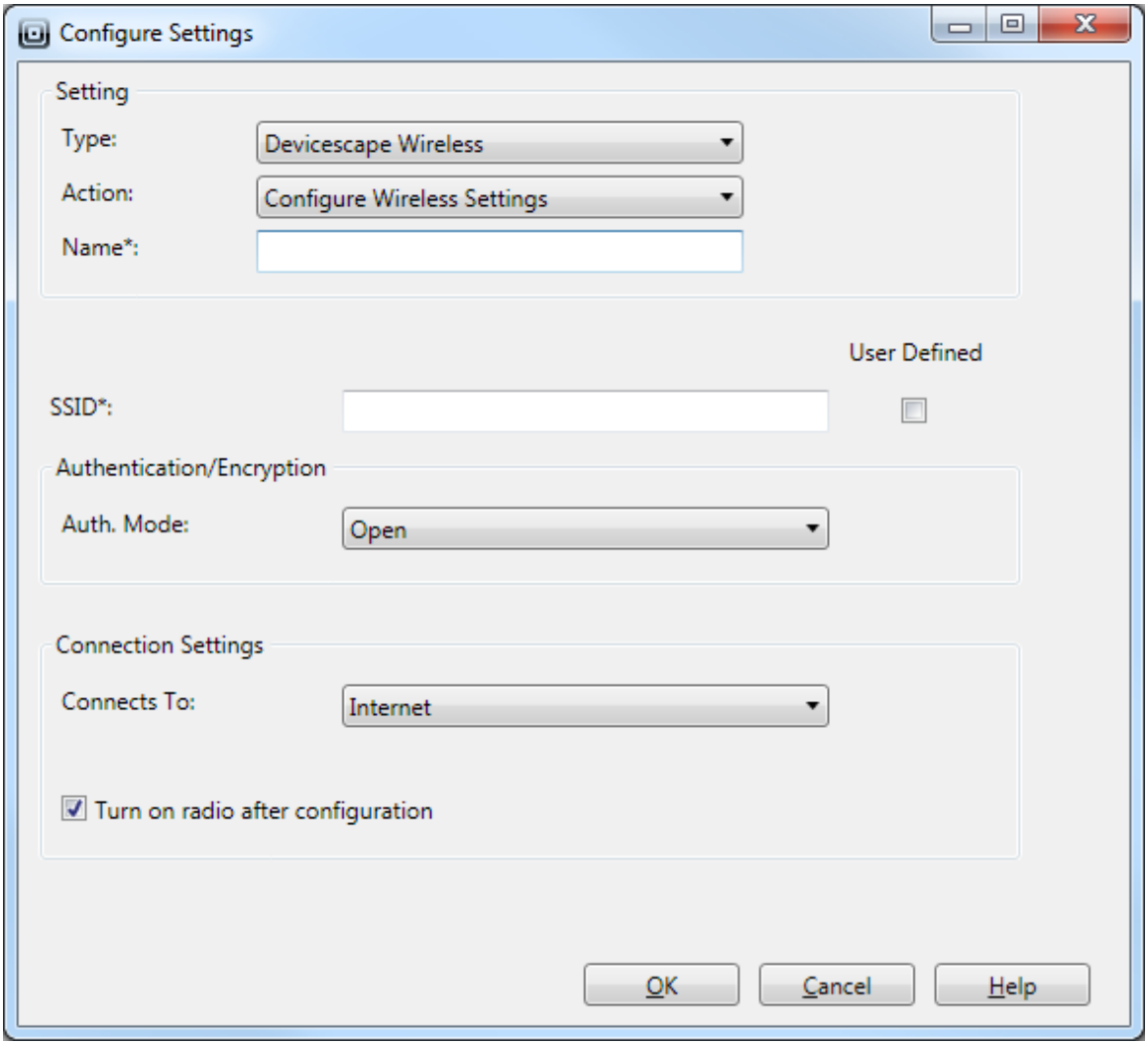


Field Name	Description
Action	**Configure Wireless Settings**: This option will allow you to configure WiFi settings for Fusion. **Turn on radio**: This option allows you to turn ON the WiFi radio.

Field Name	Description
	Turn off radio: This option allows you to turn OFF the WiFi radio.
Name	Enter a name for your Fusion Wireless settings
Profile Name	Enter a name for your Fusion Profile. (Check the **"User Defined"** option to allow the user to enter or change this information)
ESSID	Enter your Extended Service Set Identifier (ESSID) to which radio will connect (Check the **"User Defined"** option to allow the user to enter or change this information)
Operating Mode	Select if the connection is an Infrastructure or Ad-Hoc
Security Mode	Select the type of Security mode used
Authentication Type	Select your Authentication Type associated with the profile. You can choose from the following types: TLS, EAP-Fast,PEAP,LEAP AND TTLS.
Encryption Type	Select the type of Encryption used.
Connects to	Select if this network connects to Internet or Work
Turn on radio after configuration	If the option is checked, it will turn ON the WiFi radio of the device after configuring Fusion

Devicescape Wireless

Adds a wireless profile for Devicescape.

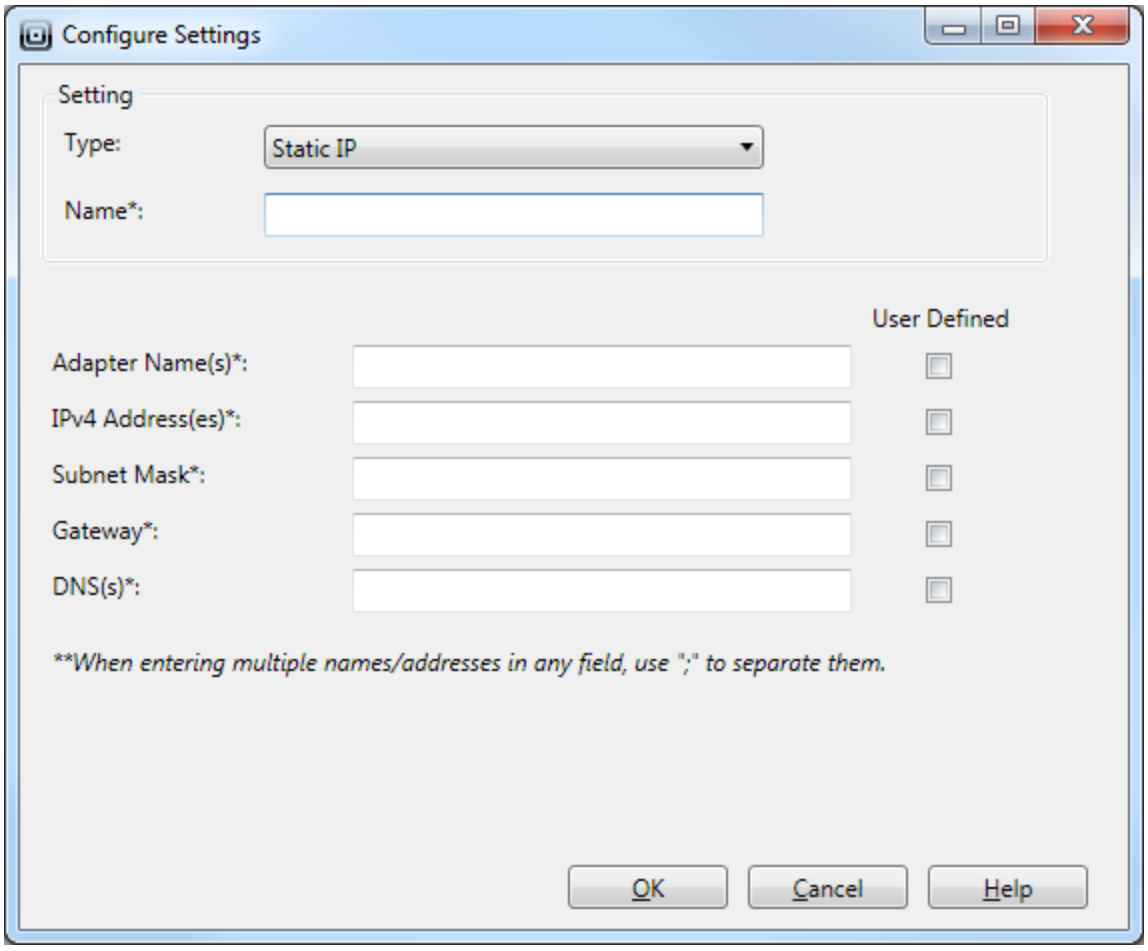


Field Name	Description
Action	**Configure Wireless Settings**: This option will allow you to configure WiFi settings for Devicescape Wireless. **Turn on radio**: This option allows you to turn ON the WiFi radio. **Turn off radio**: This option allows you to turn OFF the WiFi radio.
Name	Enter a name for your Devicescape Wireless settings
SSID	Enter your Service Set Identifier (ESSID) to which radio will connect (Check the **"User Defined"** option to allow the user to enter or change this information)
Auth. Mode	Select your Authentication Mode associated with the profile. You can choose from the following types: WEP, 802.1X, WPA-Personal,WPA-Enterprise,WPA2-Personal,WPA2-Enterprise & CCKM

Field Name	Description
Encryption	Select the type of Encryption according to your Authentication Mode.
Connects to	Select if this network connects to Internet or Work
Turn on radio after configuration	If the option is checked, it will turn ON the WiFi radio of the device after configuring Devicescape Wireless.

Static IP

Sets static IP addresses for the network adapter.

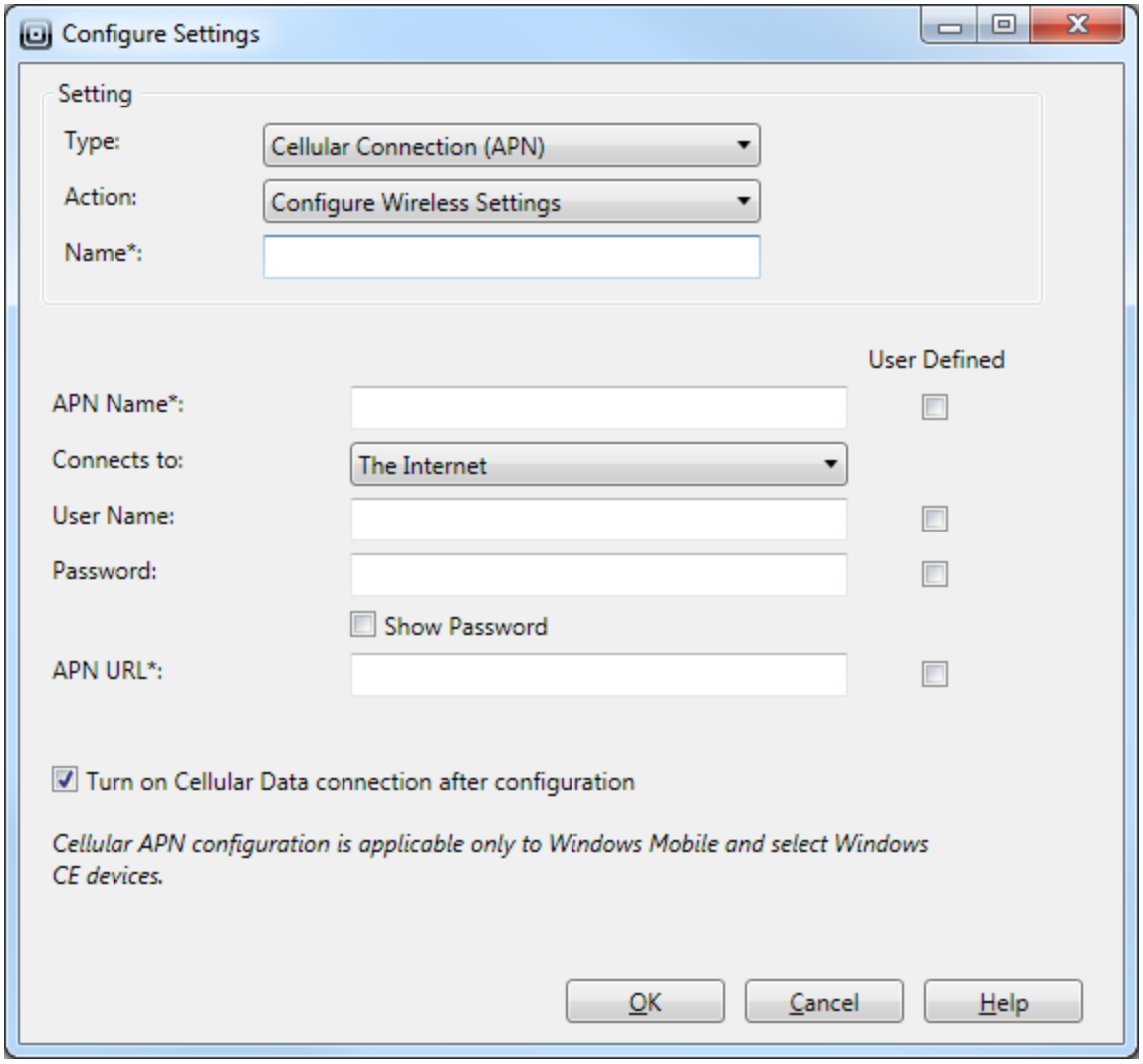


Field Name	Description
Name	Enter a name for your Static IP settings
Adapter Name	Enter a name/names for your adapter

Field Name	Description
(s)	(Check the **"User Defined"** option to allow the user to enter or change this information)
IPv4 Address (es)	Enter the static IPv4 address(es) for your adapter (Check the **"User Defined"** option to allow the user to enter or change this information)
Subnet Mask	Enter the Subnet Mask (Check the **"User Defined"** option to allow the user to enter or change this information)
Gateway	Enter the Gateway's IP address(es) (Check the **"User Defined"** option to allow the user to enter or change this information)
DNS(s)	Enter the Domain Name Server's IP address(es) (Check the **"User Defined"** option to allow the user to enter or change this information)

Cellular Connection (APN)

Adds a Cellular/APN connection (for Internet or Work) on the device.



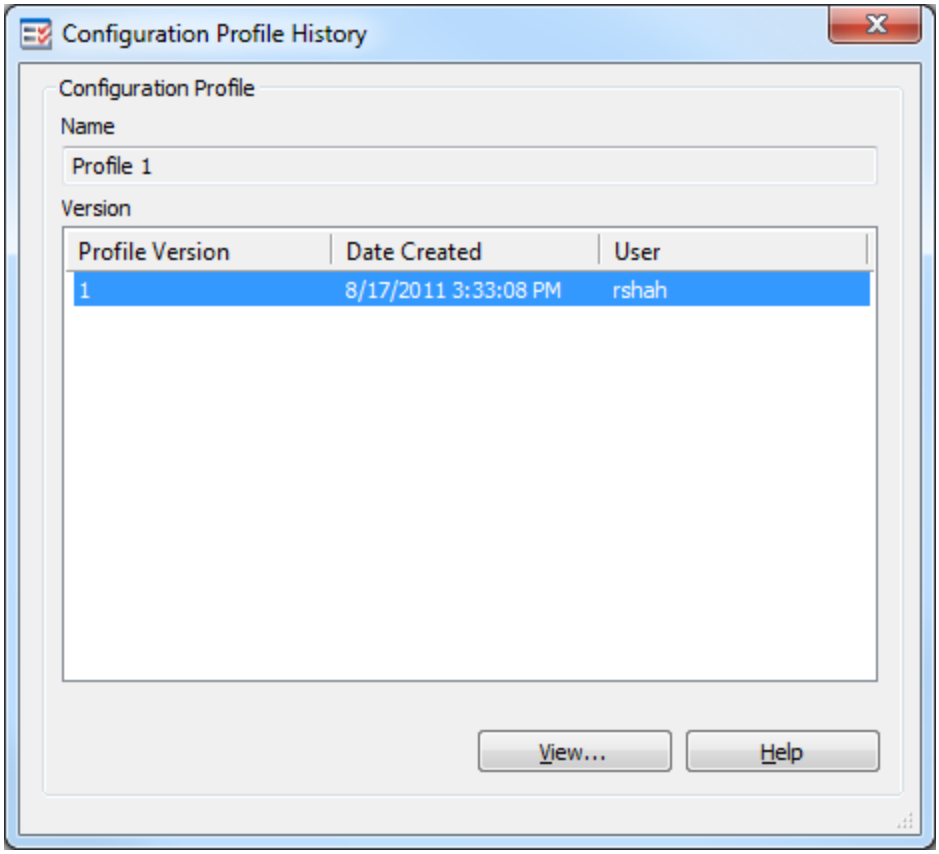
Field Name	Description
Action	**Configure Wireless Settings**: This option will allow you to configure the settings for your APN/Cellular connection **Turn on radio**: This option just allows you to start the Cellular connection, without configuring any APN connection settings. **Turn off radio**: This option just allows you to shutdown the Cellular connection, without configuring any APN connection settings.
Name	Enter the name for your Cellular connection (APN)
APN Name	Enter your Access Point Name (Check the **"User Defined"** option to allow the user to enter or change this information)
Connects to	Select if this network connects to Internet or Work

Field Name	Description
User Name	Enter the User Name (Check the **"User Defined"** option to allow the user to enter or change this information)
Password	Enter the Password (Check the **"User Defined"** option to allow the user to enter or change this information)
APN URL	Enter the Access Point URL/address (Check the **"User Defined"** option to allow the user to enter or change this information)
Turn on Cellular Data connection after configuration	If this option is checked, it will initiate the Cellular Data connection of the device after configuring APN connection settings.

4. Generate Configuration Profile

   Click on **Finish** to generate the Configuration Profile with your configured settings.

   In order to view the version history of a Profile, right click on that Profile and click on **View History**. It will show the following screen:



Please refer the Generating a Barcode section for information on generating a barcode using the Configuration profile.

Devices View

The Devices view (tab) is the main view into the status of the devices in the MobiControl system.

Device Tree

The device tree provides a structured view of the devices in the system. The group structure is easily defined by the user by creating new groups and dragging and dropping devices between groups. Please see the "Device Groups" topic on page 124 for detailed information on groups and virtual groups.

Commonly-reported device information can be easily referenced in the device tree window by right-clicking in any open space in the device tree window and selecting the information that you would like to see displayed.

Devices are added to the system by defining an add device rule and creating a MobiControl Device Agent that is installed on the device. Please see the "Add Devices" topic on page 127 for a detailed explanation of how to add devices to MobiControl.

The device tree view can also be filtered. This allows you to easily identify devices that meet a certain filtering criteria, for example, the subnet to which they are connected. Please see the "Device Filters" topic on page 130 for more information on filters.

Info Panel

The Info panel provides detailed status information about the group or device that is selected in the device tree. When a group is selected, the displayed information includes the number of subgroups and how many unique, online, offline, or disabled devices are in the group. For devices, the displayed information includes device ID, IP address, battery and memory status. In addition, custom data retrieved from your devices may also be displayed. Please see the "Custom Data" topic on page 175 for detailed information about configuring custom data retrieval.

The content displayed in this panel is stored in the MobiControl database. This information is refreshed when a device establishes a new connection to the MobiControl Deployment Server, and when you click **Refresh** or press F5 on this tab.

Rules Assigned Panel

The Rules Assigned panel lists the deployment and file sync rules assigned to the group or device that is selected in the device tree. Rules are inherited from parent groups; a rule will apply to a device if it belongs to group to which the rule has been assigned.

The assignment of rules to groups provides a flexible and convenient means for easily configuring devices. For example, once you have set up your rules for software or data distribution, you can automatically provision your devices by simply adding them to the appropriate group within the device tree. Please see the "Rules" topic on page 257 for information on creating deployment rules and file sync rules.

Logs Panel

The Logs panel provides a listing of the events occurring in the MobiControl system. This listing is filtered based on the group or device that is selected in the device tree. If only one device is selected, only the events related to that device are displayed. If a group is selected, events for the group and all the devices that belong to that group are displayed.

You have the option to show or hide logging, adjust the maximum number of logs displayed, and the frequency with which the Manager should refresh the log view.

NOTE:

You can select multiple log entries by holding the Ctrl (Control) key on your keyboard down and clicking on different log entries or by pressing CTRL+A to select all log entries. To copy these logs you can press CTRL+C after selecting them or right click on the log window and select copy. The contents will be pasted on the system clipboard and will be available for pasting.

Packages Panel

The Packages panel lists the packages that are configured on the device that is selected in the device tree. The assignment of packages is directly based on the assigned rules. This panel provides a status column which indicates the state of the package for that device. For example, the status "Pending" indicates that the package has been queued and its installation on the device is pending.

You can force the re-installation of a package on a given device by right-clicking on the package in the Package Panel and selecting **Force Package Reinstall on Next Schedule** or **Force Package Reinstall Now.**

Programs Panel

The Programs panel lists the applications that are installed on the device that is selected in the device tree. This is the same listing that is displayed by the **Remove Programs** applet provided by the Microsoft operating system.

Notes Panel

The Notes panel lists the notes that are associated with the selected device. If a group is selected in the device tree, all the notes for the devices that belong to the group are listed. Notes are a convenient way to maintain information about the device such as trouble tickets. Please see the "Device Notes" topic on page 143 for information on creating device notes.

Collected Data Panel

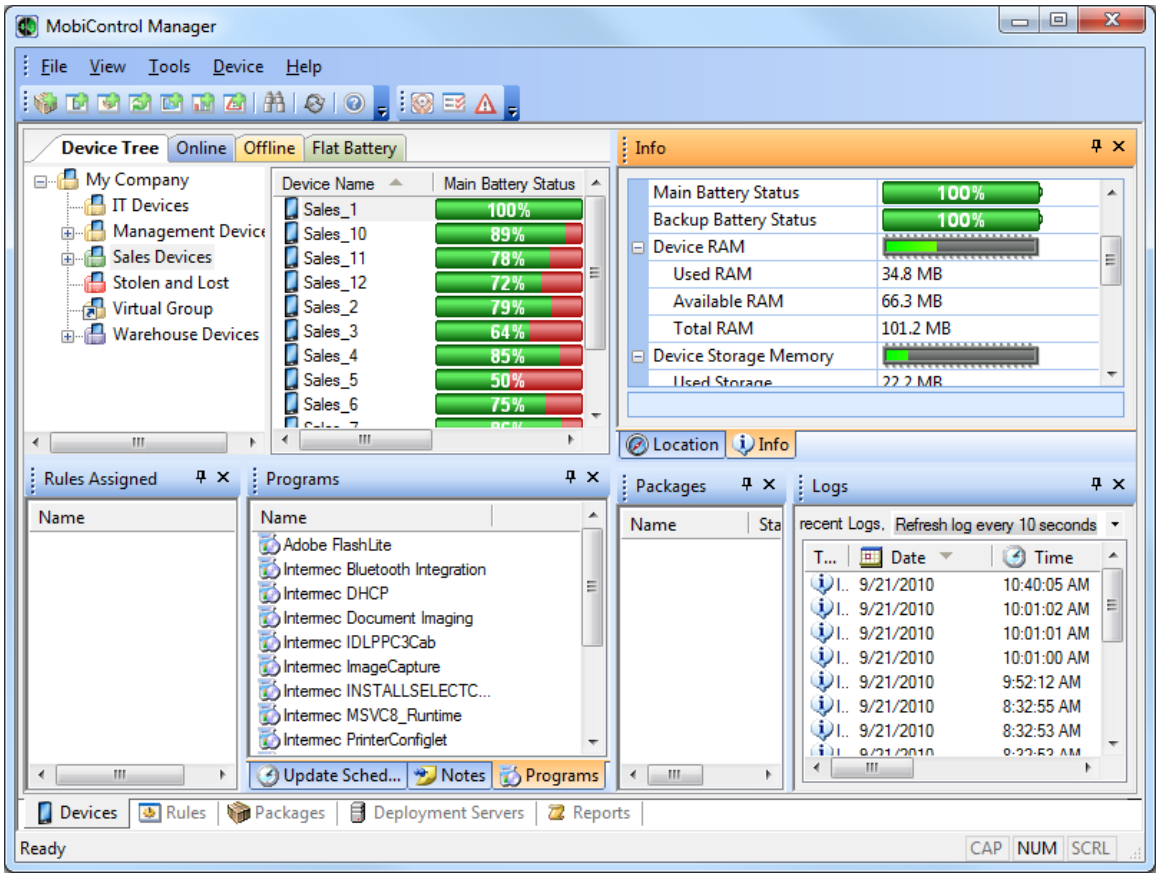
The Data Collection Panel allows you to view the collected historical data for a set of devices. By creating a Data Collection Rule you will be able to specify which items to collect data from, how often to collect them, and when to upload the collected data to the server. Please see the Creating Data Collection Rules page for information on creating Data Collection.

Location Panel

The Location Panel gives the ability to locate, track and gather information on the movement of your GPS enabled devices, no matter where they are in the world which is powered by Microsoft's Bing maps technology. Whether you need to confirm the current location of a particular field-worker, track the progress of an important shipment or collect historical information on the movement of a group of devices or vehicles in order to analyze performance, MobiControl's Location Services can help. Please see the Location Services page for more information.

Update Schedule Panel

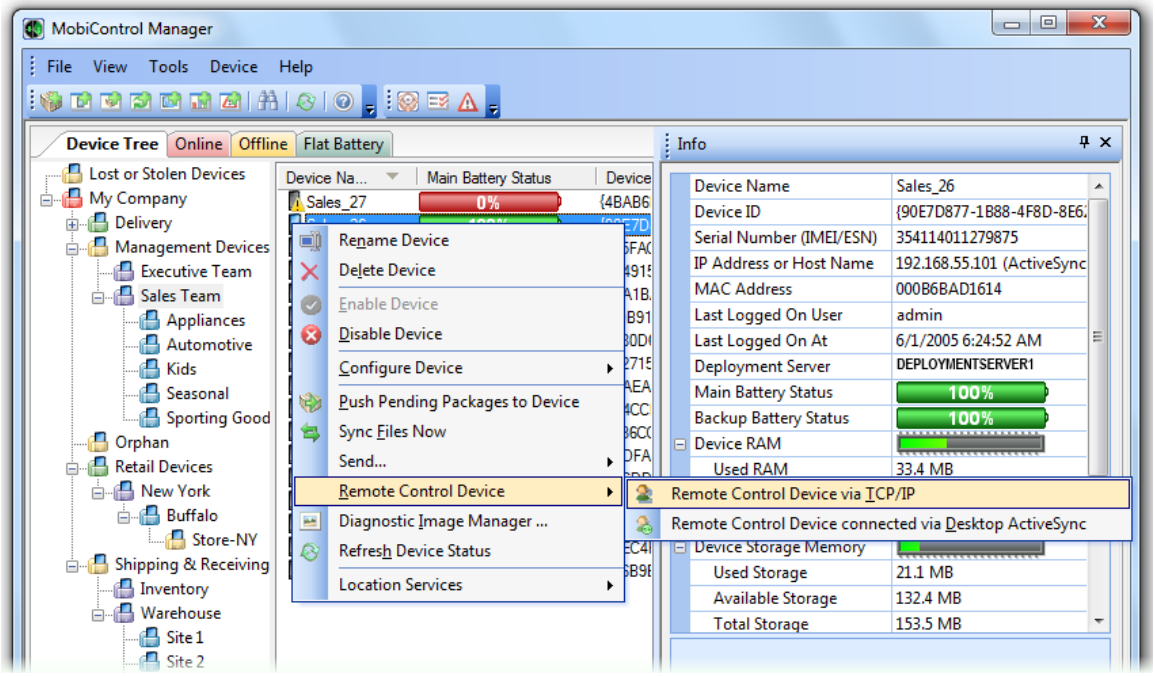
The Update Schedule panel lists the dates and times when the device is programmed to query the MobiControl system to check for updates. By default, a device will also check for updates whenever it connects to the MobiControl system. Please see the "Device Update Schedule" topic on page 160 for more information.



MobiControl Manager Devices view (tab)

MobiControl Help Desk (Remote Control)

The MobiControl Help Desk, also known as the MobiControl Remote, can be accessed from the MobiControl Manager Devices view (tab). To open a remote control session, select a connected device in the MobiControl Manager Devices view (tab), then right-click on the device in the device list and select one of the remote control options. If the device is connected over TCP/IP select **Remote Control Device via TCP/IP**; if the device is docked via ActiveSync select **Remote Control Device connected via ActiveSync**.

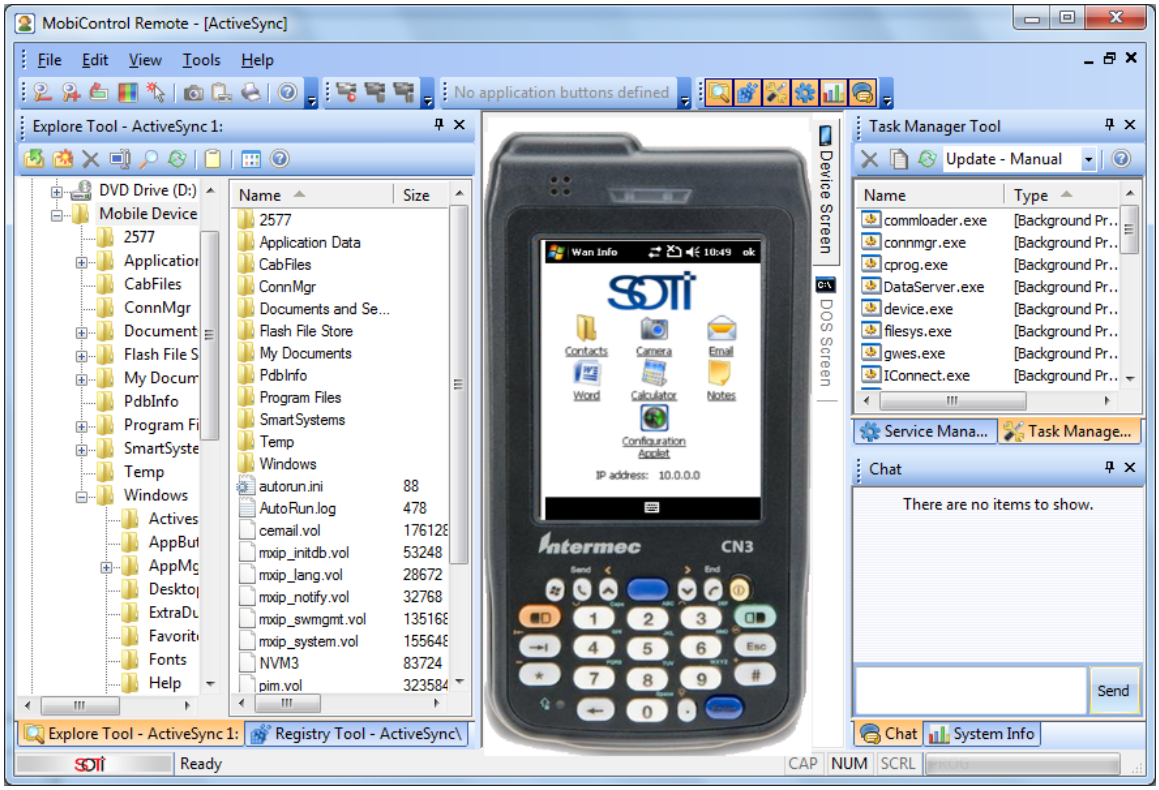


Selecting "Remote Control Device via TCP/IP" in the Device menu

NOTE:

The color of the screen in the device icons indicate if a device is currently connected or not. For connected devices screen color in the icon is light blue; for disconnected devices the screen color is black.

The following screen shows a MobiControl remote control session to a device.



MobiControl Tutorial

This is step 4 of the MobiControl Tutorial. Please see the "Generate Reports" topic on page 390 for the last step.

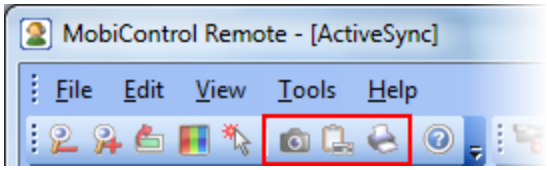
File Menu

The following is a description of the **File** menu items:

- Use **Disconnect** to disconnect from a mobile device. This menu item will be enabled only if a connected device has been selected in the device tree.
- Use **Save Screen to Disk** to capture a mobile device screen image and save it to disk in `.jpeg`, `.png` or `.bmp` format. Please see the "Saving the Screen to Disk or Clipboard" topic on page 31.
- Use **Save Screen to Clipboard**to save the mobile device screen to the clipboard on your desktop computer, this can then be pasted into other programs. Please see the "Saving the Screen to Disk or Clipboard" topic on page 31.
- Use **Print** to print the screen. MobiControl Remote supports WYSIWYG (What You See Is What You Get) printing. If your screen is zoomed to 200%, the image that is printed will also be zoomed to 200%. If you are using MobiControl Remote in landscape view, the image printed will also be printed in landscape view. Therefore, before printing, it is important to adjust the screen size and orientation according to what you would like to see on the printed image.
- Use **Print Preview** to preview the print output.
- Use **Print Setup** to configure the print settings.
- Use **Exit** to close MobiControl Remote.

Saving the Screen to Disk or Clipboard

The image of the device screen (with or without the skin) can be saved as an image file by using the **Save to screen** button in the toolbar.

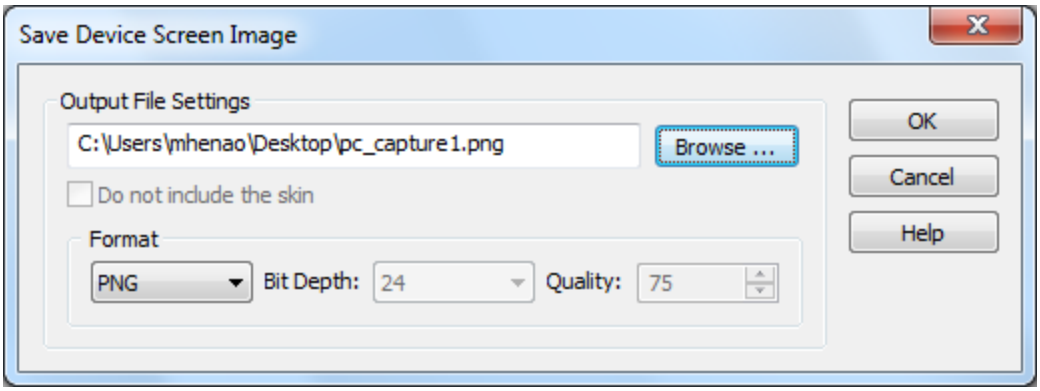


Save Screen to Disk toolbar

The following functions are available using the buttons located on the MobiControl Remote toolbar:

Function	Description
Save screen to disk	Clicking this button causes the **Save Device Screen Image** dialog box to open in order to save an image of the devices display with or without a skin to an image file on your computer.
Save screen to clipboard	Clicking this button will copy the devices screen with or without the skin to the computers clipboard. Use this feature to copy and paste into a photo editor application (such as Microsoft Paint in common Windows computers) for editing an image with the devices screen capture.
Print	This button allows the user to print the devices screen.

The **Save Device Screen Image** dialog box appears prompting the user for the file name and graphics format to use for the screen capture image file. You can use the browse button to select a folder and type in the new filename. If you are capturing a screen while in skin view, you can choose to include or exclude the skin in the captured image.



Save Device Screen Image dialog box

The following options are available depending on the type of image format that is to be generated. The image format can be selected from the **Format** drop-down box:

Image Format	Description
PNG	No further parameters are required.
JPEG	**Compression and quality factor** is a value between and including 0 and 100. This value should serve as a compromise between grain quality of the picture and color approximation and the size of the resultant file. A value of 100 means that the file is uncompressed and maximum quality is required. A value close to or equal to zero means that picture and color quality is poor and approximate but the size of the file is the smallest possible.
GIF	No further parameters are required.
TIFF	No further parameters are required.
BMP	Choose between 16 bit, 24 bit or 32 bit format for the saved bitmap file.

Edit Menu

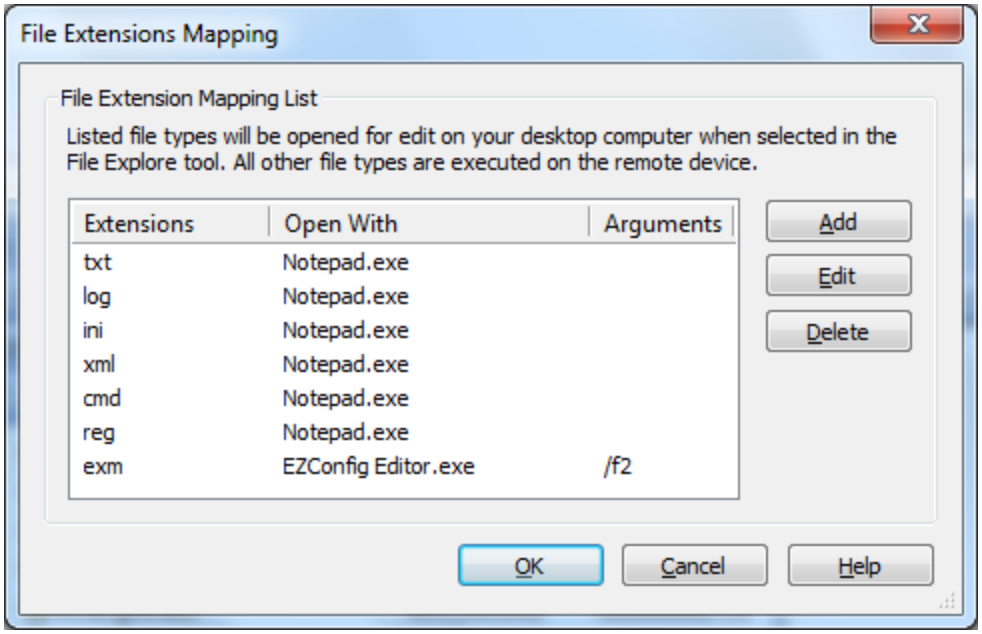
The **Edit** menu contains the following selections:

- When the **Automatically Synchronize Clipboards** menu item is checked, MobiControl Remote automatically copies any text placed in the desktop or notebook computer clipboard to the mobile device clipboard, and copies any text in the mobile device clipboard to the desktop or notebook computer clipboard. Use this feature to copy and paste text between desktop and mobile device applications.
- The **Keyboard Shortcut Settings** menu allows users to configure shortcut keys for the device. Please see the "Configure Shortcut Keys for device" topic on page 36.
- The **File Extension Mapping** option allows users to configure the device file type to open for edit on your desktop computer when selected in the File Explore tool. Please see the File Extension Mapping page.

File Extension Mapping

File extension mapping allows you to configure the device file type to open for edit on your desktop computer when selected in the File Explore tool. All other file types are executed on the remote device.

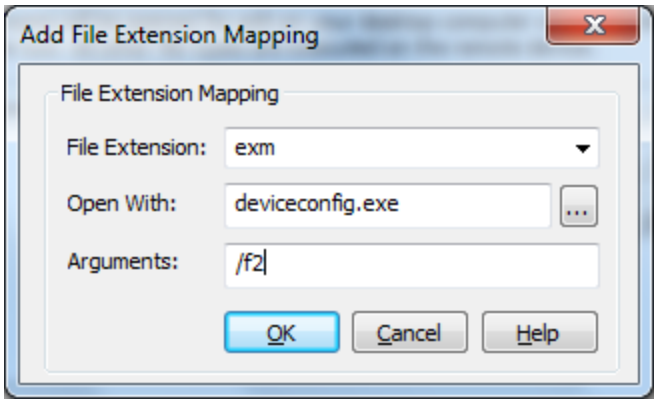
To access the File Extension Mapping tool, click **Edit**, then **File Extension Mapping** in the menu bar of the MobiControl Remote window.



File Extensions Mapping dialog box

The table below describes each field of the **File Extensions Mapping** dialog box:

Field Name	Description
Add	Add a custom extension map
Edit	Edit an existing extension map
Delete	Delete an extension map
Extensions	The mapped extensions that will run on your desktop
Open With	What application will be used to open the mapped extension



Add File Extension Mapping dialog box

The table below describes each field of the **Add File Extension Mapping** dialog box:

Field Name	Description
File Extension	The extension of the file on the device that you would like to map, e.g. `.ini`
Open With	Choose the application you would like to open files having the selected file extension, e.g. `Notepad.exe`
Arguments	Command line options to run with the application, e.g. `Notepad.exe /a`

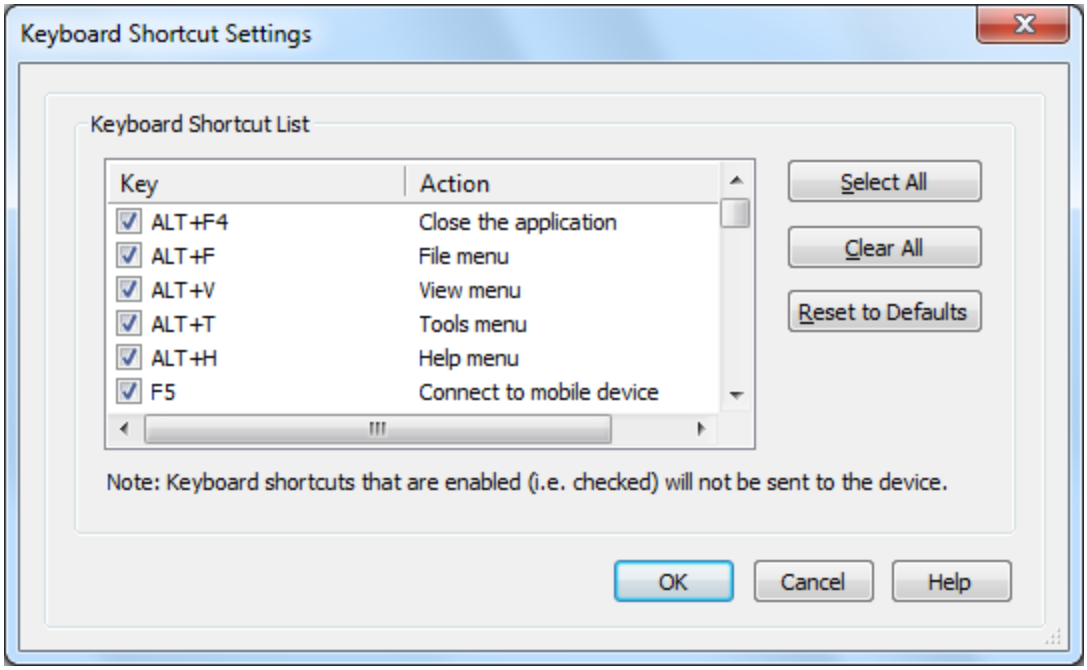
NOTE:

`.txt`, `.log`, `.ini`, `.xml`, `.cmd`, and `.reg` are all set to open, by default, in Notepad on your desktop. They may be edited by highlighting the extension and clicking **Edit**.

Configuring Shortcut Keys

Keyboard shortcut settings allows you to configure shortcut keys for the device. You can select a list of shortcut keys which you want to filter. This means that the device can receive all shortcut keys except the selected keys. By default a few standard shortcut are selected.

The keyboard shortcut settings can be accessed through the **Edit** menu, then the **Shortcut Redirection Settings** item in the menu bar of the MobiControl Remote window.



Keyboard Shortcut Settings dialog box

The table below describes each field of the **Keyboard Shortcut Settings** dialog box:

Field Name	Description
Key	List of shortcut keys, of which the selected keys will not be sent to the device
Select All	Select all shortcut keys in the list
Clear All	Unselect all shortcut keys
Reset to Defaults	Select the default shortcut keys

View Menu

The following is a description of the **View** menu items:

- The **Toolbars** sub-menu allows you to show or hide toolbars that will be displayed on the screen. The Macro, Tools, Video and Application buttons toolbars can be enabled or disabled with this menu.
- When the **Status Bar** menu option is selected, MobiControl Remote will display a status bar at the bottom of the main MobiControl Remote window.
- A **Theme** allows you to set a preset package containing graphical appearance details used to customize the look and feel of the MobiControl Remote screen.
- The **Zoom** sub-menu allows you to enlarge or shrink the mobile device screen when it is displayed on the desktop computer. The following zoom sizes are currently available: 50%, 75%, 100%, 120%, 150%, 200%, and 300%. You can also enlarge or shrink the screen size using the **Shrink Screen** and **Enlarge Screen** buttons at the top of the screen.

- **Rotation** toggles the mobile device screen orientation between portrait and landscape. This feature is especially useful for viewing slides, pictures or diagrams that need you to turn your mobile device on its side for viewing. You can view the mobile device screen in portrait or landscape modes when running MobiControl Remote with or without a skin. You can also access this feature by clicking on the Rotate icon at the top of the screen. 
- The **Color Quality** gives the capability to change color quality level 'on-the-fly' from within remote control. You can also access this feature by clicking on the Color Quality icon at the top of the screen.  To permanently change this setting, see Color reduction options here.

> **NOTE:**
>
> This setting is NOT saved back to the connection profile. If you want to start Remote Control at a certain quality level, it needs to be specified in the Remote Control Profile.

- The **Laser Pointer** allows the user to view where you have your pointer over their device screen. You can enable/disable this feature by selecting it from the Menu (View -> Laser Pointer) or by clicking on the Laser Pointer icon at the top of the screen. 

Tools Menu

The menu contains the follow selections:

- The **Explore tool** allows users to browse the file system of the mobile device as well as the desktop computer. The tool additionally allows users to transfer files between the desktop computer and mobile devices, it supports all standard file system operations such as: copy, cut, delete, rename, create folders, or drag and drop. Please see the "Explore Tool in Help Desk" topic on page 40.
- The **Registry tool** allows users to browse the registry of the mobile device, it additionally supports all standard registry operations (i.e. copy, cut, delete, rename, create registry values and create keys, export, import, find). Please see the "Registry Tool" topic on page 44.
- The **Task Manager tool** allows users to view information about the applications and processes running on mobile devices. This tool additionally allows users to stop processes, activate processes, and view detailed system information about running processes. Please see the "Task Manager Tool" topic on page 48.
- The **Service Manager tool** allows users to start and stop services on remote devices. Please see the "Service Manager Tool" topic on page 51.
- The **System Information tool** allows the user to view connected mobile device utilization and system information from their desktop. Please see the "System Info" topic on page 52.
- The **Creating Recordings** menu item allows users to create video recordings of screens on a mobile device. Captured video recordings can be to demonstrate software functionality as well as a tool for help desk personnel to document/record situations. The **Video** menu item contains two sub-items, **Record** and **Stop Recording**. Please see the "Creating Video Recordings" topic on page 54.
- The **Macro Recording and Playing** menu item allows users to record macro scripts of keyboard and mouse events. The **Macro** menu item contains five sub-items: **Record, Play, Stop, Pause, Macro Test Manager**. (Please see the "Macro Test Manager" topic on page 66 for more information about this.) Macros can be played back either through the **Play** sub-menu item or through the DOS Box as a script. Please see the "Macro Recording / Playing" topic on page 58.
- The **Soft Reset Device** menu item allows the remote mobile device to be remotely rebooted. It is possible to soft reset or hard reset the mobile device by this item. When you select the **Soft Reset Device** menu item, the soft reset reboot is going to be processed. When you hold down the `CTRL` key while selecting the **Soft Reset Device** menu item, you will be asked if you want to process the hard reset of the mobile device.

- The **Send Ctrl-Alt-Del** is used in Windows PC systems to activate the Winlogon process. This feature will ONLY be available when remote controlling into a Windows PC and is useful whenever trying to trigger Ctrl-Alt-Del function when in a remote control session to a Windows PC. The keyboard shortcut combination pressed will bring up the Ctrl+Alt-Del function on the local machine instead of the machine remotely logged on via MobiControl Remote Control. This behavior is by design though, as Ctrl-Alt-Del key combination is too important for any PC (to run especially when computer encounters halt error or hang). As such, Ctrl-Alt-Del keyboard shortcut is always reserved for local host computer. In order to send Ctrl-Alt-Del keystrokes to the remote computer, you would need to click on Tools, and then the Send Ctrl-Alt-Del.

  NOTES:

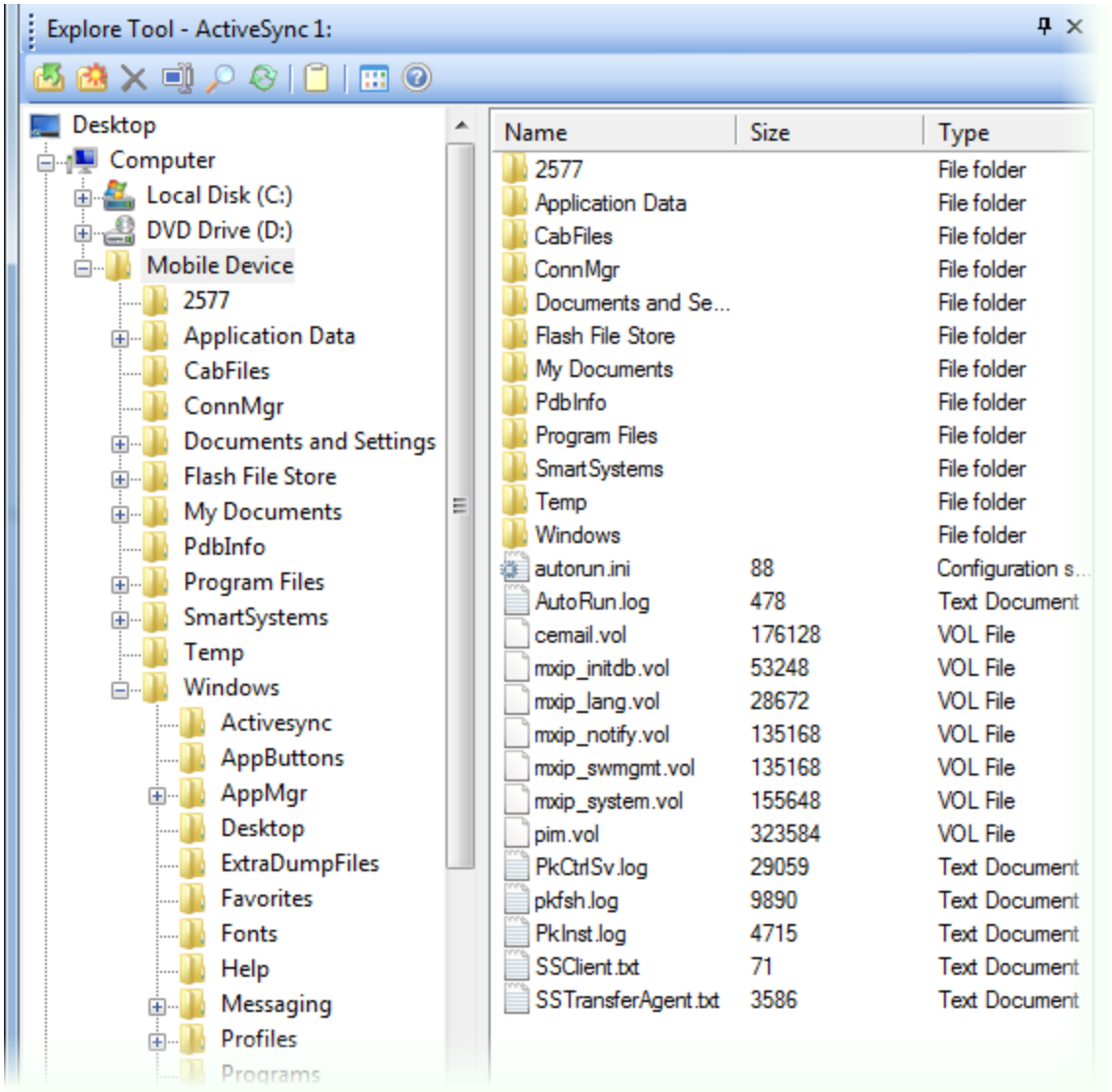
  - When remote controlling a Windows 7 PC, you must have the Windows logon options "software secure attention sequence" enabled. To enable this feature, you must have administrative rights on the Windows 7 computer and perform the following:

    1. Open up your systems Command Prompt by clicking Start and then typing **cmd** in the start menu search.
    2. On the command line type **gpedit**
    3. Go to **Administrative Templates**
    4. Go to **Windows Components**
    5. Go to **Windows Logon Options**, right click and select edit on **"Disable or Enable Software Secure Attention Sequence"**
    6. Select the **Enabled button**, and choose **"Services"** from the Option drop down.
    7. Then click the **OK** button.

- The **Application buttons** emulate the functionality of the buttons on the case or body of your mobile device. Clicking these buttons would launch the applications or functions that pressing the buttons on the device would launch. If the buttons are remapped to a different application on the device, clicking the application buttons in MobiControl would reflect that. Application buttons are only available when skin mode is enabled.

Explore Tool

The MobiControl Explore tool allows users to browse the file system of the mobile device as a part of the computer's file system. In addition to browsing, the Explore tool allows users to perform standard file management operations, such as search for files or folders, transfer files between the computer and the mobile device, delete files, rename files, create folders, and set file attributes.



Explore Tool dialog box

Smart Editing

The MobiControl Explore tool supports smart editing, allowing you to view and edit text files directly from your mobile device. You can double-click on any file with a `.txt`, `.ini` or `.log` file extension and MobiControl will open it on your computer using Windows Notepad. You can make changes to the file and save it quickly back onto the mobile device.

Viewing or editing a file

1. Double-click the text file you want to view or edit.
2. On the desktop computer, the selected file will be open in Notepad.
3. Edit, save and close the file.
4. If the file changed, it will display a message to save the changed file onto the device.
5. Select **Yes** to save the changed file, otherwise select **No**.

Executing or Running a Program on the Device

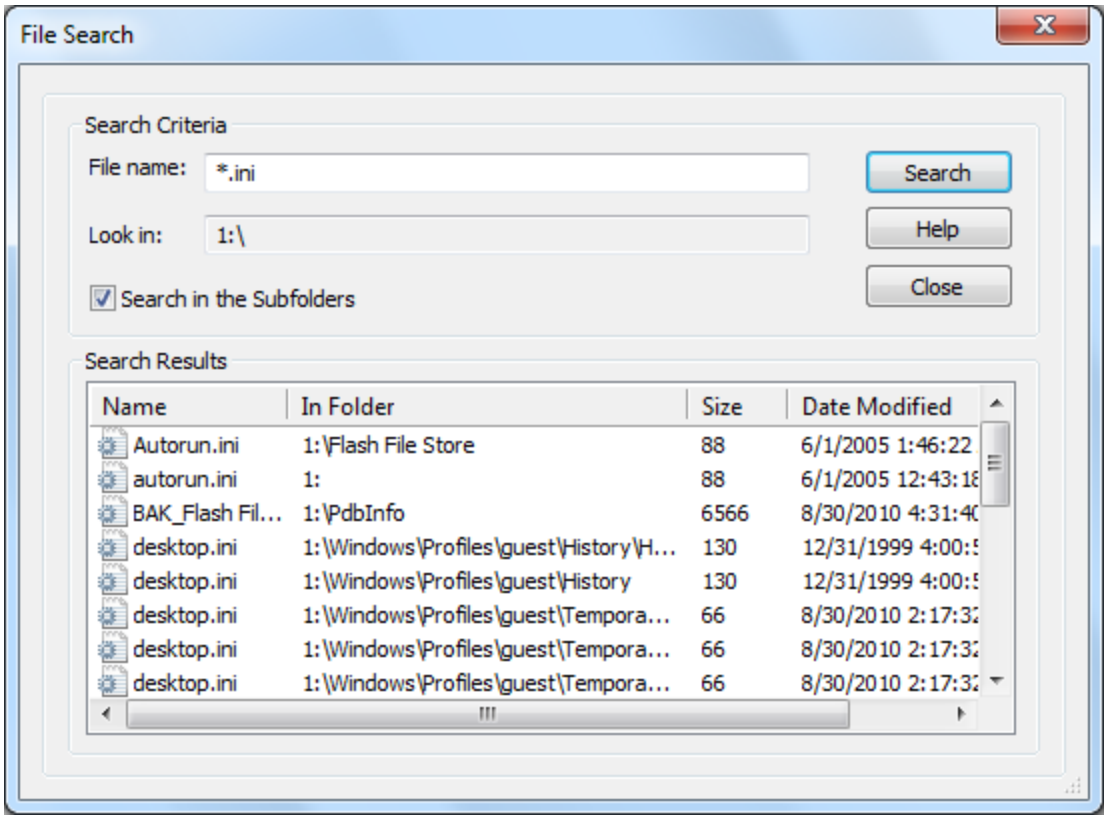
You can double-click other files to open or launch them on the mobile device. For example, if you double-click a file with a `.cab` or `.exe` file extension in the Explore tool, the file and the related application would be launched on the device. If you double-click a file with a `.doc` or `.xls` extension, the appropriate application will be launched on the mobile device and the file would be opened using that application (for example, double-clicking a `.doc` file would launch Word Mobile on the mobile device and open the document). Double-clicking a registry file with a `.reg` extension will update the mobile device's settings and merge the registry settings with the mobile device's registry.

View System Files

The Explore tool allows you to view hidden system files on the mobile device. To view the files, select 'Show System Files' from the **View** menu in the File Explore tool.

To Search for a File or Folder

Select the drive or folder in left pane of the Explore Tool, and then either right-click on the selected folder and then select the **Search** menu option or click on search icon  in the toolbar. The **File Search** dialog box will be displayed.



File Search dialog box

Enter the file specification of what you are searching for in the **File Name** field. If you need sub-directories to be searched, select the **Search in Subfolders** option, and then click **Search**.

The list of matching files or folders will be displayed in the **Search Results** list.

Double-clicking a file in the **Search Results** pane would open the folder containing the file in the Explore tool for quickly locating a file.

NOTE:

The MobiControl Explore tool shows the file system of the mobile device two which it is connected as the `1:\` drive.

Common File or Folder Operations

Rename a file or folder

1. Select the file or folder you want to rename.
2. Select **Rename** from the **File** menu or right-click on the selected file or folder and select **Rename** from the pop-up menu.

3. Type the new name, and then press ENTER.

Copy and paste file(s) or folder(s)

1. Select the file(s) or folder(s) you want to copy.
2. Select **Copy** from the **Edit** menu or right-click on the selected file or folder and select **Copy** from the pop-up menu.
3. Click on the destination folder or drive where you want to copy these file(s) or folder(s).
4. Select **Paste** from the **Edit** menu or right-click and then select **Paste** from the pop-up menu.

Move file(s) or folder using drag-and-drop operations

1. Find the files or folder you want to move.
2. Make sure the destination for the files or folder you want to move is visible.
3. Drag the files or folder to the destination.

Delete file(s) or folder(s)

1. Select the file(s) or folder(s) you want to delete.
2. Select **Delete** from the **File** menu or right-click on the selected file(s) or folder(s) and select **Delete** from the pop-up menu.

Change the properties of a file or folder

1. Select the file or folder for which you want to get or set properties.
2. Select **Properties** from the **File** menu or right-click on the selected file or folder and select **Properties** from the pop-up menu.
3. The **File Properties** dialog box will be displayed.
4. Change the file attributes and click **Apply**.

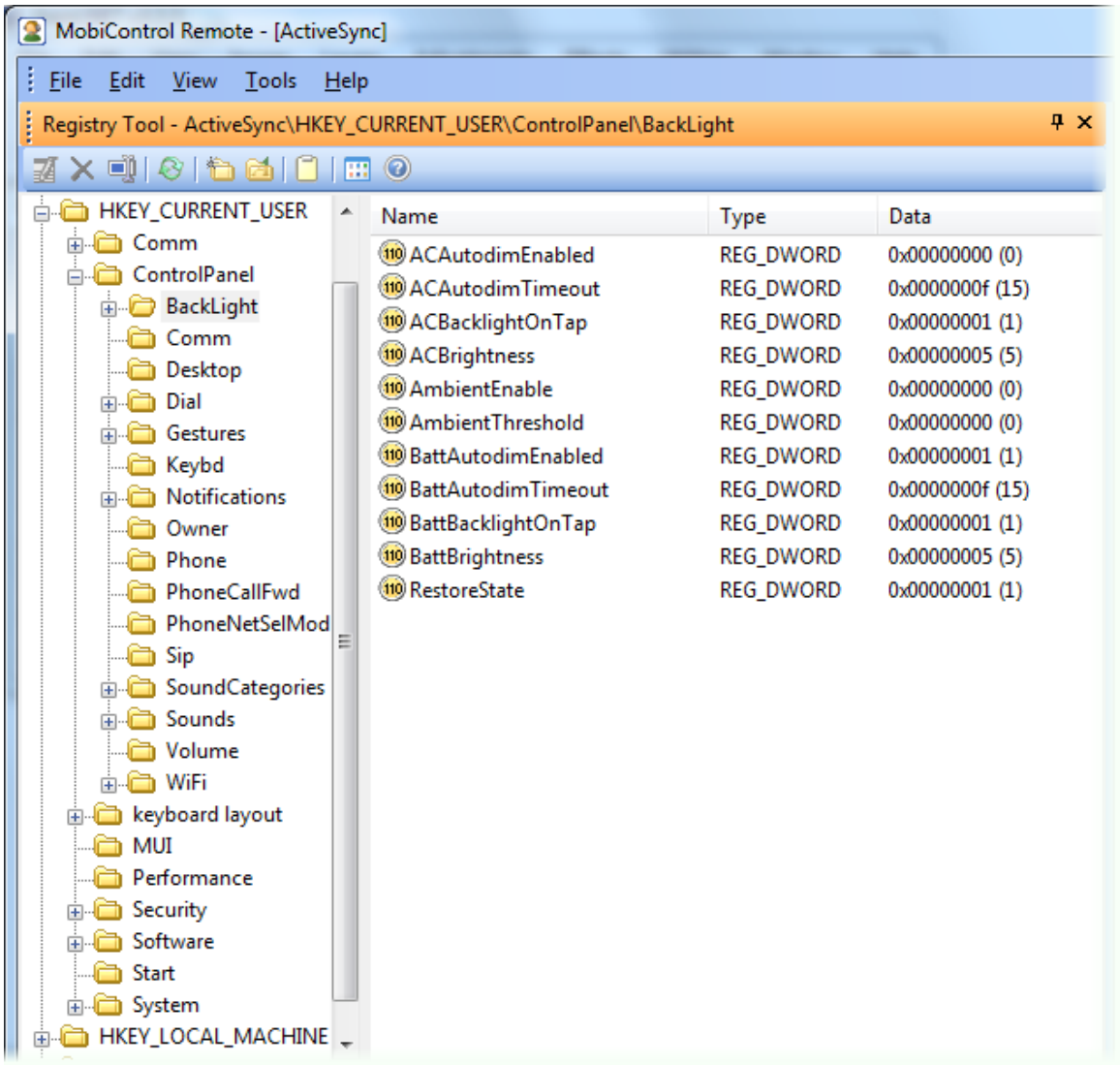
Registry Tool

MobiControl Remote Registry tool can be used whenever MobiControl Remote is connected to the mobile device over an ActiveSync or a TCP/IP or a serial connection.

The MobiControl Remote Registry tool allows users to manage the registry of the mobile device. In addition to browsing, the MobiControl Registry Tool allows users to perform standard registry operations, such as creating, deleting, modifying and renaming keys as well as string, DWORD, binary and multi-string values. You can export the registry from the device and save it to an ANSI or UNICODE format registry file (with a `.reg` file extension). This can be useful for creating a backup of the device's registry which can be imported into the device when needed.

IMPORTANT:

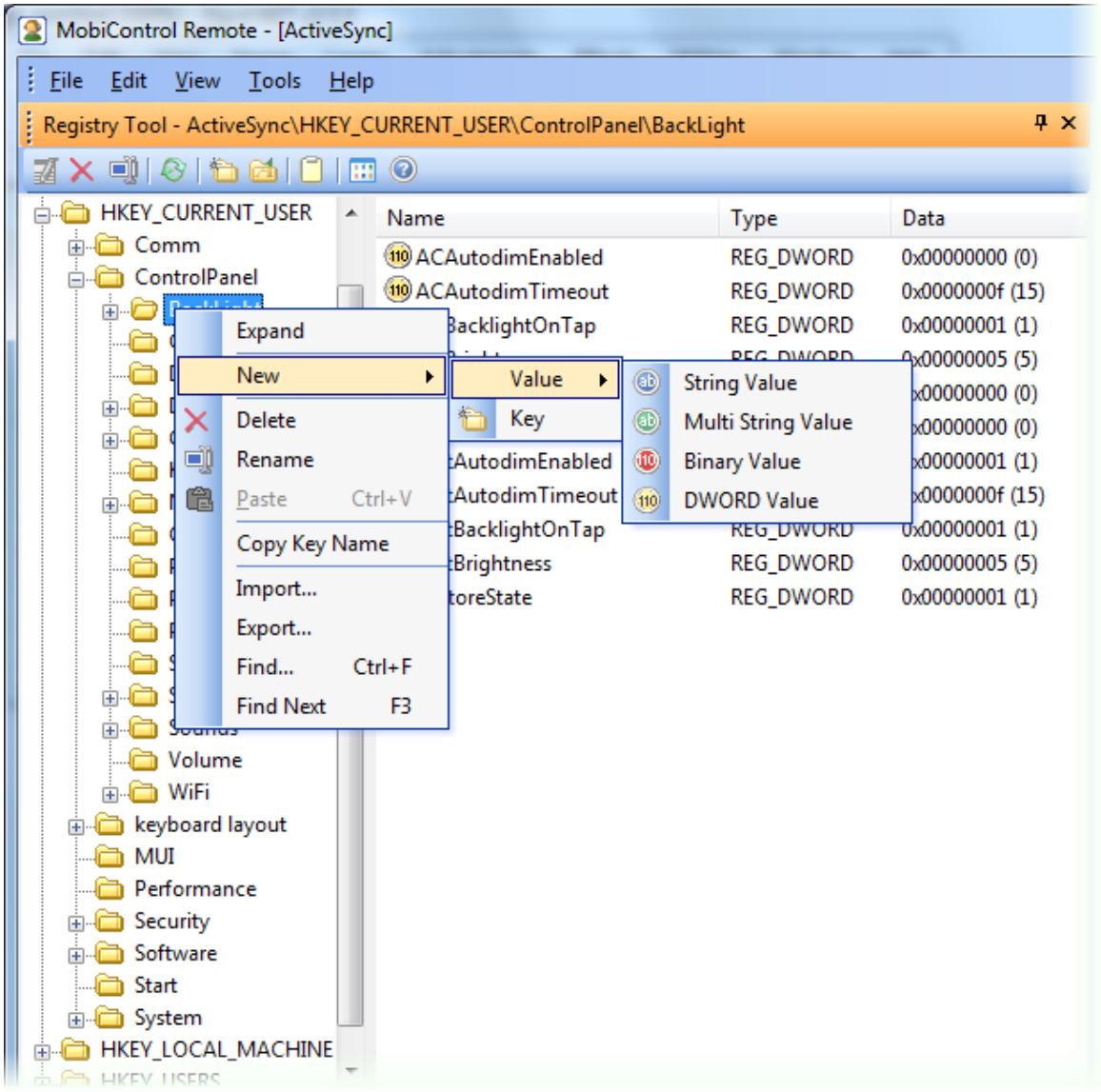
The MobiControl Registry tool is recommended for advanced users. Using the Registry tool incorrectly can cause serious mobile device problems that may require you to perform a master reset / wipe to restore the device settings back to the factory defaults. SOTI is not responsible for any problems resulting from incorrect use of the Registry tool.



Registry Tool dialog box

Creating and Editing Registry Values

The registry tool allows you to create new registry values or edit existing values for any registry key. To create a new value, right-click in the registry values pane and select **New** from the **Registry Values** menu that appears or select **New** from the **View** menu. You can create different types of registry values as shown in the image below. To edit a value, double-click that value in the Values pane.

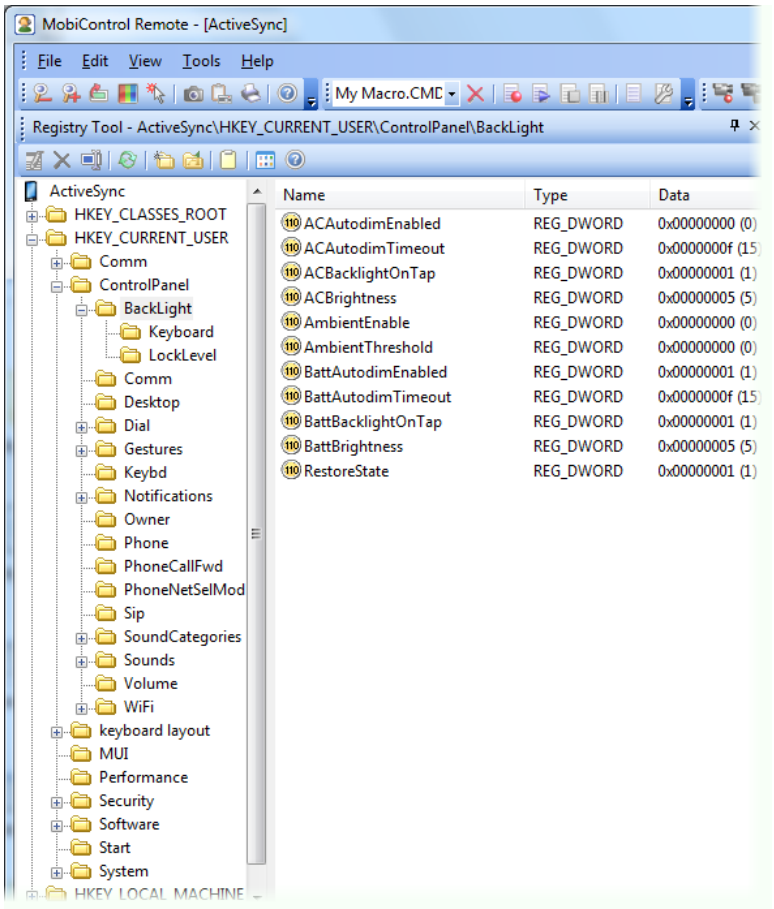


Registry Values menu

Exporting and Importing Registry Keys

Advanced registry functions can be accessed by right-clicking in the Registry Tree pane to bring up the **Registry Keys** menu or by selecting the appropriate function from the **Edit** menu.

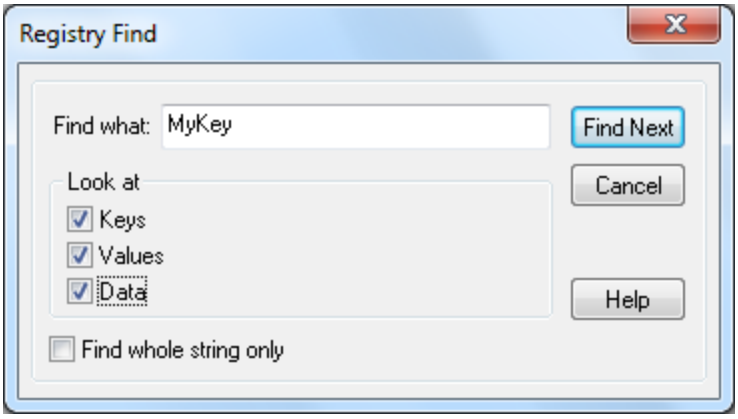
It is possible to export any part of the registry subtree to a `.reg` file, which can be imported back into the device allowing for backup and restore of the mobile device's registry. To export a registry key, right-click on the desired registry key (folder), and select **Export** from the pop-up menu. While importing registry subtree(s), you cannot specify the registry subtree where you wish to store the imported data. The subtree location is already saved in the file you are about to import and cannot be changed. This behavior is similar to the desktop tool `re-edit.exe` from Microsoft.



Registry tool functions

Searching the Registry

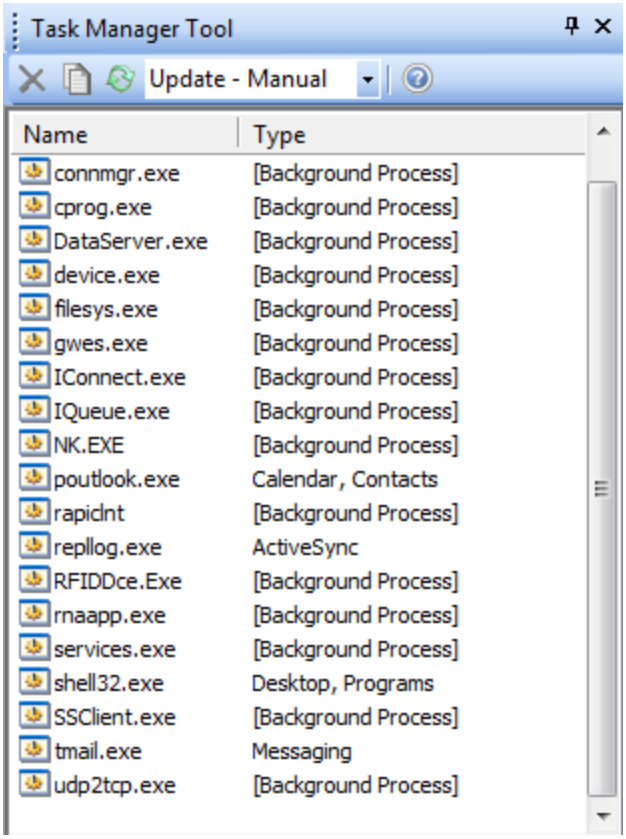
The Find feature allows you to find keys, values or data in the registry. Searching through data is limited to string or multi-string values only.



Task Manager Tool

The MobiControl Manager tool allows you to view a list of the various applications and processes running on the mobile device. This list includes the processes actively running on the device as well as the background processes that may be running, allowing better visibility over the resource utilization on the device. This information may be useful if the device is running slow or some application or process is causing the device to freeze or "hang."

Additionally, the user can view the details for a process and kill or stop a process. Using the Task Manager, you can also view which processes are using the device's memory and you can determine which process is causing a problem by terminating the processes, one at a time, in a controlled manner to identify the source of the problems being observed on the device.



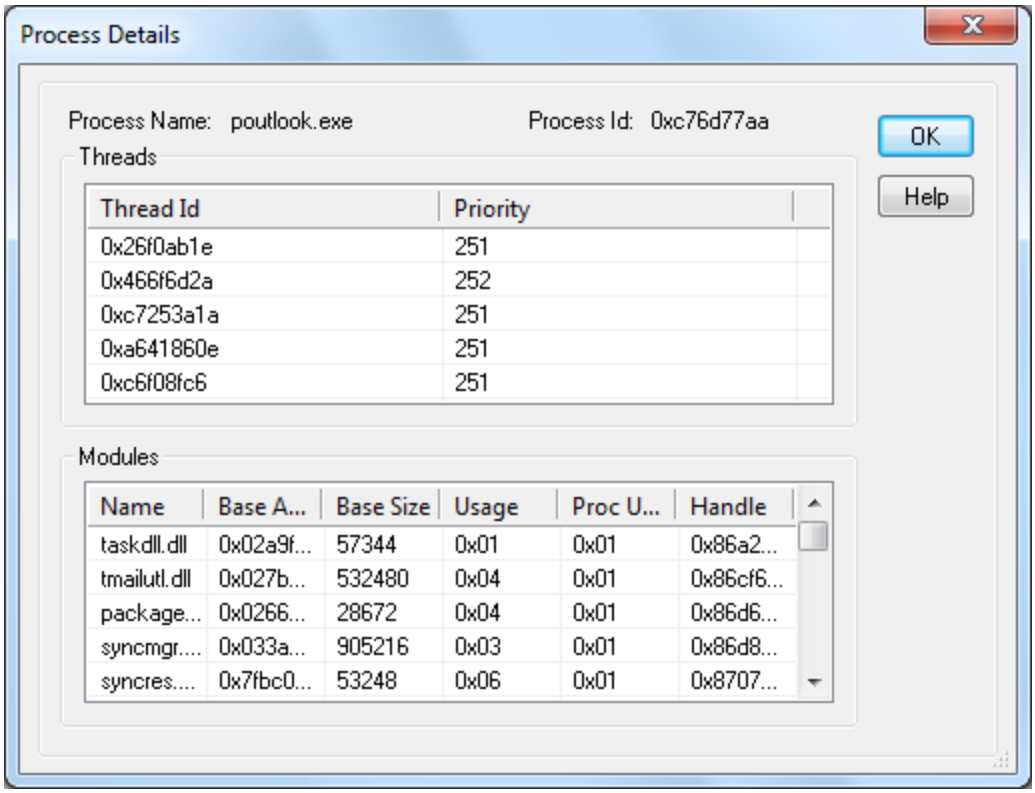
MobiControl Task Manager tool

The following functions are available using the buttons located on the top of the window:

Function	Description
Refresh	The list of processes displayed is refreshed from the mobile device
Kill Process	This button allows the user to kill or shutdown an application or process. Care must be taken not to kill or shutdown core applications or processes as the operation of the mobile device may be affected. Core applications or processes are typically described as '[Background Process]' in the Processes pane. The capability to kill a process running on the device is intended to allow the users to shutdown misbehaving programs during troubleshooting.
Details	This button allows the user to display process details for the currently selected process in the Processes pane. Please see the "Process Details Dialog Box" topic on page 49 for more information.

Process Details

This dialog box displays detailed information about a specific process. To view process details, the user must select a process from the Task Manager tool, and then click on the **Details** button.



The Threads table has one row for each thread in the process. Each row of the table contains information about a specific thread.

Field Name	Description
Thread ID	Number that is used by Windows Mobile or Windows CE to reference the thread
Priority	Higher priority threads execute before lower priority threads

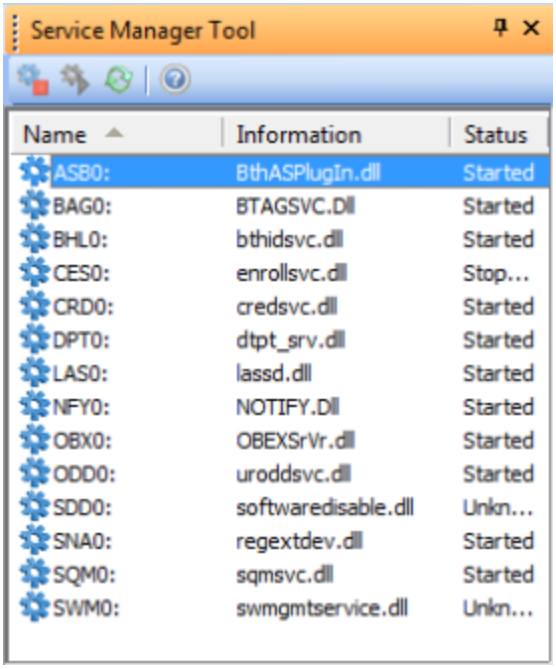
The Modules table has one row for each module or `.dll` (Dynamically Loaded Library) that is loaded by the process. The following text describes the columns in this table.

Field Name	Description
Name	Name of the module or `.dll`
Base Addr	Base address of the module in the context of the owning process
Base Size	Size in bytes of the module
Usage	Global usage count on the module
Proc Usage	Module usage count in the context of the owning process
Handle	Handle of the module in the context of the owning process

Service Manager Tool

The Service Manager tool allows you to start and stop services on remote devices.

A service is a program, routine, or process that performs a specific system function to support other programs, particularly at a low level (close to the hardware). Service applications typically provide features such as client/server applications, web servers, database servers, and other server-based applications to users.



MobiControl Service Manager Tool

The following functions are available using the buttons located on the top of the window:

Function	Description
Stop	Stops a running service
Start	Starts a stopped service
Refresh	List of services displayed is refreshed from the mobile device

System Information Tool

The System Information tool allows you to view and monitor critical performance indicators for the mobile device including device use, battery charge, memory and storage use and other useful system information graphically and numerically from your desktop. The system information includes information about the device hardware, operating system and display.

The following is a list of the fields on this dialog box and a brief description of each one.

General Information

Field Name	Description
Version	The Windows operating system on the mobile device
Processor	The type of processor used in the mobile device

Display Information

Field Name	Description
Width	The mobile device screen width in pixels
Height	The mobile device screen height in pixels
Number of colors	The number of colors the mobile device is capable of displaying
Bits per pixel	The screen resolution the mobile device is capable of displaying

Memory Information

Field Name	Description
Utilization	The percentage of memory that was being used at the time the reading was taken
Device RAM	The total physical memory, and the available physical memory at the time the reading was taken.
Virtual RAM	The total virtual memory, and the available virtual memory at the time the reading was taken
Device Storage Memory	The total object store memory, and the available object store memory at the time the reading was taken
Page Allocation Size	This is the allocation unit used by the virtual memory system to allocate new memory
Application Address	The lowest and highest memory address accessible to applications and dynamic-link libraries (`.dlls`)

Battery Information

Field Name	Description
Main	The percentage of primary battery power available, at the time the reading was taken
Backup	The percentage of backup battery power available, at the time the reading was taken

Support Chat

Support chat allows for a bidirectional text conversation between the remote helpdesk user and the end mobile device user. The remote helpdesk user can have a text conversation with the mobile device user by using the built-in Chat feature in the Chat pane when remote controlled into a device. The mobile device user can access chat from the menu options available by clicking on the MobiControl icon or the MobiControl configuration applet in control panel. This feature can be turned on or off from the Tools menu by clicking **Chat Tool** or by pressing **Ctrl+H** on your keyboard.

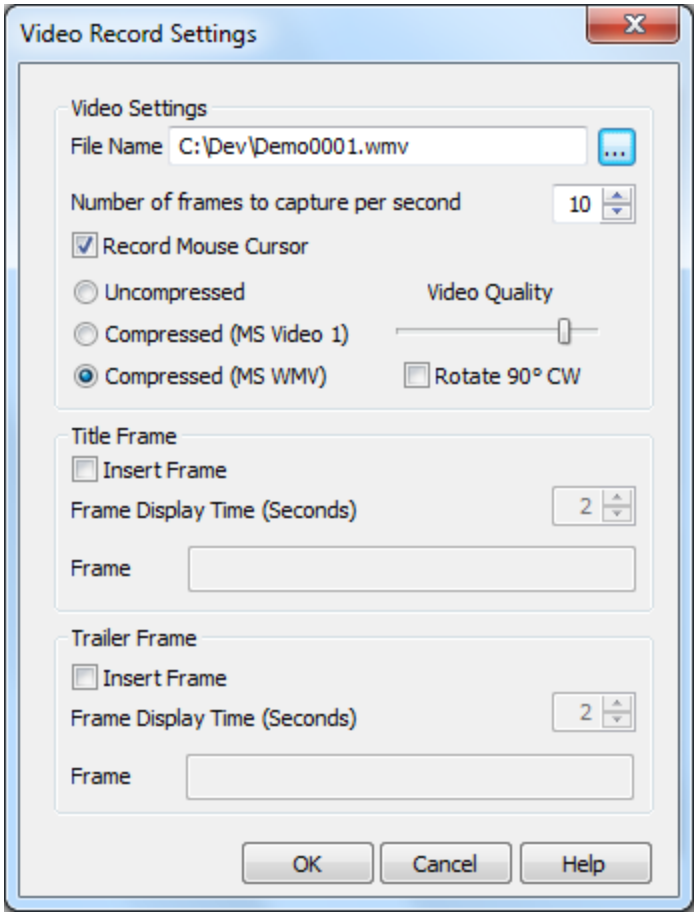
NOTE:

This feature is available on the device ONLY if the device is currently being remote controlled.

Field	Description
Chat Window	The Chat Log field displays the messages sent between the remote helpdesk user and the end mobile device user
Message	The Message Entry field enables input of text.
Send Button	The Send button transmits the typed message to the selected device.
Dismiss	Closes the Chat Window, and places in the background.

Creating Video Recordings

Recordings are commonly used to create demonstrations of mobile device software. A recording file can be easily distributed and played back on any Windows-based computer. You can save MobiControl Remote recordings in either `.wmv` or `.avi` format. These recordings can be played with the Microsoft Windows Media Player software, which is present on most Windows based computers and can also be downloaded from the Microsoft web site. The Microsoft Media Player software has several useful features for playing recordings such as "Full Screen Mode" which is useful when the recording is being projected onto a screen. Media player also has a **Repeat Forever** option that allows recordings to be continuously played back. This feature can be used in combination with the full screen setting, to display continuously running demonstrations as seen at trade shows and conferences.

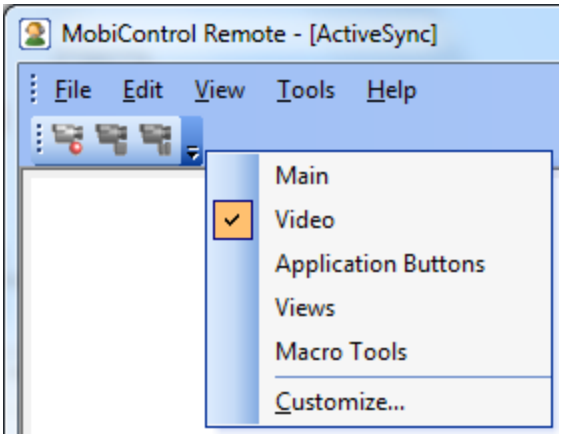


Recording Information dialog box

A recording can also be used as a training tool to record how a particular task or function can be accomplished using one or more software tools. Recordings can even be used to document problems in mobile device software and can be emailed to the appropriate support staff.

To create a recording with MobiControl Remote, click **Tools**, then **Record**, and then **Begin Recording**. The **Begin Recording** menu option will be disabled if MobiControl Remote is not connected to a mobile device. (To connect, select **Connect** from the **File** menu.) Once **Begin Recording** has been selected, the **Recording Information** dialog box will be displayed.

A Video toolbar can be added to the main Remote Control toolbar by right-clicking the toolbar and selecting **Video** for easier access.



Video Toolbar

The following is a list of the fields in the **Video Record Settings** dialog box and a description of each one:

<table>
<tr><th>Field Name</th><th>Description</th></tr>
<tr><td>File Name</td><td>Enter the name of the file to which the recording is to be saved in this field. A recording file name must have a <code>.wmv</code> or <code>.avi</code> file extension:
You can click the Browse button to the right of this field to browse to the directory in which you want to store the recording file.
EXAMPLE:
"<code>C: \Demo.WMV</code>" is a valid recording file name, but "<code>C: \Demo</code>" is not.</td></tr>
<tr><td>Number of frames to capture per second</td><td>This field is used to specify the number of frames to be captured every second, otherwise known as the frame rate. The higher the value (maximum 15) the larger the video file will be. The lowest is one.
A video file with a frame rate of four is four times larger than a video file with a frame rate of one. However if you are trying to capture very fast events on the screen that can be visible for less than say a second and the frame rate is set to one, then it may not be captured in the resulting video file.</td></tr>
<tr><td>Record Mouse Cursor</td><td>When this field is checked the recording will include mouse movements. Being able to see mouse movements in the recorded video is important when recording training segments, so that users can see which buttons or controls are being clicked on.</td></tr>
<tr><td>Uncompressed / Compressed</td><td>If you do not want the recording to be compressed, make sure that Uncompressed is selected and click the OK button. Use the radio buttons to select a compression method for the video. Different methods offer varying degrees of playback quality and compression. Generally, you should compress your video in order to save disk space. However, if you plan on editing the video, you should select the uncompressed option.
If you want the recording to be saved as a compressed file then select the appropriate compressor from the Compressor field and then click the OK button. You can select between two types of compressions:
MS Video 1
MS WMV
<table><tr><th>Method</th><th>Quality</th><th>File size</th></tr><tr><td>Uncompressed</td><td>1</td><td>3</td></tr><tr><td>Microsoft Video 1</td><td>2</td><td>2</td></tr><tr><td>Microsoft Windows Media Format</td><td>3</td><td>1</td></tr></table>1=Best quality, 1=Smallest file size</td></tr>
<tr><td>Video Quality</td><td>When creating a compressed video, this slider controls the degree of compression. Moving the slider to the right increases quality but decreases compression. Moving it to the left decreases quality and increases compression. This has no effect when creating an uncompressed video.</td></tr>
<tr><td>Rotate 90° CW</td><td>Rotates the video clockwise by 90 degrees</td></tr>
<tr><td>Title Frame - Insert Frame</td><td>If you would like to insert a title frame make sure this field is checked. A title frame is often used to insert a frame at the start of the recording that describes what the recording is about. If you are creating a recording to be used to demonstrate</td></tr>
</table>

Field Name	Description
	software, then the title frame would typically contain the name of the software and possible the version of the software.
Title Frame - Frame Display Time (Seconds)	Duration for which the title frame is to be displayed
Title Frame - Frame Text	Text to be displayed in the title frame
Trailer Frame - Insert Frame	Enable this field to insert a trailer frame. A trailer frame can be used to insert a frame at the end of the recording that has some closing information about the recording. If you are creating a recording to be used to demonstrate software, then the trailer frame might contain information about where to get more information about the software or the URL of the company's web site.
Trailer Frame - Frame Display Time (Seconds)	Duration for which the trailer frame is to be displayed
Trailer Frame - Frame Text	Text to be displayed in the trailer frame

Once you click the **OK** button on this dialog box, recording immediately begins. To stop recording, click the **Tools** menu, then click **End Recording** from the main toolbar, or click the **Video Stop** button from the MobiControl toolbar.

When recording has ended an information dialog box will appear giving you the ability to view the video or the containing folder of the video which was just recorded and saved.

IMPORTANT:

Do not forget to stop recording once you have started, as the recording will eventually consume all of your disk space.

Macro Recording and Playing

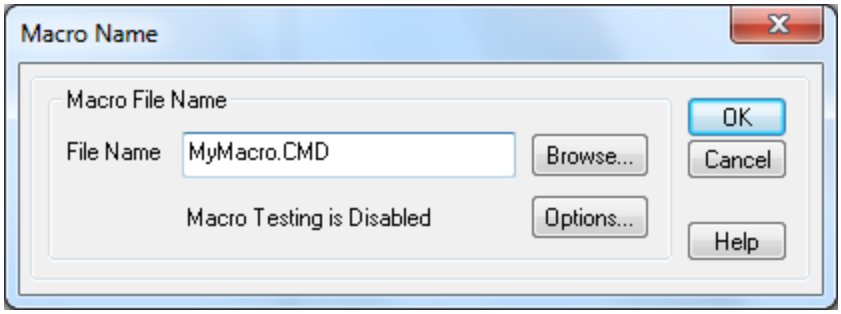
The MobiControl Remote Macro facility allows users to record keystrokes and mouse clicks or stylus taps to a file that can then be played back to the mobile device as if a real user were entering the commands. The generated recording file is a script, that can be edited and customized for specialized needs.

Macro Testing Facility

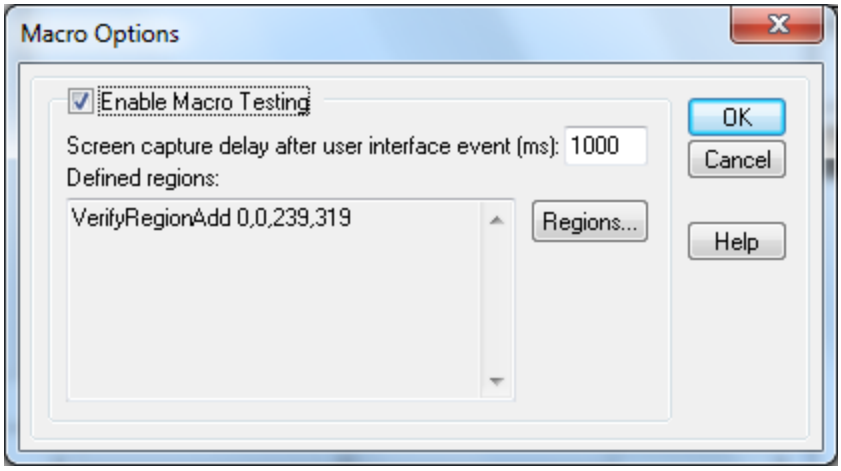
In addition to macro recording and playback functionality, the Macro subsystem also includes a 'testing facility' that allows macros to be used as a tool for software regression testing and analysis. This feature is useful for software developers and testers. When a macro is recorded with the testing feature enabled, special commands are inserted into the generated scripts so that when played back with testing enabled, the screens will be validated against the original screens that were displayed when the macro was recorded. The Macro testing functionality allows users to graphically specify the portions of screens that are to be used during testing. Additionally the macro testing facility includes tools to visually analyze the results of a macro that was run through the testing facility.

Creating a Macro Recording File

1. From the MobiControl Remote window, open the **Tools** menu, select **Macro,** and click **Record**.
2. In the **Macro Name** dialog box, enter the file name of the macro. You may browse to the appropriate directory by clicking the **Browse** button. If you wish to create a macro without testing, go to step 4.



3. To enable macro testing, click the **Options** button, then in the **Macro Options** dialog box check **Enable Macro Testing.** By default the entire screen will be used for testing, you can edit the area that you would like to use for testing by clicking the **Regions** button. (Please see the "Macro Region Definition Dialog Box" topic on page 62.) The **Screen capture delay after user interface event** field tells MobiControl Remote how many milliseconds to wait from the time a mouse/key event before capturing the screen. To set macro testing regions and screen capture delay, click the **OK** button in the **Macro Options** dialog box.



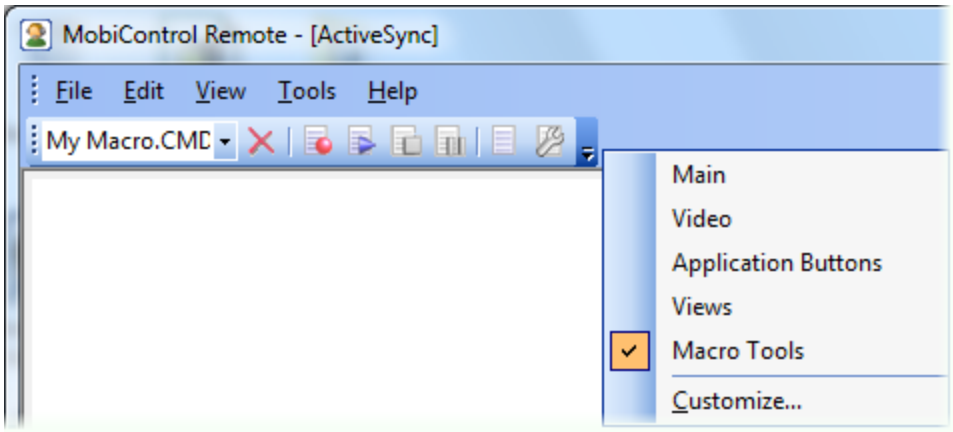
4. Click on the **OK** button to begin recording. Macro recording begins immediately; all keyboard and mouse events are recorded to the specified macro file. When playing back a macro it is generally important to start playing back a macro at the same place (i.e. same screen, same field ...) where you began recording.
5. To stop recording, from the MobiControl Remote window, open the **Tools** menu, select **Macro,** and click **Stop.**

NOTE:

If a macro is being recorded with testing enabled, macro recording can be paused at any time so that region definitions, as well as other parameters can be changed. This allows testing comparison regions to be changed as the recording goes through programs/screens with different characteristics. Testing characteristics can also be changed by manually editing the generated macro script.

Macro Toolbar

A Macro toolbar can be added to the main Remote Control toolbar by right-clicking the toolbar and selecting **Macro Tools** for easier access.



Displaying the Macro toolbar

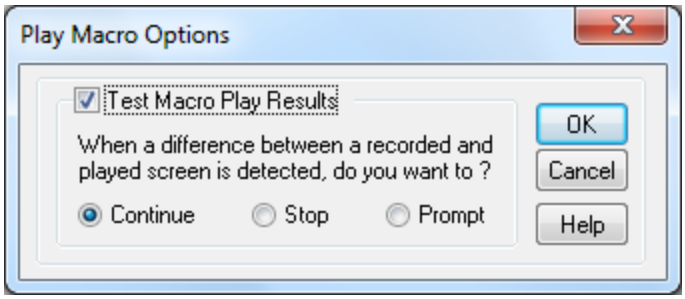
The following functions are available using the buttons located on the MobiControl Remote toolbar:

Function	Description
Macro CMD drop-down	This drop-down will display previously made macros, which can be easily played back by clicking the appropriate macro name.
Macro delete	When a macro is selected in the macro drop-down, it can be easily deleted by clicking this button.
Macro Record	Click this button to start recording a macro.
Macro Play	Click this button to play back a recorded macro when it is selected in the macro drop-down.
Macro Stop	Click this button to stop a macro when it is being recorded.
Macro Pause	Click this button to pause a macro while it is being recorded, to continue afterwards.
Macro Test Manager	Click this button to open the Macro Test Manager dialog box.
Macro Options	You can only get into the Macro options if Macro Testing is enabled. Here, you can see the testing options.

Playing a Macro File

1. From the MobiControl Remote window, open the **Tools** menu, select **Macro,** and click **Play,** or from the MobiControl Remote Macro toolbar, select the macro you just recorded and then click the **Macro Play** button. If you are not using the macro testing facility go to Step 3.

2. If the macro was recorded with the information needed for the macro testing, MobiControl Remote displays a dialog box that allows the user to select how the macro is to be played. This dialog box allows the user to select the action that MobiControl Remote should take when there is a difference between a recorded screen and a played screen.



3. Click the **OK** button to start playing the macro.
4. To stop playing a recording, from the MobiControl Remote window open the **Tools** menu, select **Macro,** and click **Stop,** or on the MobiControl Remote Macro toolbar select the **Macro Stop** button.
5. When macro playing completes a message box is displayed, if the macro was played without the Testing option, click on the **OK** button to complete playing. If the macro was played with the testing feature enabled, the **Macro Test Result** dialog box will be displayed and results of test run will be automatically exported to a log file. Please see the "Macro Test Result" topic on page 64 for more details.

Pausing Macro Recording or Macro Playback

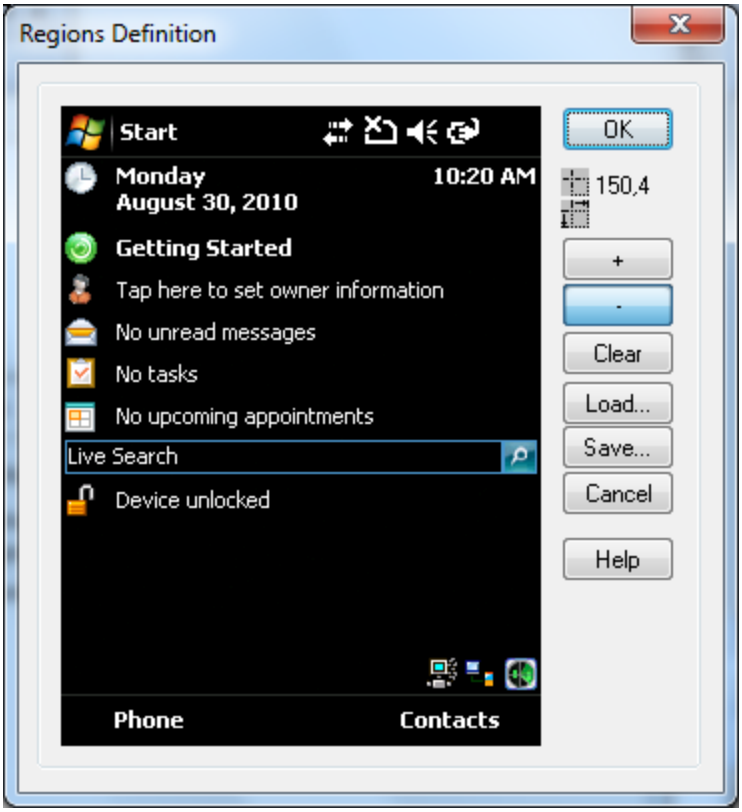
From the MobiControl Remote window, open the **Tools** menu, select **Macro,** and click **Pause.** If the macro is being recorded with testing mode enabled, you can change the region definitions and the screen capture delay. To do this, click the **Pause** button or select **Pause** from the menu, then open the **Tools** menu, select **Macro,** and click **Macro Options.** When finished, click the **Record** button again or select **Record** from the menu to continue recording. From now on, Macro Testing will use the newly defined regions and delay settings.

Stopping Macro Recording or Playback

From the MobiControl Remote window, open the **Tools** menu, select **Macro,** and click **Stop.**

Macro Region Definition

The MobiControl Remote macro testing facility allows users to specify screen regions that needs to be checked when macros are played back with testing enabled. The regions can include or exclude any rectangle on the mobile device's screen, for instance, the area with the system clock could be removed.



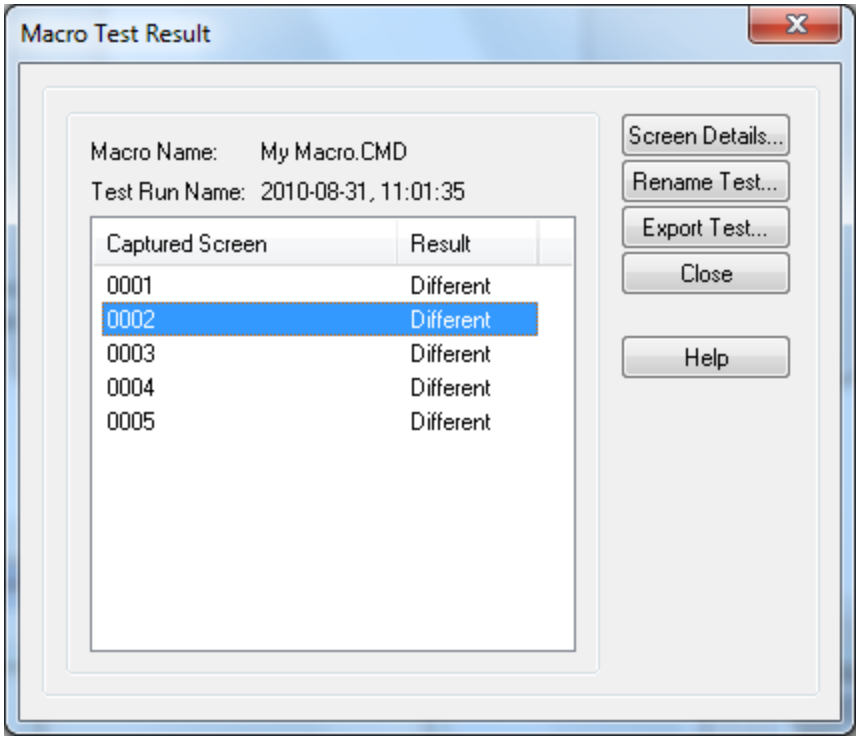
The **Regions Definition** dialog box shows a static device screen and allows users to define screen regions that are to be used for comparison during testing runs. To remove a region, click on the **-** button and use the mouse to define the region. (Click the left button and then move the mouse. Finish selecting the region by releasing the left mouse button.) To add a region click on the **+** button and use the mouse to define the region. The **Clear** button removes all defined regions. If you need to reuse the same set of region definitions, you can load or save region definitions into a region definition file (a file with the `.rgn` extension).

NOTE:

All already defined regions are lost when the regions are loaded from a region definition file.

Macro Test Result

The **Macro Test Result** dialog box lists the screens that were captured after each keyboard or mouse event in the macro. The Result column in the list shows the result of the comparison between the screen displayed during recording and the screen displayed during playback. You can view the differences, if any, by selecting a specific screen from the list and clicking on the **Screen Details** button. (Please see the "Macro Test Result Details" topic on page 68 for more information.) You can also double-click a screen in the list.



MobiControl Remote automatically generates a test name based on the date and time when the test was executed. The test name can be changed at any time by clicking on the **Rename Test** button.

When the macro is played with the testing feature enabled, there is automatically created a text log file with results when macro play finishes. The result text log file is stored in the directory which has the same name as the macro, e.g. for macro `test.cmd`, the result log file is stored in the directory `<macro_dir>\test`. The file name of the result log file is created based on the date and time the macro was run with testing enabled, e.g. `20031006150454.log`. There is also a possibility to export the test run results to the text file manually by clicking on the **Export Test** button. It asks you for the file name and location, and where you want to save the results. The format of generated text file is tab-delimited clear text.

EXAMPLE:

```
Screen  Result
0001    OK
0002    OK
0003    OK
0004    OK
0005    OK
0006    OK
0007    Different
0008    OK
```

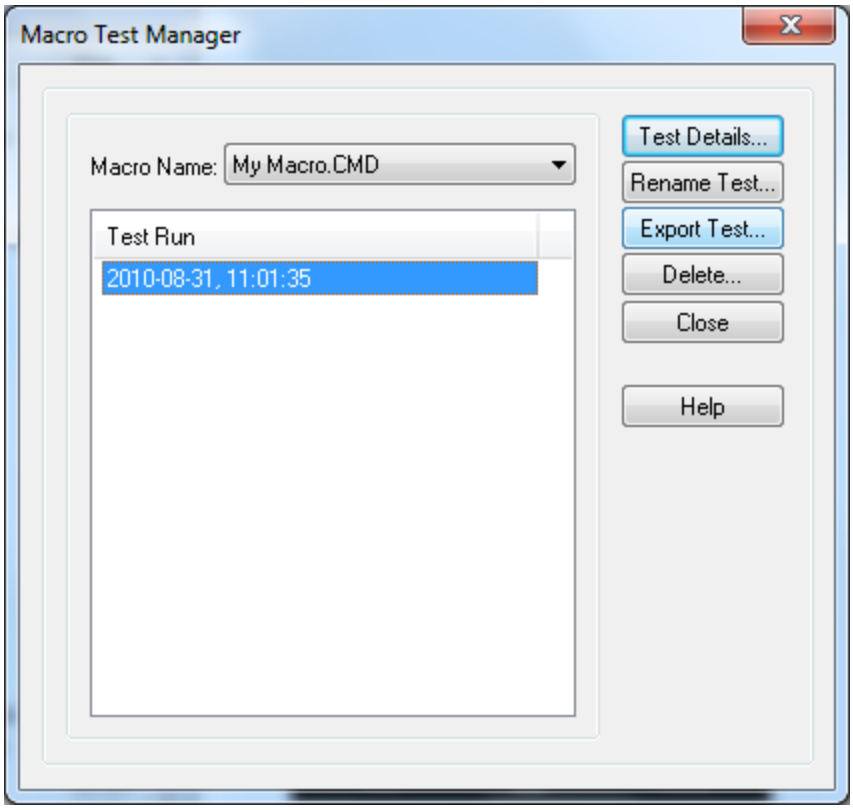
NOTE:

The results of running macros in testing mode can be accessed at any time via the Macro Test Manager tool. To access this tool, from the MobiControl Remote menu, click **Tools**, then **Macro**, and click **Macro Test Manager**. It can also be accessed from the MobiControl Remote Control toolbar. Please see the "Macro Test Manager" topic on page 66.

Macro Test Manager

The Macro Test Manager tool allows the user to select a macro, and then view the results from the various test runs of that macro. This tool can be used to go through past test runs and review unexpected differences that occurred during previous testing runs.

You can access this dialog box either by clicking on the icon in the MobiControl Remote macro toolbar or by clicking **Tools**, then **Macro**, then **Macro Test Manager** from the MobiControl Remote menu.



Macro Test Manager dialog box

The **Macro Name** drop-down menu contains all macros that were recorded with the macro testing feature enabled. The list of all available test run results for a certain macro can be listed by selecting the macro name in the **Macro Name** box.

The test run name is created based on the date and time the macro was run with testing enabled. This name can be changed by clicking the **Rename Test** button. Select any item in the list and click the **Test Details** button to view the test details. (Please see the "Macro Test Result" topic on page 64 for more information.) You can also delete the results of any unwanted test run by selecting the item and clicking the **Delete** button.

The test run results can be exported to a text file by clicking the **Export Test** button. Please see the "Macro Test Result" topic on page 64 for details about exporting the test run results.

Macro Test Result Details

The **Macro Test Result Details** window shows the differences between each screen that was saved while recording a macro and the screen that was displayed during playback of the macro.

To alternate between the two screens, click the **Recorded** button and the **Played** button. To show the screen that was captured during macro play click on the **Played** button. To show the screen captured during macro recording use the **Recorded** button. By selecting **Show region mask** you can view what areas of the screen were not considered for comparing the two screens. The smallest rectangle of the screen, where differences were detected, is framed by a dotted line.

You can navigate through the sequence of screens by using the navigation buttons at the top right hand side of the dialog box. The first and last buttons take you to the first and last screens in this sequence. The middle two buttons take you to the previous screen and the next screen respectively. They each have tool tips to inform you what each button does if you have any difficulties. Between the buttons, a display gives the number of the screen you are currently viewing.

Help Menu

The menu contains the following selections:

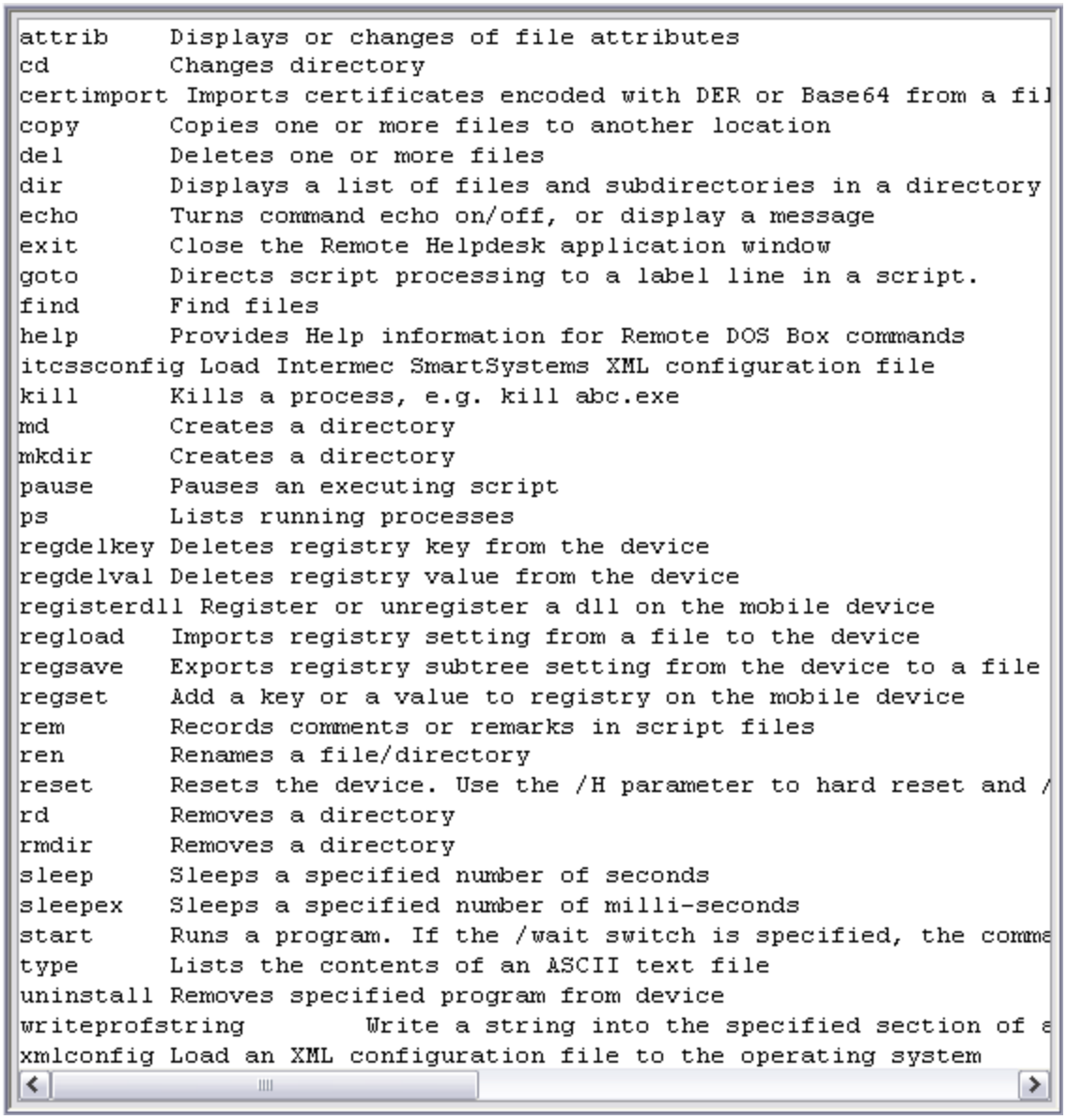
- The **Help Topics** menu item allows the user to access MobiControl Remote help.
- The **About MobiControl Remote** menu item displays version, registration and company information.

Remote DOS Box Tool

The remote DOS box allows users to open a DOS box into a remote mobile device and execute DOS-style commands. The DOS box additionally allows scripts (i.e. `.cmd` files) to be executed from within it or directly from the MobiControl Remote command line. Please see the "Script Command Set" topic on page 72.

NOTES:

- Use the notation `1:` to refer to the mobile device file system (similar to the `C:` notation).
- Executing scripts can be terminated by using the CTRL-BREAK keyboard sequence.



Remote DOS box screen

Script Command Set

Command Reference

The following is a list of commands currently supported on the following Operating Systems:

Windows Mobile and Desktop

Android

Android+

NOTE:

All scripts will be terminated within 5 minutes. This is an expected behavior of the application to ensure the script engine is not hung indefinitely.

Environment Variables

In general, an environment variable's name and value can be any ASCII character string; however, certain strings are reserved or have special meanings. (See below.) You refer to the value of an environment variable by enclosing it in "`%`" characters. You can use these expressions with any of the above commands in place of a literal value.

EXAMPLE:

The command "`showmessagebox %myVar%`" would display a message box containing the value of the variable `myVar`.

Composition

You can compose the values of environment variables.

EXAMPLE:

The two commands "`set var1=Hello`" and "`set var2=%var1% world!`" give `var2` the value "Hello world!"

Substring

You can pull parts of information from a string and put them as a variable.

EXAMPLE:

```
set Var1=Substring "Hi Hello World Goodbye" 4 11
 Showmessagebox "%Var1%"
```

would show "Hello World" on the device screen.

Errorlevel

The system reserved variable `errorlevel` always has an integral value. You can assign integer values to this variable, but you cannot delete it.

EXAMPLE:

```
set errorlevel=9.
```

Variable Initialisation Using System Information

A number of special strings allow you to extract information from the device and store it in an environment variable. You can extract this information from the following five sources:

- **Text file:** To extract a line from a text file, use a string of the form `TXT://\<filename>?LN=<line number>.`

  EXAMPLE:

  The command "`set myVar=TXT://policy.txt?LN=5`" stores line 5 of the file `policy.txt` in the variable `myVar`.

- **System registry:** To extract a value from the registry, use a string of the form "`REG://<key>?VN=<value name>`."

  EXAMPLE:

  ```
  set myVar=REG://HKEY_LOCAL_MACHINE\Windows CE Tools?VN=Platform
  ```

- **`.Ini` file:** To extract a value from a `.ini` file, use a string of the form "`INI://\<filename>?SC=<section>&NM=<name>`."

  EXAMPLE:

  ```
  set myVar=INI://settings.ini?SC=Config&NM=PreferredOption
  ```

- **Exit code:** You can store the exit code of an executable program, but this does not work on the Windows CE and Pocket PC platforms. Use a string of the form "`EXE://<command line>`."

  EXAMPLE:

  The command "`set myVar=EXE://scansystem /o`" runs the command "`scansystem /o`" and stores its return code in `myVar`.

- **STDOUT:** You can store the first line of output from an executable program (only supported on Windows 2000/XP platform). Use a string of the form "`STDOUT://<command line>`."

  EXAMPLE:

  The command "`set myVar=STDOUT://checkmessages`" runs the command "`checkmessages`" and stores the first line of its output in `myVar`.

Windows Mobile and Desktop Script Commands

Command	Description	Example(s)
`@`	Prefix any command by this character to stop the command from being displayed when executing commands in a script file.	To hide the output from the dir command: `@dir`
`abortpkg`	Aborts the installation of a package and forces it to show up as "Failed" in the MobiControl Manager, when used in a MobiControl Pre-Install script. Please see the "MobiControl Package Studio" topic on page 413 for more details.	
`abortsync`	Aborts the file synchronization process, when used in a MobiControl Pre-Sync script. Please see the "File Sync Rule"	To abort file synchronization if the first octet of the device's IP address is 169 (i.e. the IP is of the form `169.254.0.1`): `set firstoctet=ipoctet %IP% 1`

Command	Description	Example(s)
	topic on page 344 for more details.	`if %firstoctet%==169 abortsync`
`attrib`	Displays or changes file attributes. Syntax: `attrib [+R | -R] [+A | -A] [+S | -S] [+H | -H] [drive:][path] [filename]` "**+**" sets an attribute. "**-**" clears an attribute. "**R**" is the read-only file attribute. "**A**" is the archive file attribute. "**S**" is the system file attribute. "**H**" is the hidden file attribute.	attrib +A 1:\database_info.txt
`cd`	Changes the current directory.	To change to Windows directory: `cd Windows`
`certimport`	Imports a user-specified certificate of X.509 type, which could be either DER or Base64 encoded. Syntax: `certimport -cert "<filepath>" -stype "<storagetype>" -storage "<storage>"` "**<filepath>**" is the relative or absolute path of the certificate (`.cer`) file to import. "**<storagetype>**" is the type of storage into which to import the certificate. Not all OSs support all available options: • "**CSSCS**" is the current system service certificate storage. • "**CSSCU**" is the current user certificate storage. • "**CSSCUGP**" is the current user group policy certificate storage. • "**CSSLM**" is the local machine certificate storage.	• To import a certificate `test.cer` into current user storage of "`MY`" type: `certimport -cert "test.cer"` • To import a certificate `test.cer` into root user storage of the local machine: `certimport -cert "test.cer" -storagetype "CSSLM" -storage "ROOT"`

Command	Description	Example(s)
	• "**CSSLME**" is the local machine enterprise certificate storage. • "**CSSLMGP**" is the local machine group policy certificate storage. • "**CSSS**" is the system services certificate storage. • "**CSSU**" is the user's certificate storage. "**<storage>**" specifies storage into which to import the certificate. Available options are not supported by all OSs: • "**MY**" is the personal user certificate storage. • "**ROOT**" is the root certificate storage. • "**CA**" is the certificate authority certificate storage. • "**Trust**" is the trusted certificate storage. • "**SPC**" is the software publisher certificate storage.	
`cls`	Clears the screen.	
`copy`	Copies one or more files to another location. Syntax: `copy <source> <destination>` Files can be copied between the desktop computer and mobile devices.	To copy files with the extension `.txt` from the `c:\temp` to the `temp` directory on the mobile device: `copy c:\temp\*.txt 1:\temp`
`del`	Deletes one or more files. Syntax: `del <names>`	To delete all files with the extension `.tmp` in the current directory: `del *.tmp`
`dir`	Displays a list of files and subdirectories in a directory. Syntax: `dir [drive:][path] [filename]`	To list the files in Temp directory of the mobile device enter the following command. (The mobile device file system is denoted by `1:`.) `dir 1:\Temp\`
`echo`	Displays messages, or turns command-echoing on or off.	• To turn command echoing off: `echo off`

Command	Description	Example(s)

		• To turn command echoing on:
		`echo on`
		• To display the message "Copying Files ...":
		`echo Copying Files ...`

`exit`	Close the remote help desk application window	
`find`	Syntax: `find [/s] [filename]` "**`/s`**" is to search files in subfolders. "**`filename`**" is the file specification for which you are searching.	To search for all files with a `.txt` file extension including subfolders: `find /s *.txt`

`finishpkg`	Finishes the current script without processing the rest of the package and reports package installation as successful to the Deployment Server. This is useful particularly in packages that involve wiping a device. This script command can be used to skip reinstalling the package but still report back as successfully installed to the deployment server.
	When a hard reset is initiated from a package's post-install script, the entire package will re-install after the reset. A check can be included in the pre-install script that determines whether the package's files have already been installed.
	NOTES:
	• This command is of no consequence as a script command but only useful in the event of a package that involves cold boot.
		If a package's post-install script contains:
		`md "1:\PersistantStorage\subfolder"`
		`reset /w`
		Then the pre-install script could contain a check to prevent the package from being re-installed endlessly:
		`if exist "1:\PersistantStorage\subfolder" finishpkg`

`goto`	Directs script execution to a labelled line in a script. This	To go to label ":end": `copy *.* 1:\tmp`

Command	Description	Example(s)
	command is only for use in scripts.	goto end ... :end
help or ?	Displays a list of the commands supported and a brief description of each command.	
if	If errorlevel is greater than or equal to <number> (or less than <number> if "not" is present), then execute <command>: if [not] errorlevel <number> <command> If two operands are identical (not identical if "not" is present) execute <command>. The operand can be a string constant or environment variable: if [not] (<string> | %<environment variable>%) == (<string> | %<environment variable>%) <command> If a file or folder exists (does not exist, if "not" is present) execute <command>. If directory information is specified in the <file/folder name> then search in the directory, otherwise search in current directory. Use 1:\ to specify device root folder: if [not] exist <file/folder name> <command> If <processname.extension> is found running in the memory of the device, then execute <command>. If [not] is specified and the <processname.extension> is not found running in memory, execute <command>: if [not] procexists <Processname.extensio	• if errorlevel 0 echo "errorlevel is greater/equal to 0" • if abc==%xyz% echo "value of environment variable xyz is equal to abc" • If a variable contains white space, then the string must be within "". if "%name%==John Smith" echo "This is John Smith" • if exist "1:\IPSM\abc.cab" echo "1:\IPSM\abc.cab exists" • if procexists filesys.exe echo yes • if errorlevel 0 if not errorlevel 1 echo "errorlevel is 0"

Command	Description	Example(s)
	n> <command> **NOTES:** • <environment variable> and <string> can be any ASCII char string. • <command> can be any script command including the if command, which means the if command can be nested.	
ipoctet	Returns the specified octet of an IP address and saves it to an environment variable, when called from within a MobiControl device script. Syntax: ipoctet <IP Address> <Octet number> Please see the Environment Variables section below for more information.	• To save the value of the 4th octet of an IP address to the environment variable myOctet: set myOctet=ipoctet 192.168.1.225 4 This gives myOctet the value 225. • To save the value of the 1st octet of the device's IP address to an environment variable in a device script: set myOctet=ipoctet %IP% 1 This gives myOctet the value 192 if the IP address is of the form 192.XXX.XXX.XXX.
itcssconfig	Load the specified XML configuration file to the operating system. This command is applicable only for Intermec devices with Intermec SmartSystems. The complete path for the XML file must be provided. Syntax: itcssconfig <xmlfile.xml> This command will take the supplied XML file containing the SmartSystems request and in return, create an output file in the same directory with inserting *.out.* before the extension. The command passes the XML files to SmartSystems API without modification, so it	• itcssconfig 1:\FullPath\itcss.xml Response: itcss.out.xml • XML script that enables "Code 39" decoding in all devices in the Scanners group: <Subsystem Name="Data Collection"> <Group Name="Scanners" Instance="0"> <Group Name="Symbologies"> <Group Name="Code 39"> <Field Name="Enable Code 39">1</Field> </Group> </Group> </Group> </Subsystem>

Command	Description	Example(s)
	will accept any valid request (either "Get" or "Set"). It's possible to use XML files generated with SmartSystems Console. Please see the "Intermec SmartSystems Settings: Advanced XML Scripting" topic on page 376 for more information.	
`kill`	Terminate a process that is currently running on the mobile device. Syntax: `kill <executable filename>`	To terminate the `pword.exe` process on the mobile device: `kill pword.exe`

`log`	Send a custom message back to MobiControl Deployment Server from the mobile device. This message will show up in the LOG panel of the mobile device in the Devices View (tab) in MobiControl Manager.
	Syntax:
	`log <type> <message>`
	"**`log`**" is the command.
	"**`<type>`**" is the type of message that should get associated. The options are:
	• Error (`-e`)
	• Warning (`-w`)
	• Information (`-i`)
	"**`<message>`**" is the message that will be displayed in the device log in MobiControl Manager.
		During a software push from MobiControl to your mobile device, you can use this command to send notification to MobiControl Manager at certain intervals during the software push:
		`*** Command in the Pre-Install Script ***`
		`log -i "Starting Software Push"`

`mkdir` or `md`	Creates a directory.
	Syntax:
	`mkdir [drive:] < path>`
		• To create a directory called "test" from the current directory:
		`md test`
		• To create "test\test1\test2\test3" recursively:
		`md test \test1 \test2 \test3`

`move`	This command moves a file from source specified to destination specified. You can also rename the file being moved by	• To move a file `test.bat`:
		`move test.bat 2:\`
		`move test.bat 2:\test.bat`

Command	Description	Example(s)
	specifying a different name for the destination filename. Syntax: `move [source file path]<filename> <destination file path>[filename]`	• To move and rename a file at the same time: `move 1:\test.bat 2:\test2.cmd`

`pause`	Prompts and waits for user input to continue. This command is only for use in scripts or .CMD files.
	Syntax:
	`pause`
		Example:
		`pause`
		Display:
		`Press any key to continue...`

`ps`	List the running processes on the mobile device.	
`regdelkey`	Delete a key from registry on the mobile device. Syntax: `regdelkey <registry key>`	To delete registry key `HKEY_CLASSES_ROOT\.2bp`: `regdelkey HKEY_CLASSES_ROOT\.2bp`
`regdelval`	Delete a value from registry on the mobile device. Syntax: `regdelval <registry key>\<value name>`	To delete registry value `HKEY_CURRENT_USER\Start\test`: `regdelval HKEY_CURRENT_USER\Start\test`

`registerdll`	Register or unregister a DLL on the mobile device.
	To register a DLL:
	`registerdll <dll filename>`
	To unregister a DLL:
	`registerdll -u <dll filename>`
		Register Example:
		`registerdll MCSetup.dll`
		Unregister Example:
		`registerdll -u MCSetup.dll`

`regload`	Import a registration file to registry on the mobile device. Syntax: `regload <registry file path>`	To import registration file `c:\test.reg` to the mobile device's registry: `regload c:\test.reg`
`regsave`	Export the mobile device registry subtree to a file. Syntax: `regsave [-A | -U] [drive:][path] filename subtree [regpath]`	To export the `HKEY_LOCAL_MACHINE` subtree from the mobile device registry to a UNICODE file `C:\hklm.reg`: `regsave -U C:\hklm.reg HKEY_LOCAL_MACHINE`

Command	Description	Example(s)
	"**-A**" is for ANSI format of output file. "**-U**" is for UNICODE format of output file (default). "**[drive:][path] filename**" is a file to where registry subtree will be saved. "**subtree[regpath]**" specifies what part of device's registry will be exported. Possible values are: • "*****" for everything (no 'regpath') • "**HKLM**" for HKEY_LOCAL_MACHINE • "**HKCU**" for HKEY_CURRENT_USER • **HKCR** for HKEY_CLASSES_ROOT	

`regset`	Add a key or a value to registry on the mobile device.
	Syntax:
	`regset <registry key> [value name] [data]`
		To add a new key and two values to that key:
		`regset HKLM\software\apps testkey`
		`regset HKLM\software\apps\testkey testvalue1 abc`
		`regset HKLM \software \apps \testkey testvalue2 dword:123`

`rem`	The `rem` command is used to insert a comment line in a script/batch file.	
`rename` or `ren`	Renames a file or folder. Syntax: `rename <source filename> <destination filename>`	To rename the file `test.txt` to `test.bak`: `ren test.txt test.bak`
`replacetxt`	This command allows to change all occurrences of a particular character or string in the specified file. Syntax: `replacetxt <filename> <string to replace> <new string>`	Example: `replacetxt "\Temp\My Device.txt" Device Psion`

Command	Description	Example(s)
`reset`	This command performs a Soft or Hard reset of the device. Syntax: `reset [/S(Default)| /H | /W]` • `reset /S (Default)`: To soft reset the device and also close the desktop remote control session if the device is being remote controlled. • `reset /H`: To hard reset a device running Windows Pocket PC or Windows CE platforms. This command will result in clearing data stored in volatile memory. On Windows Mobile 5.0 and later devices this is equivalent to a soft reset. The real-time clock may also reset depending on the device make and model. • `reset /W`: To perform the secure deletion of data stored on the device as well as a reset to factory default settings. Please note that the wipe command is only supported on the Windows Mobile 5 operating system with AKU2 or later and newer versions of Windows Mobile.	• To soft reset a device: `reset` **NOTE:** The `reset /H or /W` command will perform a system reboot similar to restart on Windows Desktop Agent.
`resetpassword`	Reset device password to new password Syntax: `resetpassword <new password>`	To reset the user password on the device to "1234": `resetpassword 1234`

`rmdir` or `rd`	Removes (deletes) a directory.
	Syntax:
	`rmdir [/S] path`
		• To remove an empty directory called "Test" from the current directory:
		`rmdir test`
		• To remove a directory called "Test" and all of its contents:
		`rmdir /S test`

`sendsms`	This script command can be used to send an outbound SMS (text message) from any online or ActiveSynced mobile device to 1 or more devices. Syntax:	• To send an SMS message to 1 number: `sendsms 416-555-0505 "This is a test message"`

Command	Description	Example(s)
	`sendsms [recipient (s)] "[message]"` Separate recipient phone numbers with a semi-colon ";".	• To send an SMS message to multiple numbers: `sendsms 416-555-0505;905-555-5050;919-555-5500 "This is a test message"` **NOTE:** The device receiving the SMS *MUST* have MobiControl installed in order for the command to complete successfully.
`set`	Set, edit or show values of environment variables. Syntax: "`set`" lists all environment variables. "`set <environment variable>`" shows the value of `<environment variable>` "`set <environment variable>=`" deletes `<environment variable>` "`set <environment variable>=<string>`" sets the value of `<environment variable>` to `<string>` "`set <environment variable>=substring "<string>" <startpos> [noofchars]`" sets the value of `<environment variable>` to the string returned by the substring command. (The substring command returns part of the string based on starting position and number of characters specified.) "`set <environment variable>++`" increments the value of `<environment variable>`. The variable must have an integer value. "`set <environment variable>--`" decrements	• Set Var1=test will set the value of variable Var1 to "test" • Set Var2=substring "testing" 1 4 will set the value of variable Var2 to "test"

Command	Description	Example(s)
	the value of `<environment variable>`. The variable must have an integer value.	

setdate	Sets the date, and time:
	
	Syntax:
	`setdate <date> [time]`
	Usage:
	`setdate <mm-dd-yyyy> [HH:MM:SS]`
		To set the date and time of the device:
		
		`setdate 08-20-2009 13:32:00`

`shellexecute`	Launches the registered application for the given file extension.
	Syntax:
	`shellexecute <filepath> <-verb> [-w<seconds>]`
		To launch the registered application for the given file extension:
		
		`shellexecute 1:\temp\temp.upg -open`
		
		`shellexecute 1:\temp\temp.upg -run -w5`

`showmessagebox`	Shows a message box on the device screen. Syntax: `showmessagebox <message> [timeout] [type] [default button]` "**`<message>`**" is the message shown in the message box. Use quotation marks if there are spaces in the message. "**`[timeout]`**" is the number of seconds until the message box is closed automatically. If `[timeout]` or if the keyword `NO_TIMER` is not present, the message box will be shown until user dismisses it. For `MB_OK` and `MB_ICONERROR` message box types, timeout is optional. "**`[type]`**" is the message box type (optional): • "**`MB_OK`**" is for an information window with an **OK** button. • "**`MB_YESNO`**" is for a question window with **Yes** (default) and **No** buttons	• `showmessagebox "This is a test message"` • `showmessagebox "Your device's IP address is %IP%"` • `showmessagebox "This is a test message with a 3 second timeout" 3` • `showmessagebox "This is a test message with Yes/No button and no timeout" NO_TIMER MB_YESNO` • `showmessagebox "Abort the operation?" NO_TIMER MB_ICONQUESTION YES if % ShowMessageBoxReturn %== IDYES goto Exit`

Command	Description	Example(s)
	• "**MB_ICONEXCLAMATION**" is for a warning window with an **OK** button • "**MB_ICONQUESTION**" is for a question window with **OK** (default) and **Cancel** buttons • "**MB_ICONERROR**" is for an error window with an **OK** button "**[default button]**" (Optional) is for use with the keywords YES and NO to set the default button for MB_YESNO and MB_ICONQUESTION. In the case of MC_ICONQUESTION, YES is **OK** and NO is **Cancel.** The return values for showmessagebox are stored in a global variable ShowMessageBoxReturn. This variable can be used in scripts as %ShowMessageBoxReturn% to execute actions based on user interaction. Possible return values are IDYES, IDNO, IDOK, IDCANCEL. The value for this global variable does not change if the type is not MB_YESNO or MB_ICONQUESTION.	
sleep	Sleep for a specified number of seconds. This command is only for use in scripts.	Example: sleep 5
sleepex	Sleep for a specified number of milliseconds. This command is only for use in scripts.	To sleep for 3.5 seconds: sleepex 3500
smsreportpn	Sends a hidden encoded SMS message to a device to store it's current phone number in the registry. Some SIM cards are not provisioned by the cellular carrier with their phone number post purchase. This prevents MobiControl from obtaining the devices phone number from the standard API calls used.	The following command needs to be issued via MobiControl from a device that has SMS service. The phone number in the command is the phone number of the device in question. To set a device's phone number's information: smsreportpn 9675555555

Command	Description	Example(s)
	The smsreportpn command has been provided to acquire the devices current phone number via an SMS message exchange with another device running the MobiControl agent. Upon completion of the message exchange the phone number is set in the following registry section: "HKLM\Software\Apps\SOTI\" with the key name of "PhoneNumber" The registry key value will be set on the target device. Syntax: `smsreportpn <phone number>`	**NOTE:** There will be a total of two SMS messages, one from each device (The originating and target devices).
`start`	Start a program on the mobile device. When the "`/wait`" option is specified, the script processor waits for the started program to terminate before executing the next command in the script.	To start Pocket Word and wait until it is terminated: `start /wait pword`
`type`	Display the contents of an ASCII text file.	To display the contents of the file `test.cmd`: `type test.cmd`
`uninstall`	Removes the specified program from the device. This is equivalent to uninstalling a program by using the 'Remove Programs' applet in the device's control panel. Syntax: `uninstall [/w] [program]` "**`/w`**" is to wait for the uninstallation to complete before proceeding in a script. "**`program`**" is for the program to be removed. The program name must be the complete name consisting of the application provider and the application name. This is the name that appears in the	To remove the program 1-Calc: `uninstall 1-Calc`

Command	Description	Example(s)
	Remove Programs applet in the device's control panel.	
`writeprofstring`	Write a string into the specified section of an initialization file. Syntax: `writeprofstring <filename> <section> [key] [value]` "**`filename`**" is the name of the `.ini` file. "**`section`**" is the name of the section in the `.ini` file to which the value is to be written. If the section does not exist, it is created. The name of the section is case-sensitive. "**`key`**" is the name of the key. If the key does not exist in the specified section, it is created. If this parameter is not entered, the entire section, including all entries within it, is deleted. "**`value`**" is the string to be written to the file. If this parameter is not entered, the key is deleted. Use quotes if the key or the value contain white space.	To set the Color key in the "Video" section of the `\Movie\mov.ini` file to a value of "Red": `writeprofstring \Movie\mov.ini Video Color Red`
`xmlconfig`	Load the specified XML configuration file to the operating system. Syntax: `xmlconfig <xmlfile.xml>` This command will take the supplied XML file and load it onto the operating system. This command is only valid on devices running Pocket PC 2003 or later. The XML file is handled by Microsoft's configuration manager. Use of this command will allow you to script in complicated device configuration schemas for easy deployment. Please see the "Advanced XML Setup Script" topic on page 370 for more details.	`xmlconfig 1:\FullPath\xmlfile.xml` **NOTE:** The complete path for the XML file must be provided.

Command	Description	Example(s)
`1:`	Select the drive/file system. The mobile device file system is denoted by `1:`.	To switch to the `c:` drive on your desktop computer: `c:`

To run a program on the mobile device or to execute a script file.	Enter the name of a program or command file followed by any command line arguments.
	All script files must have the `.cmd` file extension.
		• To get Pocket Word to open the document `notes.doc`:
		`pword notes.doc`
		• To run a script file called "`test.cmd`":
		`test.cmd`

Android Script Commands

Command	Description	Example(s)
`connect`	Tells the MobiControl Device Agent to try to come online. Syntax: `Connect`	To Tell the device to come online: `Connect`
`del`	Deletes one or more files. Syntax: `del <names>`	To delete all files with the extension `.tmp` in the current directory: `del *.tmp`
`devrename`	Change device name Syntax: `devrename <New  Name>`	To change the devices name: `devrename "New Device Name"`

`foreground mode`	Switches the MobiControl service between foreground and background modes. While running in the foreground mode, the MobiControl process will not be killed by the system.
	While in foreground mode, a MobiControl icon will be displayed in the notification area.
	Syntax:
	`foregroundmode enable|disable`
		To switch to foreground mode:
		`foregroundmode enable`
		To switch back to normal mode:
		`foregroundmode disable`

`install`	Install an Android .APK file. User will be prompted to allow install. Syntax: `Install <Path> <Android.APK>`	Install a new Android Application. User must agree to install. `Install "\sdcard\AndroidApp.APK"`

`log`	Send a custom message back to MobiControl Deployment Server from the mobile device. This message will show up in the LOG panel of the mobile device in the Devices View (tab) in MobiControl Manager.
	Syntax:
	`log <type> <message>`
	"**`log`**" is the command.
	"**`<type>`**" is the type of message that should get associated. The options are:
	• Error (`-e`)
	• Warning (`-w`)
	• Information (`-i`)
	"**`<message>`**" is the message that will be displayed in the device log in MobiControl Manager.
		During a software push from MobiControl to your mobile device, you can use this command to send notification to MobiControl Manager at certain intervals during the software push:
		`*** Command in the Pre-Install Script ***`
		`log -i "Starting Software Push"`

`lock`	Turn device screen off and if there is a password next time it asks for the password	To force the device to lock, and prompt for password (if there is one configured)

Command	Description	Example(s)
		`Lock`

`manualBlacklist`	Manually configure Application Run Control to Blacklist applications.
	Syntax:
	ManualBlacklist <type> <Bundle Identifier>
	"**<type>**" is the type of message that should get associated. The options are:
	• Add (`-add`)
	• Remove(`-remove`)
	• On(`-on`) - Turn the Blacklist on
	• Off(`-off`) - Turn the Blacklist Off
	• List(`-list`) -List the blocked applications in the Device Agent Log window.
	<Bundle Identifier>" is ID of the application. Example the Bundle ID for Google Maps is com.google.android.apps.maps.
		To turn on Application Run Control Blacklist and block Google Maps:
		`manualblacklist on`
		`manualblacklist add com.google.android.apps.maps`

`reset`	This command performs a Hard reset of the device. Syntax: `reset /W]` • `reset` : To perform a soft reset of the device. • `reset /W` : To perform the secure deletion of data stored on the device as well as a reset to factory default settings.	To reset a device: `reset /W`
`resetagent`	The command restarts the MobiControl device agent on the device. Syntax: `reset`	To restart the MobiControl device agent: `reset`
`resetpassword`	Completely remove the password from the device. Syntax: `resetpassword`	To remove the device password: `resetpassword`

`rmdir` or `rd`	Removes (deletes) a directory.
	Syntax:
	`rmdir [/S] path`
		• To remove an empty directory called "Test" from the current directory:
		`rmdir test`
		• To remove a directory called "Test" and all of its contents:
		`rmdir /S test`

Command	Description	Example(s)
showmessagebox	Shows a message box on the device screen. Syntax: showmessagebox <message> [timeout] "**<message>**" is the message shown in the message box. Use quotation marks if there are spaces in the message. "**[timeout]**" is the number of seconds until the message box is closed automatically. If [timeout] or if the keyword NO_TIMER is not present, the message box will be shown until user dismisses it.	• showmessagebox "This is a test message" • showmessagebox "This is a test message with a 3 second timeout"
start	Starts an application/activity. Syntax: start [activity|process] <Bundle Identifier> [activity|process] is the start mode of the application being launched. Process will start the main application, while activity will start a specific activity.	To start the email application: start process com.google.email To start the Account list activity inside the email application: start activity com.google.email/ com.google.email.AccountListActivity
Unlock	Turn device screen on and remove password screen	To unlock the device and dismiss the password lock screen: Unlock
Uninstall	Uninstall an Android .APK file. User will be prompted to allow uninstall. Syntax: Uninstall <Bundle Identifier>	Uninstall Google Maps. User must agree to uninstall. Uninstall com.google.android.apps.maps

Android+ Script Commands

Command	Description	Example(s)
Blockuninstall	Allows or Deny's the users ability to remove an application. Syntax: Blockuninstall <Bundle Identifier>	To block the uninstallation of the MobiControl Device Agent: Blockuninstall net.soti.mobicontrol
Connect	Tells the MobiControl Device Agent to try to come online. Syntax: Connect	To Tell the device to come online: Connect

Command	Description	Example(s)
`del`	Deletes one or more files. Syntax: `del <names>`	To delete all files with the extension `.tmp` in the current directory: `del *.tmp`
`devrename`	Change device name Syntax: `devrename <New Name>`	To change the devices name: `devrename "New Device Name"`

`foregroundmode`	Switches the MobiControl service between foreground and background modes. While running in the foreground mode, the MobiControl process will not be killed by the system.
	While in foreground mode, a MobiControl icon will be displayed in the notification area.
	Syntax:
	`foregroundmode enable|disable`
		To switch to foreground mode:
		`foregroundmode enable`
		To switch back to normal mode:
		`foregroundmode disable`

`Install`	Install an Android .APK file. Syntax: `Install <Path> <Android.APK>`	Install a new Android Application. `Install "sdcard\AndroidApp.APK"`
`installPackage`	Install a MobiControl Package built from the Package Studio. `Installpackage <Path> <PackageName.PCG>`	Installing a package from %tmp% folder. `Installpackage "%tmp%\PackageName.pcg"`
`lock`	Turn device screen off and if there is a password next time it asks for the password	To force the device to lock, and prompt for password (if there is one configured) `Lock`

`lockdownorientation`	Change the orientation of the device lockdown
	Syntax:
	`Lockdownorientation <orientation>`
		To make the lockdown show up as landscape:
		`Lockdownorientation landscape`
		To make the lockdown show up as portrait:
		`Lockdownorientation portrait`

`log`	Send a custom message back to MobiControl Deployment Server from	During a software push from MobiControl to your mobile device, you can use this command to send notification to MobiControl

Command	Description	Example(s)

	the mobile device. This message will show up in the LOG panel of the mobile device in the Devices View (tab) in MobiControl Manager.
	Syntax:
	`log <type> <message>`
	"**log**" is the command.
	"**<type>**" is the type of message that should get associated. The options are:
	• Error (`-e`)
	• Warning (`-w`)
	• Information (`-i`)
	"**<message>**" is the message that will be displayed in the device log in MobiControl Manager.
		Manager at certain intervals during the software push:
		`*** Command in the Pre-Install Script ***`
		`log -i "Starting Software Push"`

`manualBlacklist`	Manually configure Application Run Control to Blacklist applications.
	Syntax:
	ManualBlacklist <type> <Bundle Identifier>
	"**<type>**" is the type of message that should get associated. The options are:
	• Add (`-add`)
	• Remove(`-remove`)
	• On(`-on`) - Turn the Blacklist on
	• Off(`-off`) - Turn the Blacklist Off
	• List(`-list`) -List the blocked applications in the Device Agent Log window.
	<Bundle Identifier>" is ID of the application. Example the Bundle ID for Google Maps is
		To turn on Application Run Control Blacklist and block Google Maps:
		`manualblacklist on`
		`manualblacklist add com.google.android.apps.maps`

Command	Description	Example(s)
	com.google.android.apps.maps.	
`reset`	This command performs a Hard reset of the device. Syntax: •`reset]`: To soft reset the device and also close the desktop remote control session if the device is being remote controlled. • `reset /W`: To perform the secure deletion of data stored on the device as well as a reset to factory default settings. • `reset /E`: To perform the secure deletion of data stored on the devices internal and external storage	• To reset a device back to factory settings and wipe data: `reset /W`
`resetagent`	The command restarts the MobiControl device agent on the device. Syntax: `reset`	To restart the MobiControl device agent: `reset`
`resetpassword`	Completely remove the password from the device. Syntax: `resetpassword`	To remove the device password: `resetpassword`

`rmdir` or `rd`	Removes (deletes) a directory.
	Syntax:
	`rmdir [/S] <path>`
		• To remove an empty directory called "Test" from the current directory:
		`rmdir test`
		• To remove a directory called "Test" and all of its contents:
		`rmdir /S test`

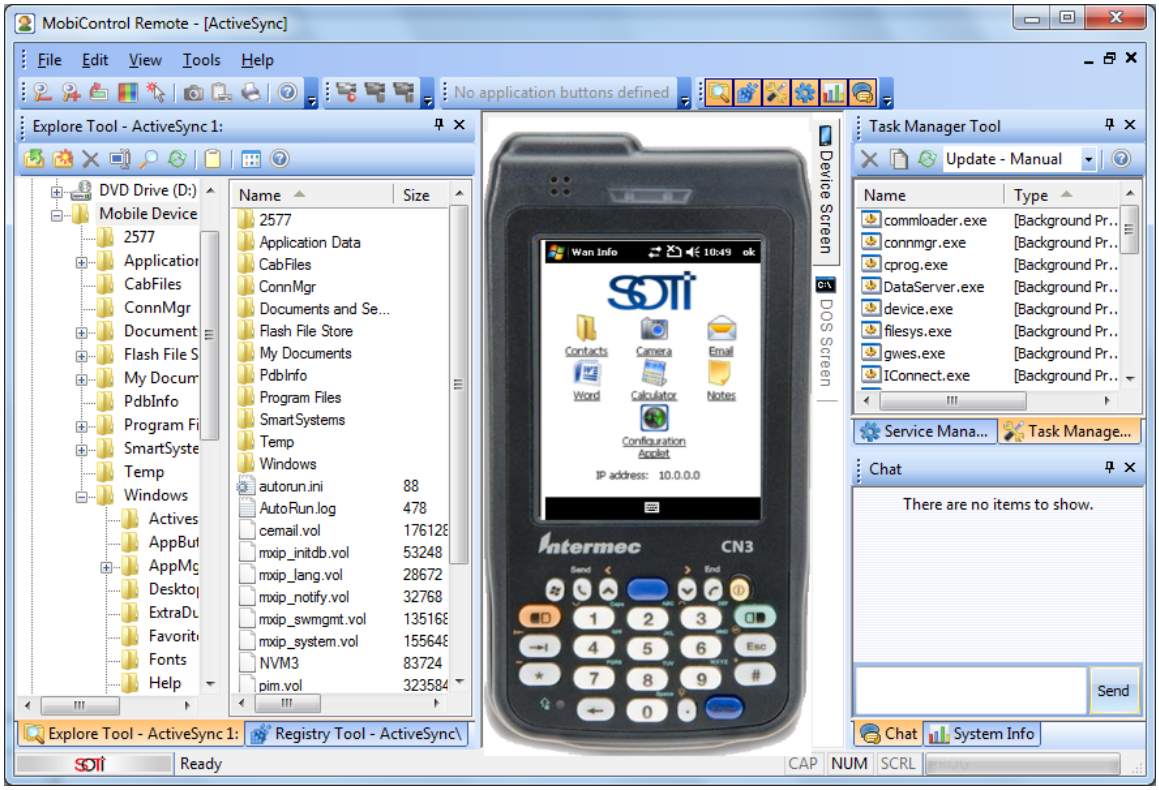
`setEncryption`	Configure file encryption for the mobile device. Syntax: `SetEncryption <I> <E>` "**`I`**" is the Internal Storage Card. To enable/disable encryption set to 1/0. "**`E`**" is the External Storage Card. To enable/disable	To enable encryption on the Internal Storage Card and disable encryption on the External Storage Card: `setencryption 1 0`

Command	Description	Example(s)
	encryption set to 1/0.	
showmessagebox	Shows a message box on the device screen. Syntax: showmessagebox <message> [timeout] "**<message>**" is the message shown in the message box. Use quotation marks if there are spaces in the message. "**[timeout]**" is the number of seconds until the message box is closed automatically. If [timeout] or if the keyword NO_TIMER is not present, the message box will be shown until user dismisses it.	• showmessagebox "This is a test message" • showmessagebox "This is a test message with a 3 second timeout" 3
start	Starts an application/activity. Syntax: start [activity|process] <Bundle Identifier> [activity|process] is the start mode of the application being launched. Process will start the main application, while activity will start a specific activity.	To start the email application: start process com.google.email To start the Account list activity inside the email application: start activity com.google.email/ com.google.email.AccountListActivity
unlock	Turn device screen on and remove password screen	To unlock the device and dismiss the password lock screen: Unlock
uninstall	Uninstall an Android .APK file. User will be prompted to allow uninstall. Syntax: uninstall <Bundle Identifier>	Uninstall Google Maps. User must agree to uninstall. uninstall com.google.android.apps.maps
wipeapplication	Wipe Application Data from Mobile Device for a specific application.	Wipe the Application data for a specific application: WipeApplications net.soti.mobicontrol

Command	Description	Example(s)
	`WipeApplication <Bundle Identifier>`	

Configuring Skins

A skin is an image of the body of your mobile device. MobiControl allows you to view your mobile device in a skin when you establish a remote control session to the device. The image below shows a remote control session to a device with a skin configured. You can download skins for your mobile devices by using the Skin Catalog tool in MobiControl Manager. (Please see the "Skin Catalog" topic on page 101.)



MobiControl remote control session using a skin for the mobile device

Accessing the Skin Catalog Tool

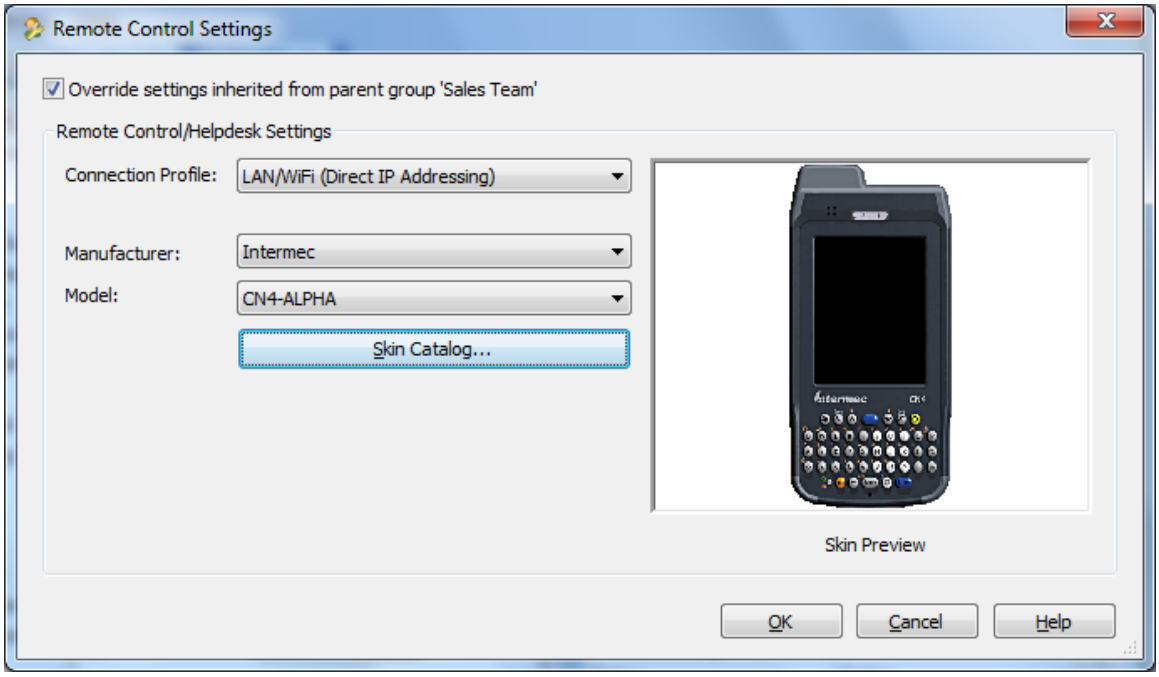
From MobiControl Manager, go to the Devices view (tab), right-click on a device in the device list, click **Configure Device**, and then click **Remote Control Settings** from the device options menu. You can also right-click the device group in the device tree to apply all the devices in the group to use the selected skin. In the Remote Control Settings dialog box, click on the **Skins Catalog** button. Your computer must have an Internet connection to download skins.

Configuring a Skin for a Device or Device Group

The following sequence of steps illustrates how to configure a skin for a device or device group:

1. Select a device or device group.

   From MobiControl Manager, go to the Devices view (tab), right-click on a device in the device list, select **Configure Devices**, then **Remote Control Settings** from the device options menu. You can also right-click the device group in the device tree to apply all the devices in the group to use the selected skin.

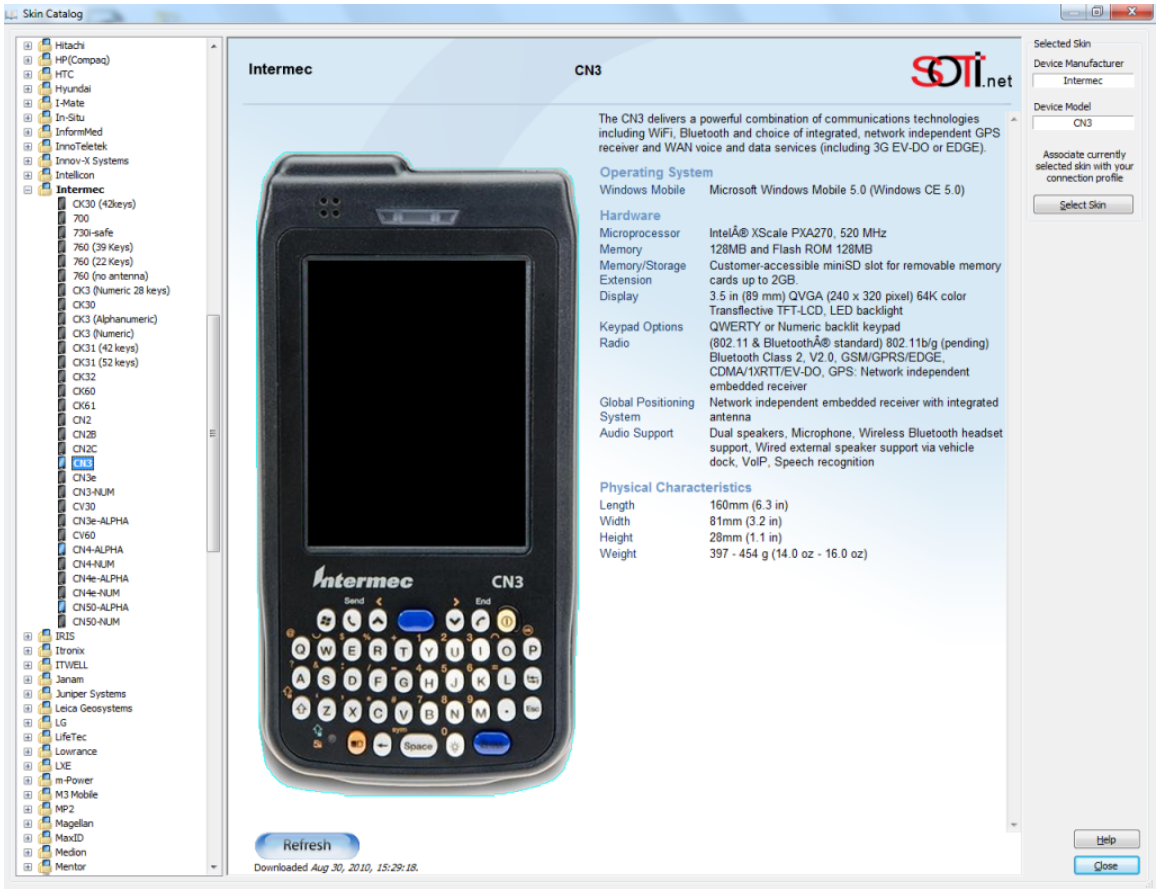


Remote Control Settings dialog box

2. Select or download a skin.

In the **Remote Control Settings** dialog box, select the manufacturer and model of your mobile device. If a skin for your device has already been installed it will immediately be displayed in the preview area. If a skin for your device is not available, click on the **Skin Catalog** button to download the skin. Skins for most Windows CE .Net, Pocket PC, and Smartphone devices are currently available. When you click the **Skin Catalog** button, the Skin Catalog tool window will open. Using the Skin Catalog, you can download and install a skin for your mobile device. If you cannot find a skin for your mobile device, please contact us.

When a skin is selected during a remote control session, the buttons on the skin are mapped to the buttons on the device. You can access the device's buttons remotely by clicking them.



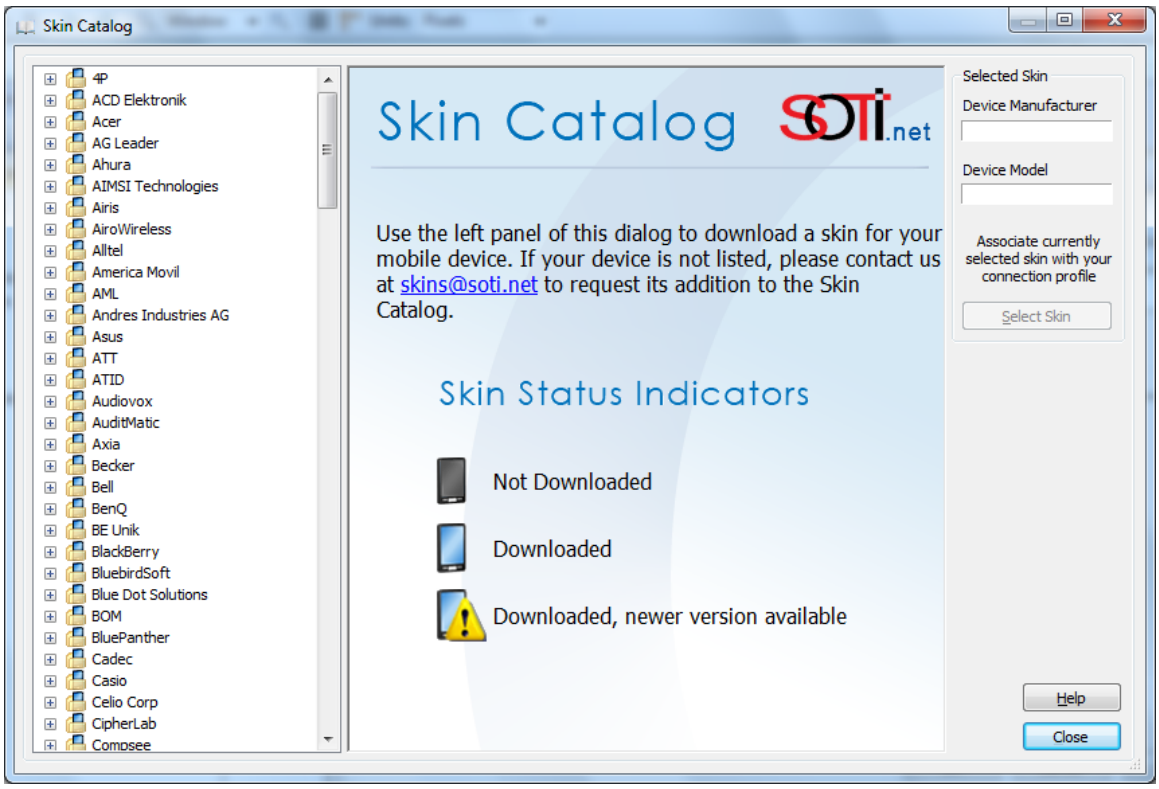
Mobile device skin selected within the MobiControl Skin Catalog

Skin Catalog

The skin catalog is a dynamic collection of mobile device skins that is updated regularly. You can access the latest skins over the Internet using the skin catalog. When you launch the skin catalog, it automatically connects to the Internet to download the latest skins from SOTI's website. If an Internet connection is not available, the skin catalog will be displayed in an offline mode, allowing you to browse only the skins that have been downloaded on your computer already.

You download the latest skin for a device or the latest content for a selected manufacturer or device by following these steps:

1. Select the device manufacturer or the device from the manufacturers pane on the left side.
2. Click the **Refresh** button to download the latest content for a selected manufacturer or device.
3. After the desired skin has been downloaded, click on that image and click **Select Skin** on the right side to select that skin.



MobiControl skin catalog

NOTES:

- If a skin for your mobile device is not available, you may request it—contact us.
- You are only entitled to download skins while the product is within its service period. If your service period has expired, contact us or your authorized reseller to renew.

Location Services

MobiControl's Location Services provides the ability to locate and track mobile devices that are equipped with a GPS receiver that is internal or external to the unit. In order to locate a device, the GPS must be enabled and correctly configured on your device. The GPS determines the current location based on its position relative to orbiting satellites. In order for this to happen, the device requires a clear view of the sky. Determining location may not be possible if the device is inside buildings or has an obstructed view of the sky.

MobiControl's GPS functionality will work with Windows Mobile, and Windows CE based mobile devices, as well as Windows based computers.

You can activate Location Services for a device in MobiControl by right- clicking on a device and selecting the **Location Services** option from the menu. The first time you select an option from the Location Services menu for a device, it will automatically use the next available license. If there are no more licenses available, you will be notified to contact SOTI for information on acquiring additional licenses for Location Services.

Please See the "Contact Us" page to contact us for more details on acquiring additional licensing.

NOTES:

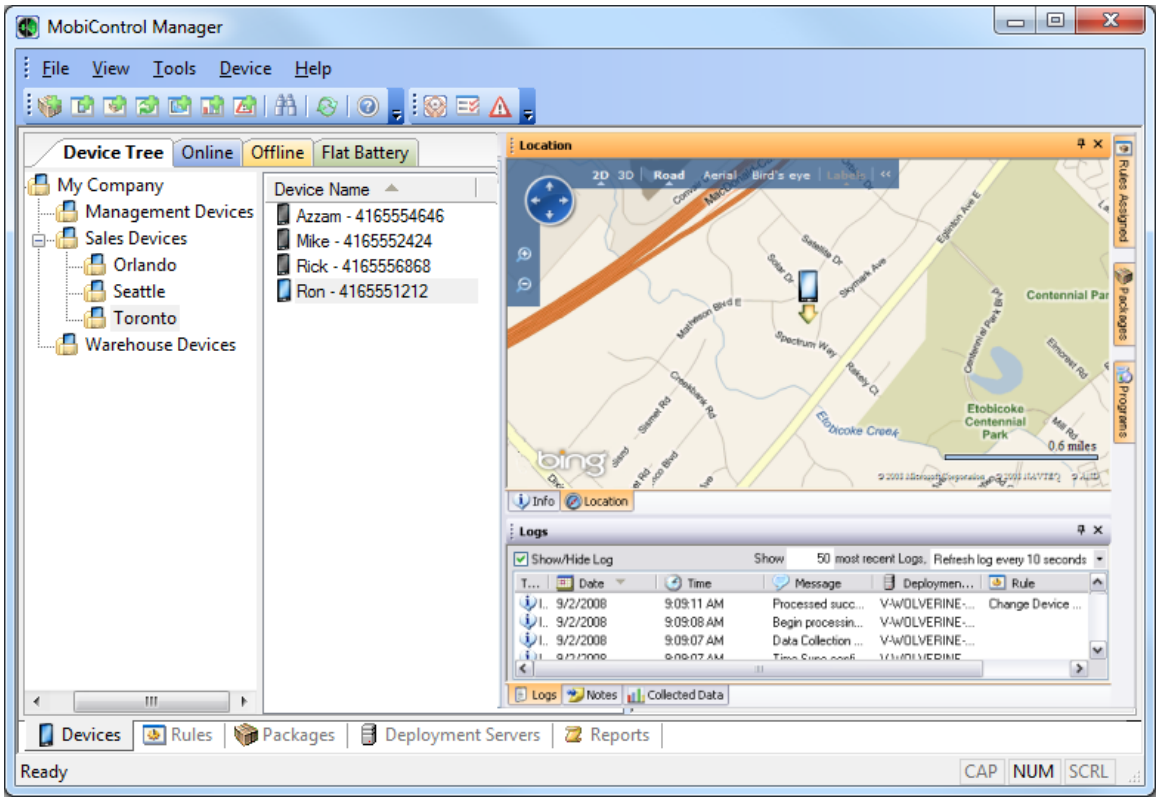
- When using Location Services in MobiControl to track devices, Internet Explorer 7 or higher is required.
- The Current Format for Regional and Language Options on your PC MUST be compatible with Bing Maps. Click here for a list of supported Bing Map control settings.

Using the Locate Feature

To use the Locate feature in MobiControl's Location Services, right-click on the device you wish to locate, select **Location Services,** and click **Locate.**

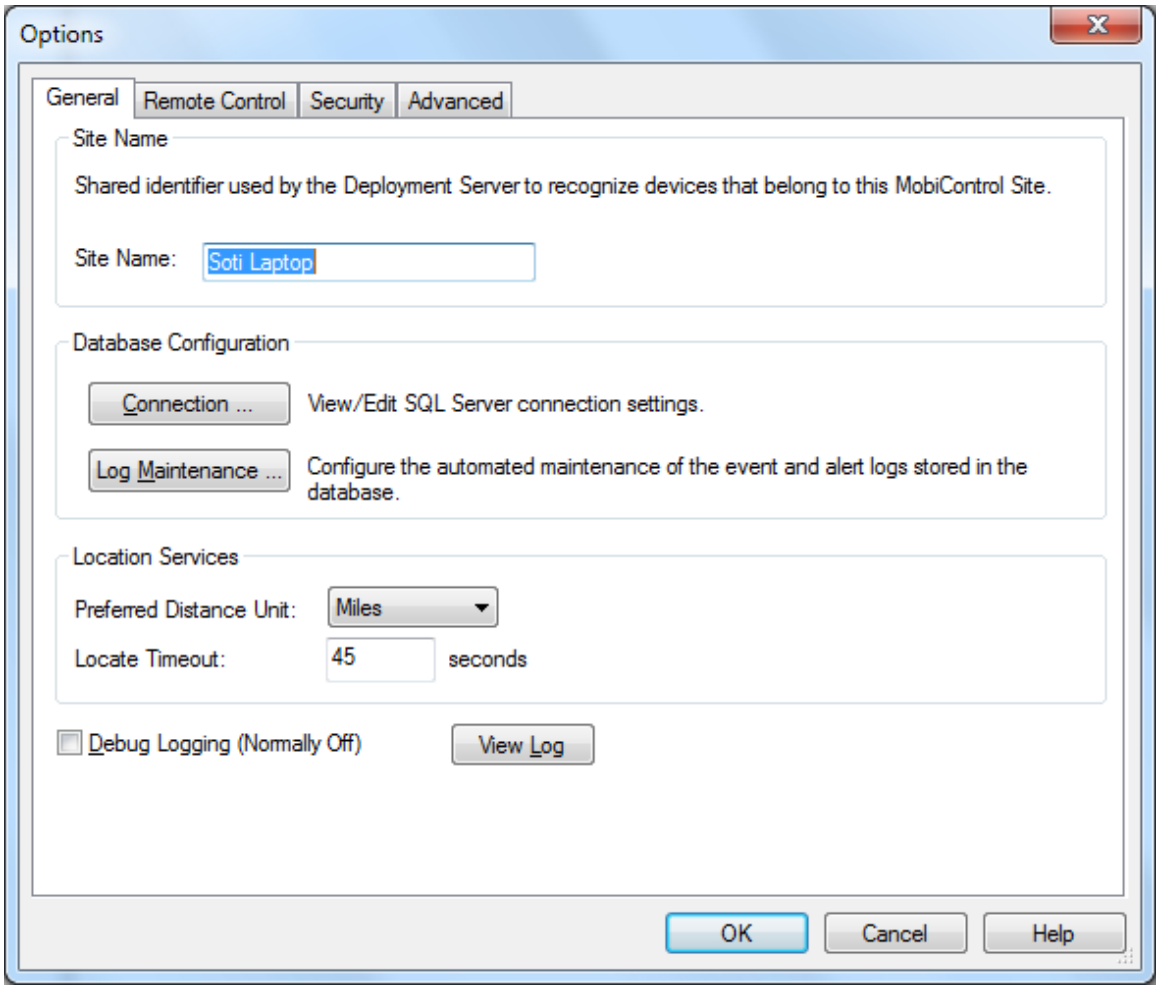
The locate feature will use the GPS unit associated with your mobile device to determine the current latitude and longitude of the device. These coordinates are returned to MobiControl and displayed in the Location panel using Microsoft's Virtual Earth. The coordinates plotted in the Location panel represent the exact position of the device at the time of the request. To follow the position of the device in real time, use the **Track** option under the **Location Services** menu.

You can locate the position of multiple devices at once: select the parent folder or hold the CTRL key and select all the devices you wish to locate, right-click, select **Location Services,** and click on **Locate.** In order to use the Locate feature, the device(s) must be online and communicating with the MobiControl Deployment Server. The status of the current (and completed) Locate and Track commands is displayed in the lower left hand corner of the screen.



Location Services locate user interface

The amount of time allotted to the GPS radio to acquire a fix can be adjusted from the ***Tools > Options*** menu. You also have the ability to change the unit in which distance is measured from this menu. For more information about the options available in this window, please click here.



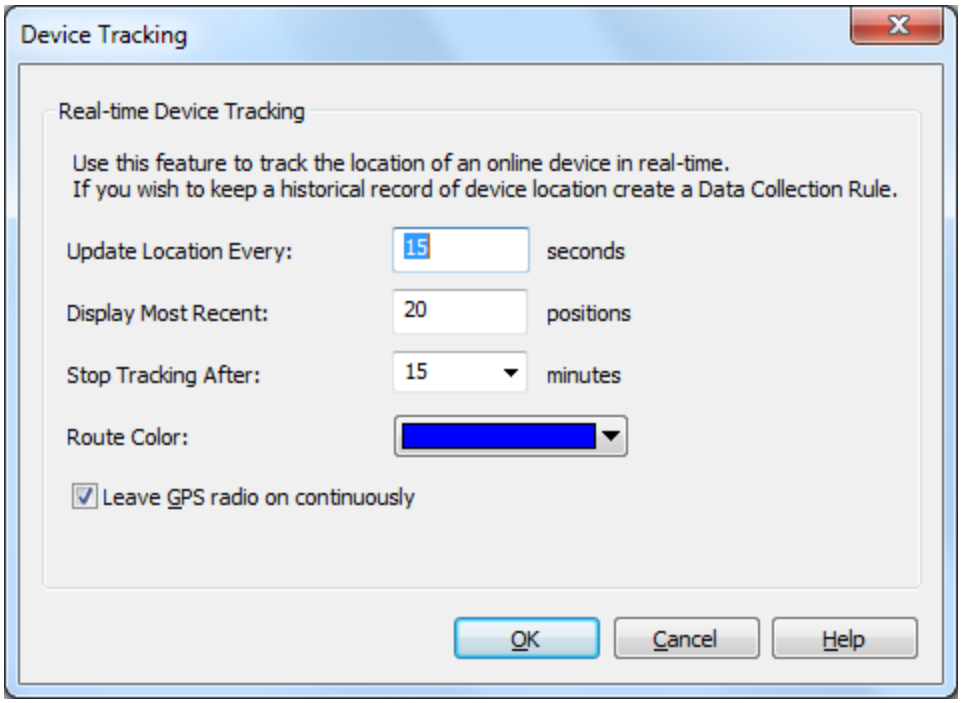
Location Services time out settings

NOTE:

If the MobiControl Manager is behind a proxy server and you are unable to use Location Services, please run the following command through the **Start** menu then **Run**:
`proxycfg -u` (on Windows XP) or
`netsh winhttp set proxy -server="http=<ProxyServerIP>: <Port>; https=<SSLProxyServerIP>: <Port>"` (on Windows Vista, **with no spaces between the quotation marks**.)
This command will update the WinHTTP service with the settings from Internet Explorer.

Using the Track Feature

To use the Track feature in MobiControl's Location Services, right-click on the device you wish to track, select **Location Services,** and click **Track.**



Device Tracking dialog box

The track feature will use the GPS unit associated with your mobile device to determine the current latitude and longitude of the device at a given schedule and send the co-ordinates back to the MobiControl Deployment Server. These co-ordinates are then displayed in the Location panel using Microsoft's Virtual Earth. The co-ordinates plotted in the Location panel represent the exact position of the device at the time of the request along with where the device has been since the request was initiated. To view where the device has been in the past, you need to use the show history option within MobiControl's Location Services.

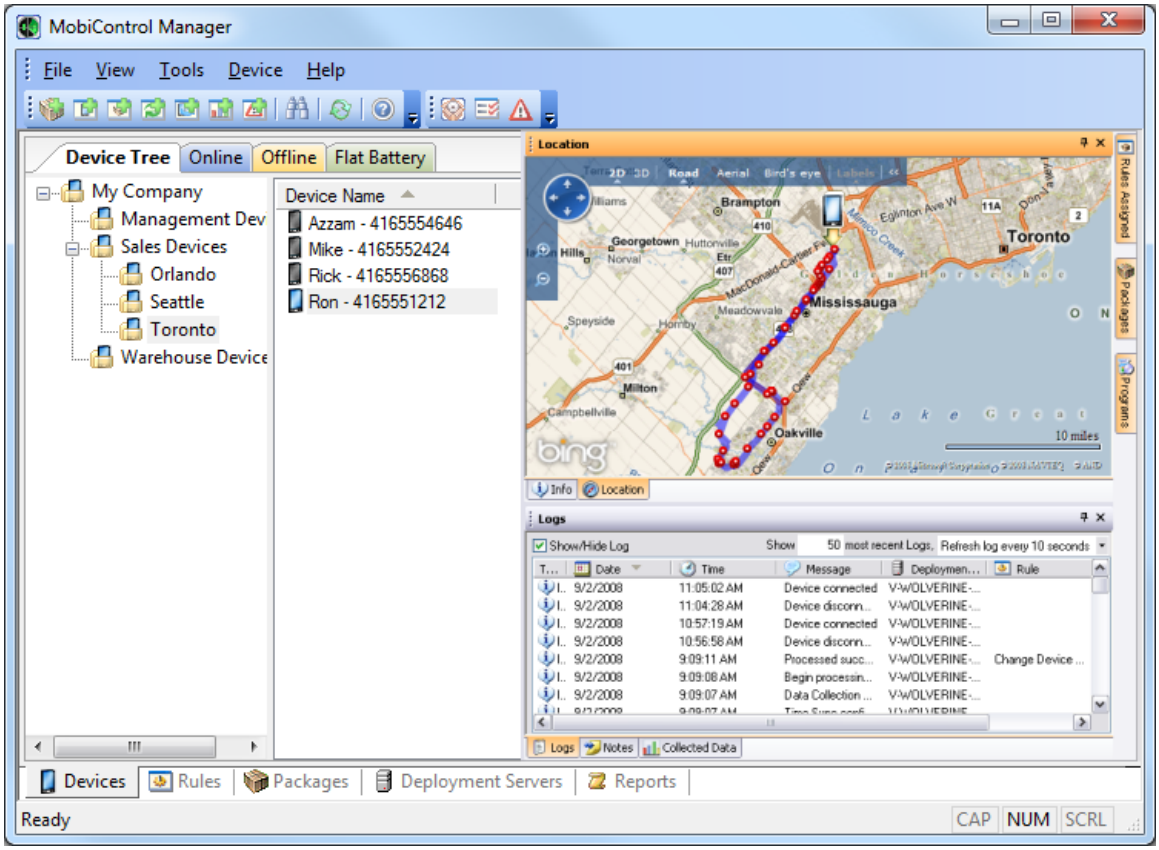
In order to use the track feature, the device must be online and communicating with the MobiControlDeployment Server.

The following table describes each field in the dialog:

Feature	Description
Update Location Every	Set a time interval in seconds (5–86400) for how frequently you would like to have the device location reported.
Display Most Recent	Choose a value to represent the number of recent positions (maximum 100) that you would like to see plotted on the map of the device(s) that you will be tracking.
Stop Tracking After	Set the time interval in minutes (5– 60) for when you would like to end tracking the device.
Route Color	Identifies the device route you will be tracking
Leave GPS radio on continuously	For faster response time from the GPS radio on the device, you should enable this check box. The device's GPS radio will constantly be on.

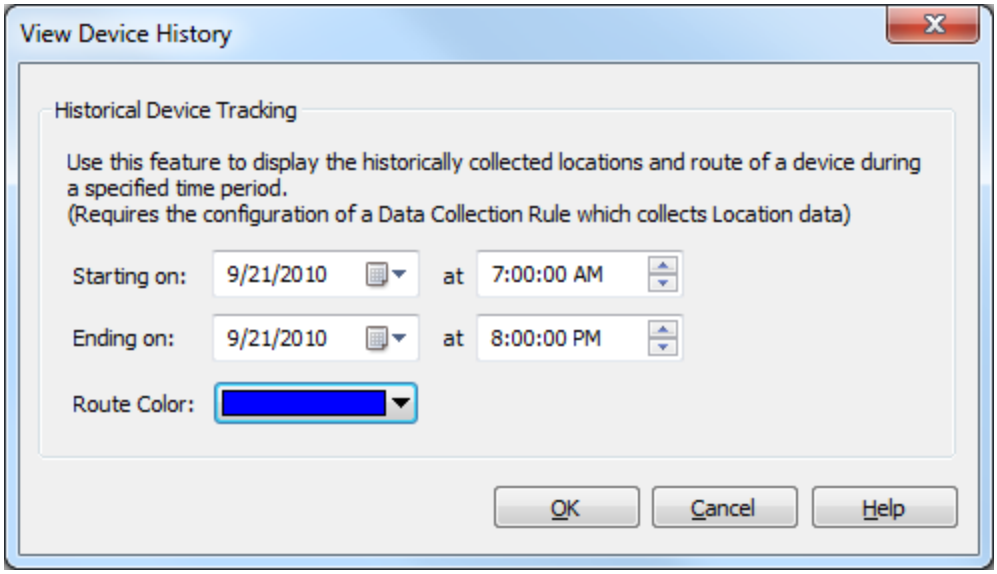
Using the Show History Feature

The show history feature will use the GPS unit associated with your mobile device, allowing you to view where the device has been over a given period of time. To use this feature, you need to set up a data collection rule that collects the location information from the device on a given schedule. The data will be sent back to the device, or, if there is no active data connection on the device, it will be collected and stored in a temporary file and then sent back to the server the next time the device connects. The show history feature does not require the device to be online and communicating with the MobiControl Deployment Server. You can plot information from the history that has been transmitted back to the server during the last active connection.



Location Services history user interface

To use the show history feature, right-click on the device you wish to view, select **Location Services,** and click **Show History.** You will then be prompted to enter the time period for which information is desired, and the route color. Once this is filled in, click **OK** and the path will be plotted.

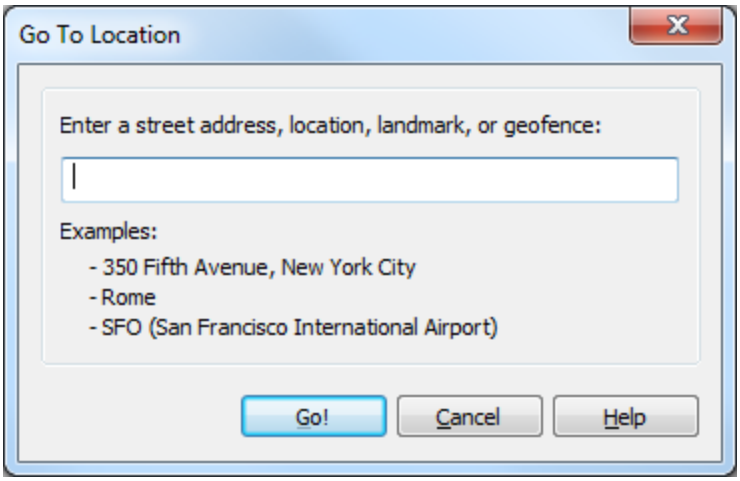


View Device History dialog box

Feature	Description
Starting On	Enter the date and time that you wish to start.
Ending On	Enter the date and time that you wish to stop.
Route Color	Select the color to be used on the map when connecting the co-ordinates.

Using Go To Location

Go To Location allows you to quickly centre and zoom the map to a specific location. Go To Location is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "Location Services" topic on page 103 for more information.

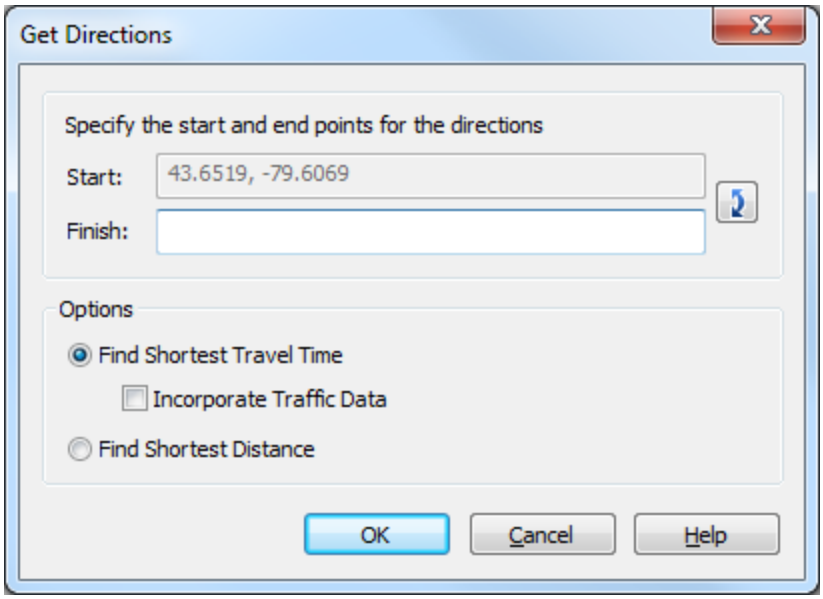


Go To Location dialog box

To use this feature, right click on the Location panel and select "Go To..." from the pop-up menu that appears to open the Go To Location window. You can then enter an address, location, landmark, or the name of an existing geofence. Once you have entered the location information, click the OK button and the map will reload centring on the information you provided. If you entered the name of an existing geofence, the map will change to the location of that geofence and display it on the screen in red.

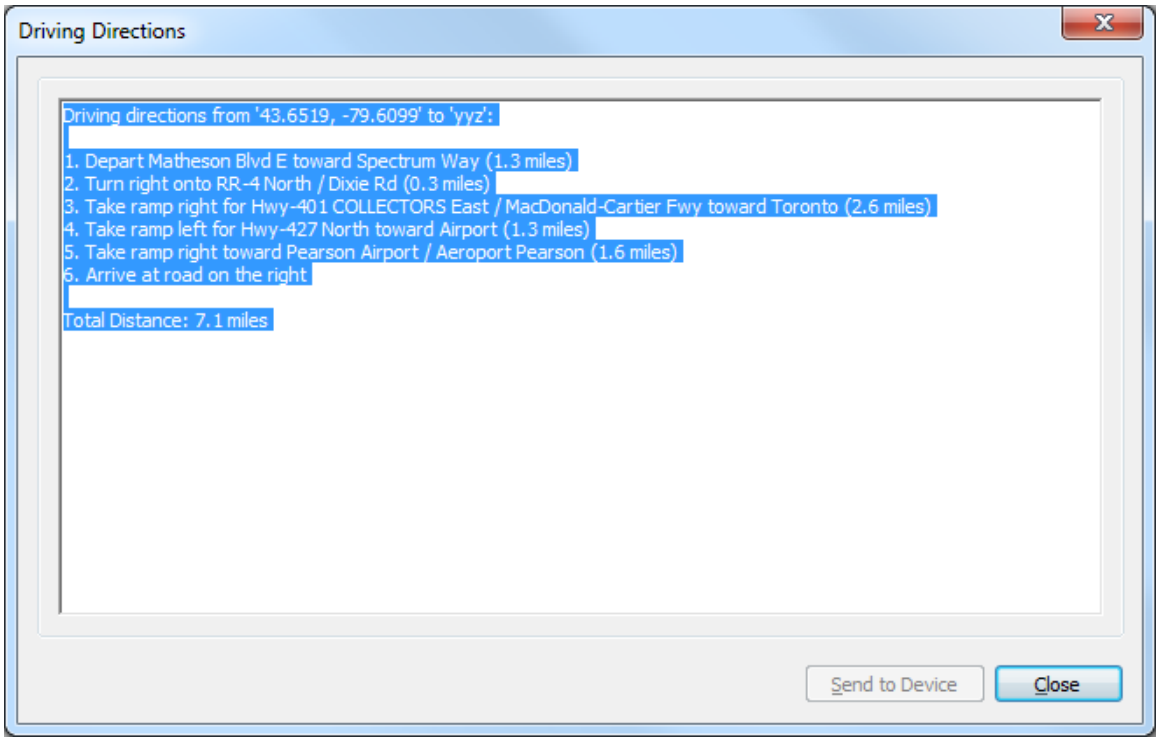
Using Get Directions

Powered by Microsoft's Bing Maps, MobiControl's Get Directions will return turn-by-turn directions between two locations on the map. These directions can be sent directly to the device, or they can be pasted into an email and sent to a larger group of people. Get Directions is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "Location Services" topic on page 103 for more information.



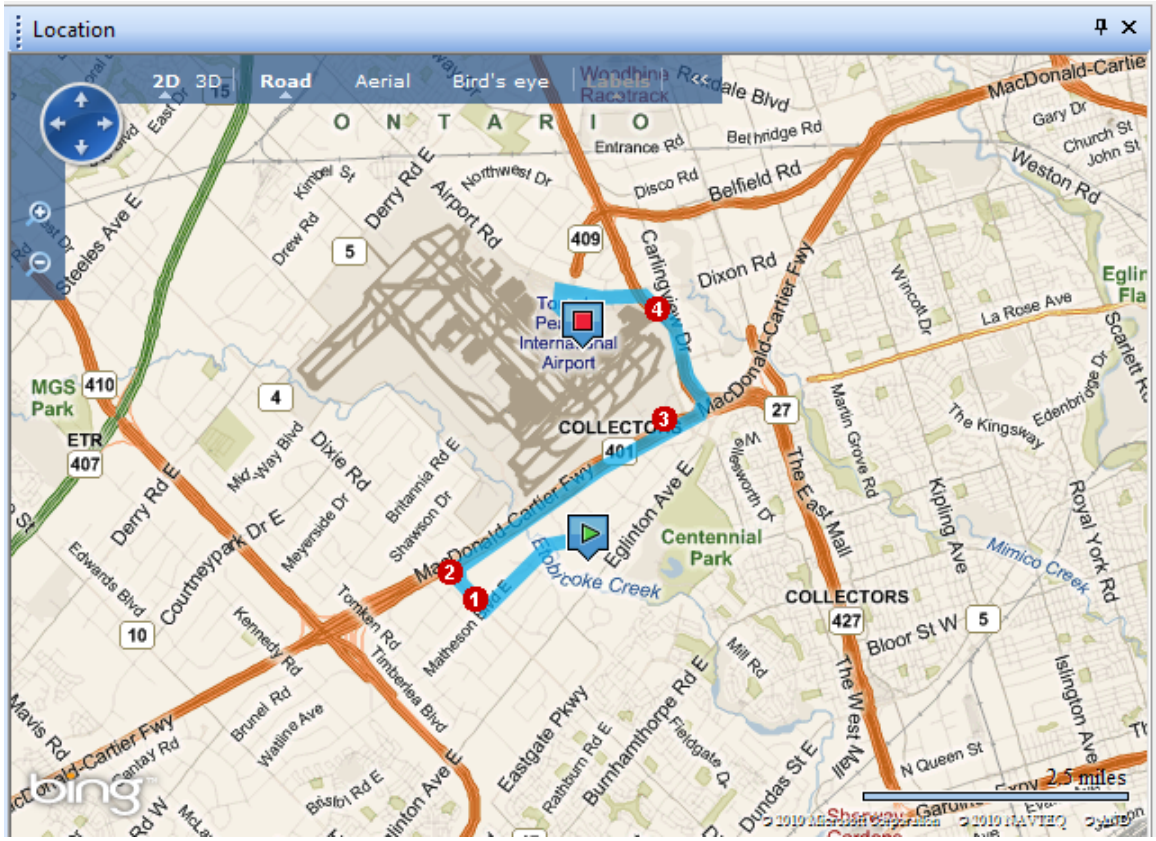
Get Directions dialog box

To use Get Directions, in the Location panel right click on any device or a point on the map and select "Get Directions" from the pop-up menu. The Get Directions dialog box will appear. Be default, the device or map location clicked on will be used as the starting point. To change this, click the double arrow button located to the left of the Start and Finish fields. You can enter GPS co-ordinates, landmarks, or an address. Directions can be optimised by selecting shortest travel time or shortest distance from the options list and press the OK button.



Driving Directions window

MobiControl will determine the turn-by-turn driving directions between the two locations you specified. The resulting directions will be displayed in the Driving Directions window. If you started by right clicking on a device, the "Send to Device" button will be enabled and you can send the instructions directly to the device. You can copy the directions from this window and paste them into an email or document or your choice.

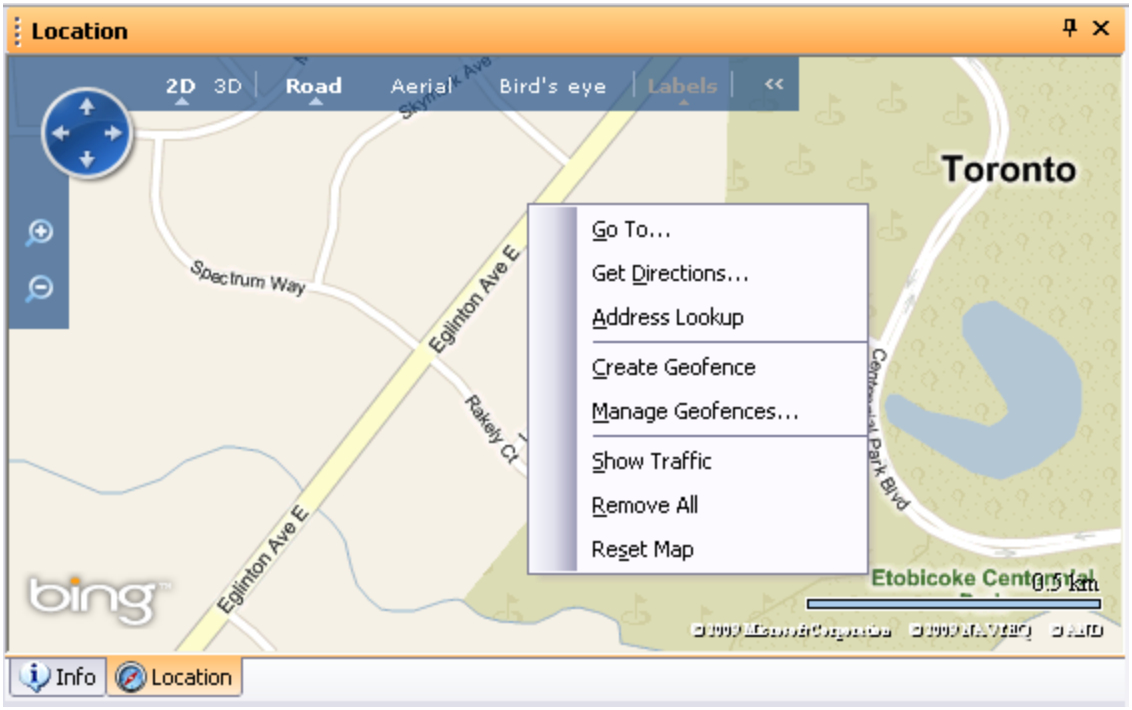


Driving directions displayed on the Map

The Location panel will reload the map to show the driving route highlighted. If the map is in Bird's Eye view, the highlight will not be displayed. Both Aerial and Road view will display the highlighted route.

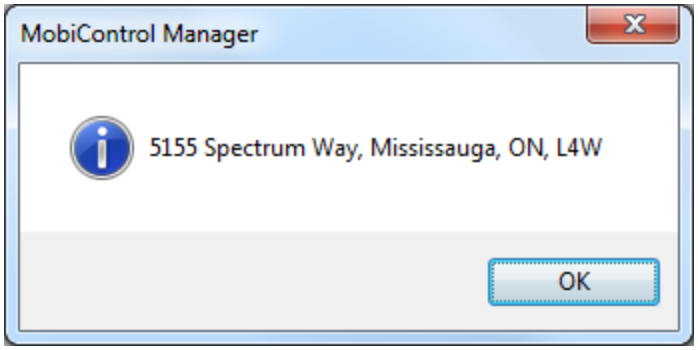
Using Address Lookup

The Address Lookup feature allows you to determine the address of a specific point on the map displayed on the Location panel. Address Lookup is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "Location Services" topic on page 103 for more information.



Location panel right click menu with Address Lookup option

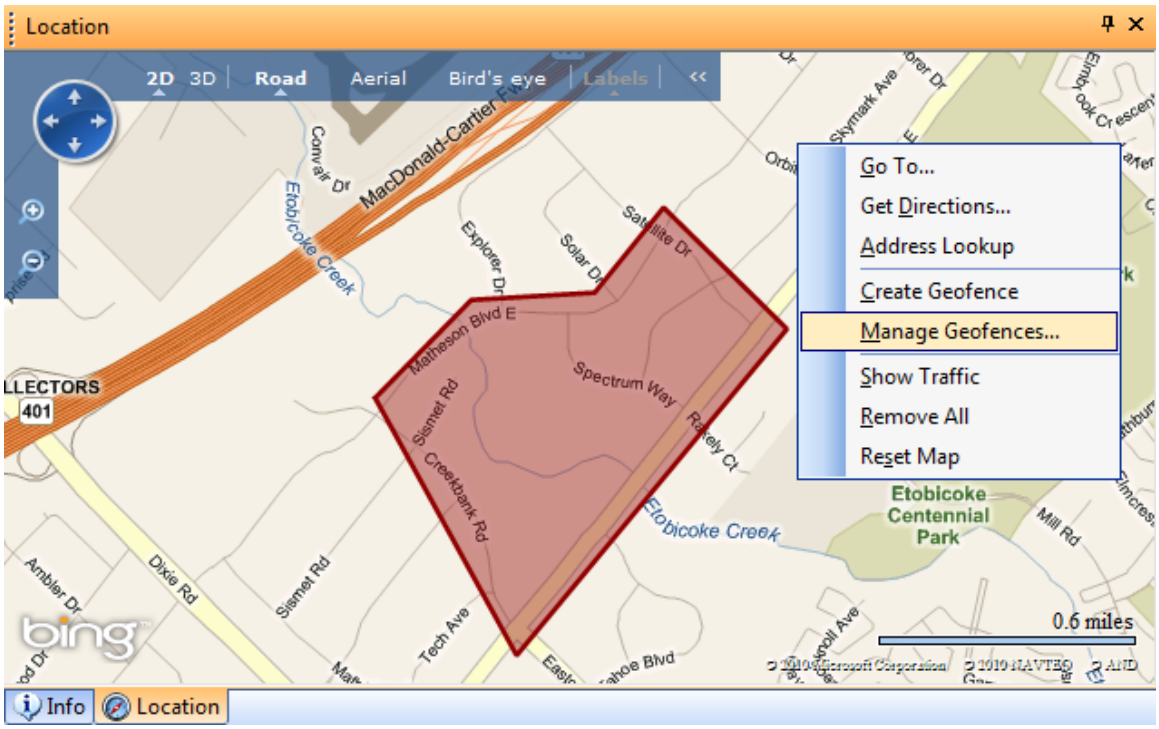
To use the Address Lookup feature, right click anywhere on the map in the Location panel and select the Address Lookup option from the menu that appears. The address of that location will be displayed in a new information window.



Address Lookup window

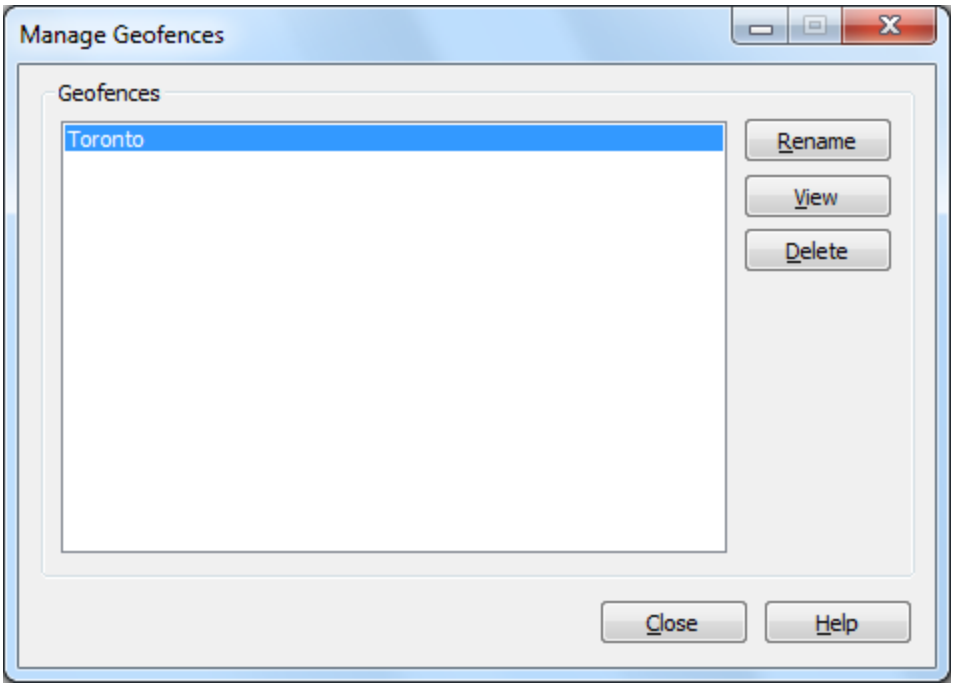
Using Manage Geofences

The Manage Geofences feature provides an area in which to rename, delete or view current created Geofences. You also have the option to create a new geofence from the drop down menu.



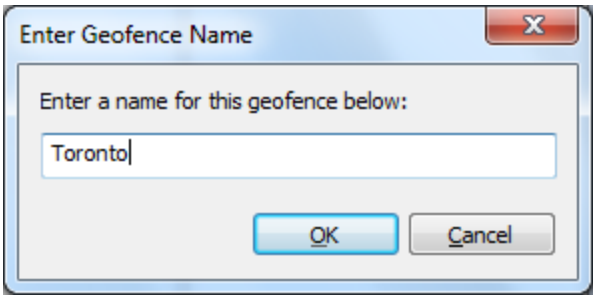
Location panel right click map and select Manage Geofence option

Selecting Manage Geofence brings up the following window.



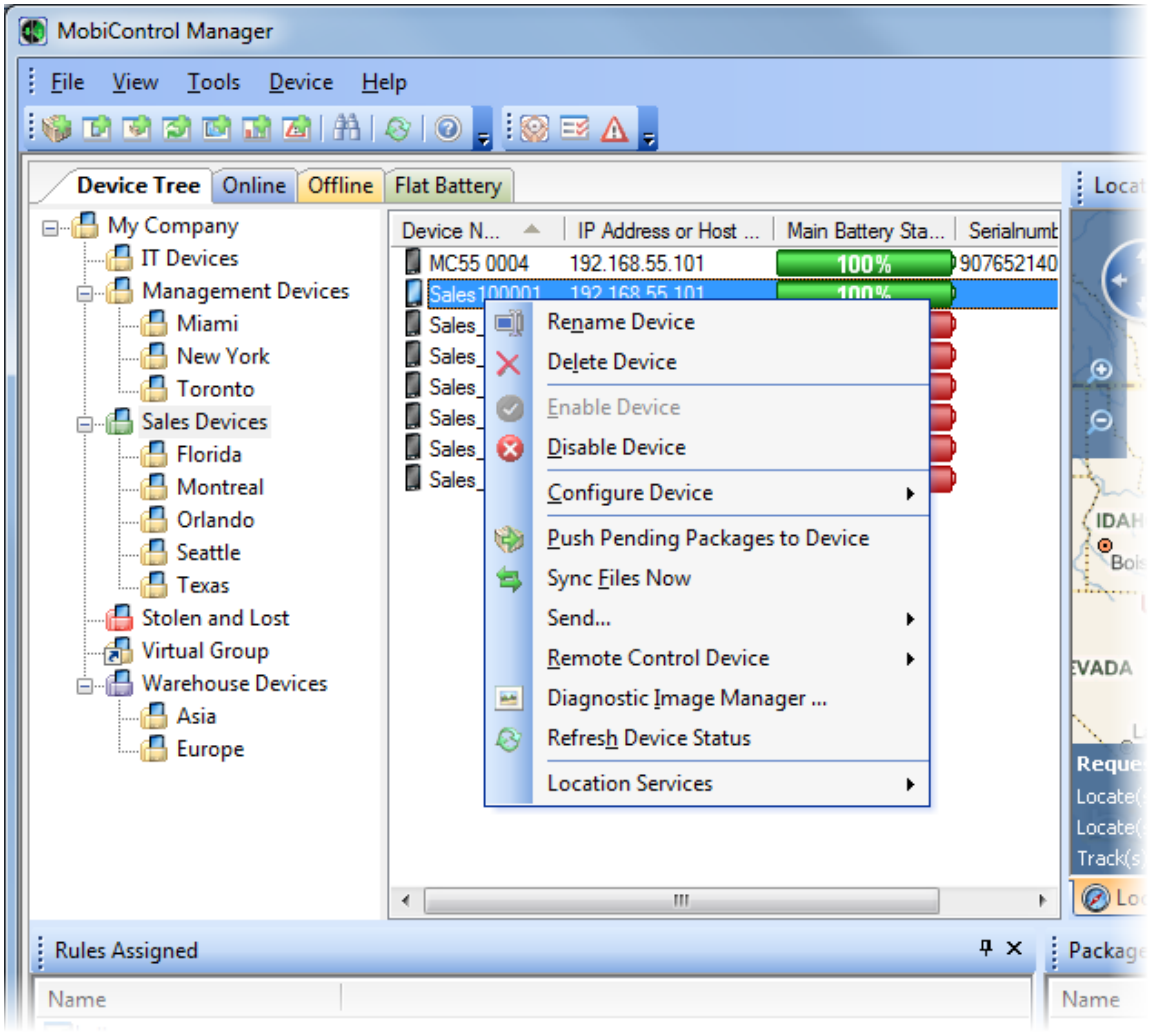
Field Name	Description
Rename	Allows you to rename a Geofence
View	Allows you to view an already created Geofence on the map
Delete	Allows you to delete a Geofence **NOTE:** In order to Delete the Geofence, no Geofence Event can be associated with it

The **Create Geofence** option allows you to begin drawing on the map. The area drawn on the map will be defined as the Geofence. The defined area must be a complete geometric shape, which means the Start Drawing point will be the same as the End Drawing point. When you have completed a proper geometric shape you be asked to name your geofenced area.



Device Menus

The **Device** menu makes device configuration easily accessible. Different items appear in the **Device** menu depending on whether a group or device is selected. The menu options are in both the pop-up menu that appears when right-clicking a device or device group, and in the drop-down **Device** menu from the main toolbar. Both menus are explained in detail.



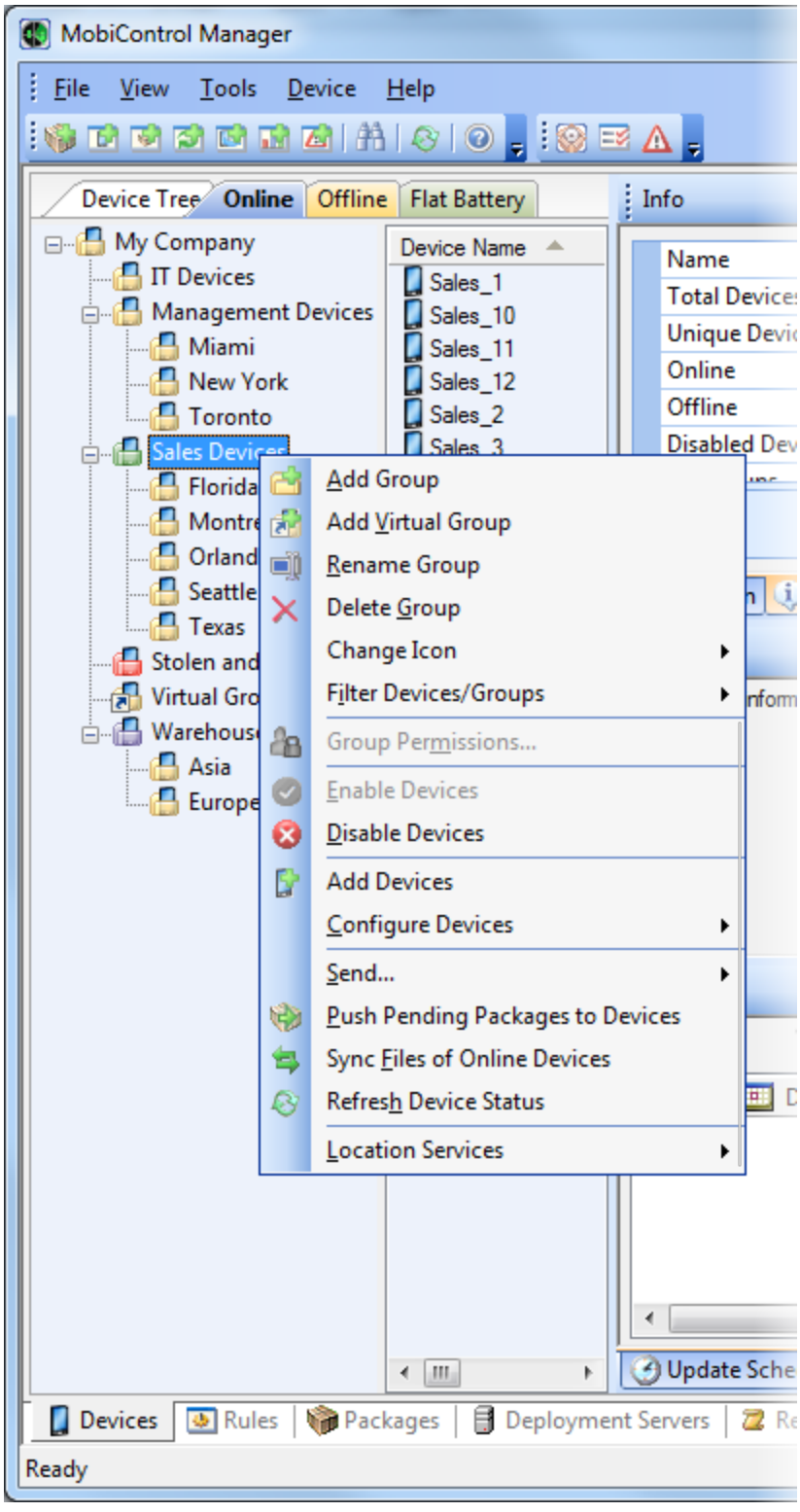
Device menu

The following table describes the menu items of the Device menu:

Field Name	Description
Rename Device	The device name is the user-friendly name for the device, but not its unique identifier (that is the role of the device ID.) It is possible to have more than one device with the same name, but this might lead to confusion. The device name can also be changed from the MobiControl applet that runs on the device.

Field Name	Description
Delete Device	It is recommended to delete the device when it is offline, and when the MobiControl Agent has been uninstalled from the device. If you do not uninstall the agent, the device may be able to reconnect, assuming a valid add devices rule will accept it, and reappear in the device tree.
Enable Device	Enables the MobiControl Device Agent on the device When a device is disabled, the MobiControl Deployment Server will not accept any connections from the device. This prevents the device from getting new packages and setting changes that may be configured while it is disabled. However, when the device is re-enabled, it will receive any packages or settings it may have missed while disabled.
Disable Device	See "Enable Device" above.
Configure Device	From the **Configure Device** sub-menu you can modify various configuration parameters for the selected device. • **Remote Control Settings** allow you to specify the default remote control connection profile for the device, as well as the 'skin' for the device.Please see the "Remote Control Settings" topic on page 158. • The **Update Schedule** option allows you to adjust when you want the device to query the Deployment Server for updates. Please see the "Device Update Schedule" topic on page 160. • The Security option allows you to set or adjust device security parameters such as lockdown. Please see the "Device Security and Control" topic on page 183. • The **Deployment Server Priority** option allows you to adjust the priority ranking of the Deployment Servers that are accessible for this device. Please see the "Deployment Server Priority" topic on page 167. • The **Advanced Settings** option allows you to adjust device connection and logging settings. Please see the "Advanced Settings" topic on page 168. • The **Device Time Synchronization** option allows you to configure device time synchronization settings. Please see the "Device Time Synchronization" topic on page 173. • The **Custom Data** option allows you to configure custom data collection. Please see the "Custom Data" topic on page 175.
Push Pending Packages to Device	Select this option to force the Deployment Server to immediately deliver any packages that have been queued for the device, but have not been delivered yet because there has not been a scheduled check for updates since the package(s) were deployed. This option is only available if the device is currently online. In addition to delivering packages to the device, execution of this command also causes packages that have been scheduled for uninstallation to be removed immediately.
Sync Files Now	Select this option to have this device execute all of the file sync rules that are assigned to it. If there are no file sync rules assigned to this device, nothing will be transmitted. This option is available only if the device is online.
Send...	Select this option to send a message to the device's screen, send it a script, soft reset the device, or turn off the device. The latter two options are available only if the device is online. Please see the "Sending Messages / Scripts" topic on page 136 for details.  **NOTE:**

Field Name	Description
	If you turn off the device, the device will disconnect from the MobiControl Deployment Server to which it is currently connected. You will not be able to remotely manage the device until it is turned on again.
Remote Control Device	From the **Remote Control Device** sub-menu you can choose to remote control via TCP/IP or ActiveSync. This option is available only if the device is online. • Select the **TCP/IP** option when your device is remotely connected to the network (i.e. LAN, Wi-Fi, cellular). • Select the **ActiveSync** option when your device is directly connected to your computer via ActiveSync. Please see the "Help Desk" topic on page 28 for a detailed explanation of the remote help desk console.
Diagnostic Image Manager	The Diagnostic Image Manager is a powerful diagnostic tool that allows you to easily identify changes in a device's state,for instance, changes to the file system or the registry. Please see the "Diagnostic Image Manager" topic on page 145 for a description.
Refresh Device Status	Refreshing entails immediately pulling the most up-to-date information about the devices from the database, and sending a request to each device to have them send updated status information up to the Deployment Server. Upon receipt of the updated status information from the device, the Deployment Server will update the status information in the database and notify the Manager so that it can be immediately displayed to the user.
Location Services	From the **Location Services** sub-menu, there are options to track or locate a device. Please see the "Location Services" topic on page 103 for more information about these two features.



Device Group Menu

The following table describes the menu items of the Device Group menu:

Field Name	Description
Add Group	Select this option to add a group. Once you have created the groups you need, you can easily drag and drop them to re-organize the tree. You can nest groups in each other up to 20 levels deep! Please see the "Device Groups" topic on page 124 for a detailed explanation of device groups.
Add Virtual Group	Select this option to add a virtual group. Please see the "Device Groups" topic on page 126 for a detailed explanation of virtual device groups.
Rename Group	Select this option to rename the group.
Delete Group	Select this option to remove the group from MobiControl.You can not delete a group that is associated with an add devices rule. Delete the add devices rule or modify it so that it doesn't use this group in order to delete it. **NOTE:** Deleting a group will delete all devices that are in the group from the MobiControl system.
Change Icon	Select this option to modify the color of the icon. Color-coding the device groups makes it easier to find a group of interest in the device tree.
Filter Devices/Groups	Select this option to apply a filter to the devices in this group. Applying a filter on a group is a convenient method of identifying a subset of devices that satisfy a certain criteria such as the IP subnet on which they are. Please see the "Device Filters" topic on page 130 for more information on device filters.
Enable Devices	Select this option to enable the MobiControl Device Agent on the devices within this group. See "Enable Device" in the table above for an explanation of this action.
Disable Devices	Select this option to disable the MobiControl Device Agent on the devices within this group. See "Disable Device" in the table above for an explanation of this action.
Add Devices	Select this menu option to launch the wizard Create Add Devices Rule Wizard which will guide you through the process of adding devices to the treeMobiControl. Please see the "Add Devices" topic on page 127 for details.
Configure Devices	From the **Configure Devices** sub-menu, you can modify various configuration parameters for the selected group. • **Remote Control Settings** allow you to specify the default remote control connection profile for the device, as well as the skin for the device. Please see the "Remote Control Settings" topic on page 158. • The **Update Schedule** option allows you to adjust when you want the device to query the Deployment Server for updates. Please see the "Device Update Schedule" topic on page 160. • The **Security** option allows you to set or adjust device security parameters such as lockdown. Please see the "Device Security and Control" topic on page 183. • The **Deployment Server Priority** option allows you to adjust the priority ranking of the Deployment Servers that are accessible for this device. Please see the "Deployment Server Priority" topic on page 167. • The **Advanced Settings** option allows you to adjust device connection and logging settings. Please see the "Advanced Settings" topic on page 168.

Field Name	Description
	• The **Device Time Synchronization** option allows you to configure device time synchronization settings. Please see the "Device Time Synchronization" topic on page 173. • The **Custom Data** option allows you to configure custom data collection. Please see the "Custom Data" topic on page 175.
Send...	Select this option to send a message or script to all devices in a group, or soft reset or turn off all of the devices. The latter two options apply only to online devices. Select the **Queue message for delivery to offline devices** checkbox for the message to be sent to devices that are offline. They will receive it when they come online. Messages will be stamped with the date and time it was sent. Please see the Sending Messages and Scripts page for details.  **NOTE:** If you turn off the devices, they will disconnect from the MobiControl Deployment Server to which they are currently connected. You will not be able to remotely manage the devices until they are turned on again.
Push Pending Packages to Devices	Select this option to force the Deployment Server to immediately deliver any packages that have been queued for the devices in the group, but have not been delivered yet because there has not been a scheduled check for updates since the package(s) were deployed. In addition to delivering packages to the devices, execution of this command also causes packages that have been scheduled for uninstallation to be removed immediately. This action is only executed for devices that are currently online.
Sync Files of Online Devices	Select this option to have the devices in this group execute all of the file sync rules that are assigned to them. If there are no file sync rules assigned, nothing will be transmitted. This action is only executed for devices that are currently online.
Refresh Device Status	Refreshing entails immediately pulling the most up-to-date information about the devices from the database, and sending a request to each device to have them send updated status information up to the Deployment Server. Upon receipt of the updated status information from the device, the Deployment Server will update the status information in the database and notify the Manager so that it can be immediately displayed to the user.
Location Services	From the **Location Services** sub-menu, there are options to track or locate the online devices in a group. Please see the "Location Services" topic on page 103 for more information about these two features.

Device Groups

Device groups allow administrators to organize groups of devices based on their location or function. For example, a company may have devices that are used by sales staff and other devices that are used by warehouse staff. The administrator might in this case create a group called "Sales Devices" to hold the sales devices, and a group called "Warehouse Devices" to hold the warehouse devices. Device groups also allow administrators to perform operations on an entire group of devices by simply selecting the group in the device tree.

Settings and rules are inherited based on the group structure. Hence, subgroups and devices belonging to a parent group are automatically provisioned with the rules assigned to the parent group, and are configured with the settings applied to the parent group. You do have the opportunity to override the inheritance. For example, a general lockdown configuration may be specified at the parent group level, but you can override this and specify a different lockdown configuration for a given subgroup or device.

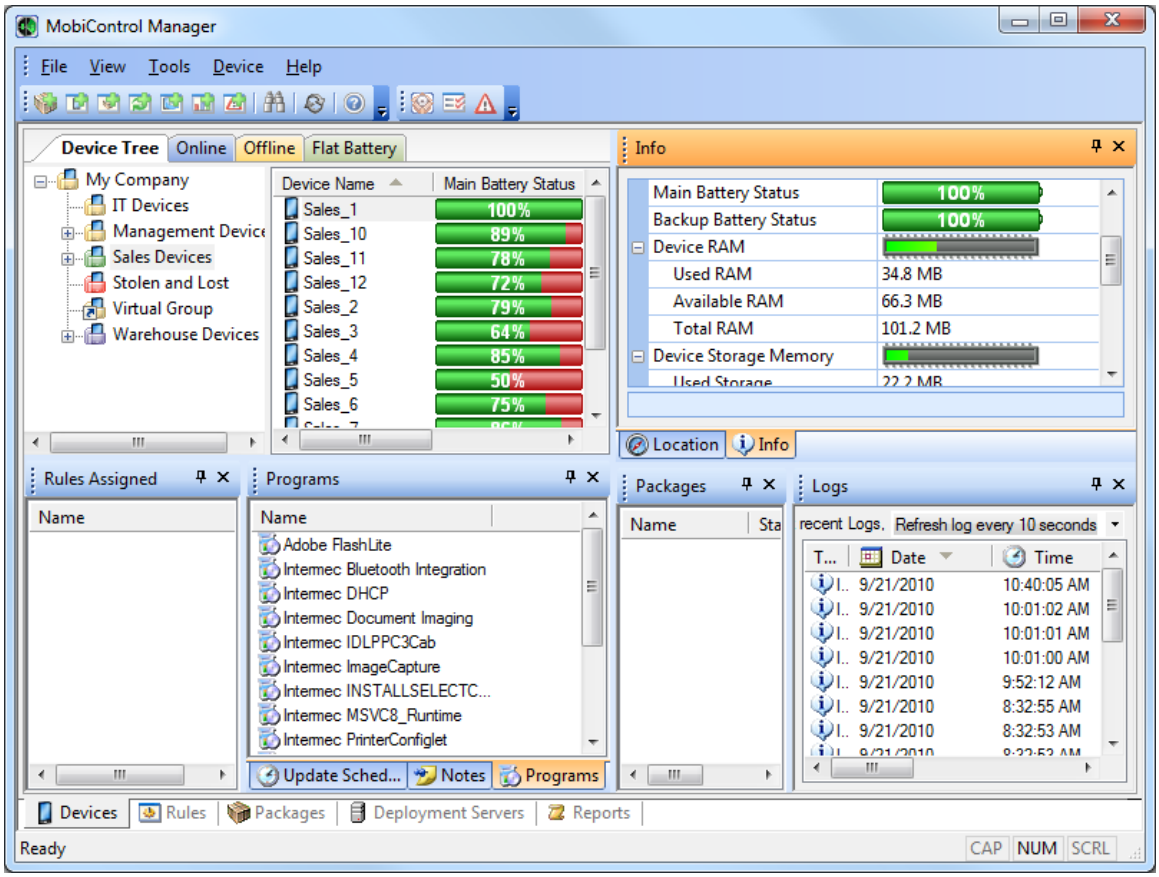
To view and configure groups in the device tree, select the Devices view (tab) in MobiControl Manager, then select the appropriate menu option from the Devices menu or right-click an item in the device tree.

TIP:

When setting up MobiControl, consider how your devices are logically organized in your business, and replicate this structure in the device tree. For example, organize based on device role (Management, Sales, Warehouse) or organize based on geographical location (Boston, New York, San Francisco).

EXAMPLE:

Warehouse Devices are assigned a rule for provisioning scanner software. A certain sub-set of the Warehouse devices also need to be provisioned with an additional package because those devices have a specialized role in the warehouse for doing inventory auditing. Hence they need the scanner software, as well as an auditing application.



MobiControl Manager Devices view (tab)

Device Group Tasks

The device tree supports standard drag-and-drop operations.

Adding a Root Group

From the **Device** menu, click **Add Root Device Group**. It is useful to have root group from which all other groups branch off as this enables you to easily distribute software or settings to all the devices in the organization.

Creating a Subgroup

Select the parent group in the device tree, then click on the **Device** menu and select **Add Device Group**. Subgroups are a great way to assign special rules or settings to a subset of devices that all should still inherit all other rules and settings from a parent group.

Deleting a Group

Select the group in the device tree, then click on the **Device** menu and select **Delete Group**. Deleting a group that contains devices will cause the devices to be deleted as well. Move the devices out of the group before deleting the group if you do not wish to delete the devices. You can not delete a group to which an active add devices rule applies. This is to ensure devices that are newly added have a parent group. In this case you must edit or delete the add devices rule before you can delete the group.

Moving Devices Between Groups

Select the devices you would like to move by holding down the CTRL key and clicking on the devices in the device tree, then dragging the selected devices to the new group.

Virtual Groups

A virtual group is a special type of group that allows you to assign deployment rules or file sync rules to a set of devices, even though the devices may actually belong to different groups in the device tree. This is useful in cases where you want a sub-set of devices to be configured with rules that are typically only assigned to mutually exclusive groups.

Devices are placed into a virtual group by dragging and dropping them into the virtual group. MobiControl automatically creates a shortcut in the virtual group for the device(s). You can easily remove a device from a virtual group by deleting the devices entry in the virtual group. This will not remove the actual device from the MobiControl system. It will only remove the shortcut.

One of the key differences between a regular group and a virtual group is that device configuration settings (remote control settings, update schedule, lockdown and Deployment Server priority) can only be specified for a regular group. The ability to locate or track devices with Location Services at the group level is not available for virtual groups.

EXAMPLE:

Suppose a device in the Management group needs software that is installed on devices in the Sales group. Create a virtual group as a child group to Sales, and then place a shortcut to the Management device in this virtual group. It will be automatically receive the software assigned to Sales devices, in addition to all the Management software it will receive based on its parent group (Management).

Creating a Virtual Group

Select the parent group in the device tree, click the **Device** menu, and select **Add Virtual Group**.

MobiControl Tutorial

This is step 1 of the MobiControl Tutorial. Please see the "Add Devices" topic on page 127 for the next step.

Adding Devices

There are three basic steps that need to be performed in order to add devices to MobiControl:

1. Create an add devices rule.

   Add devices rules configure the settings that MobiControl uses to configure and communicate with your devices. These settings include: the device group that devices are to be added to, how often the device is to check for updates, and the parameters to be used for remote control sessions. Please see the "Add Devices Rule" topic on page 261.

2. Create a Device Agent.

   A Device Agent is the MobiControl software that resides on mobile devices and communicates with MobiControl Deployment Servers. Device Agents execute instructions received from MobiControl Deployment Servers, report status information, and send real-time information to Deployment Servers. Device Agents also restore the device state after a hard reset, service remote control sessions, install/uninstall packages, and synchronize the device clock. Please see the "Device Agent Manager" topic on page 277.

3. Install the Device Agent onto the devices.

   This can be done in one of the following ways: via ActiveSync, a website download, an SD card, or using an existing software distribution mechanism. Please see the "Device Agent Manager" topic on page 277.

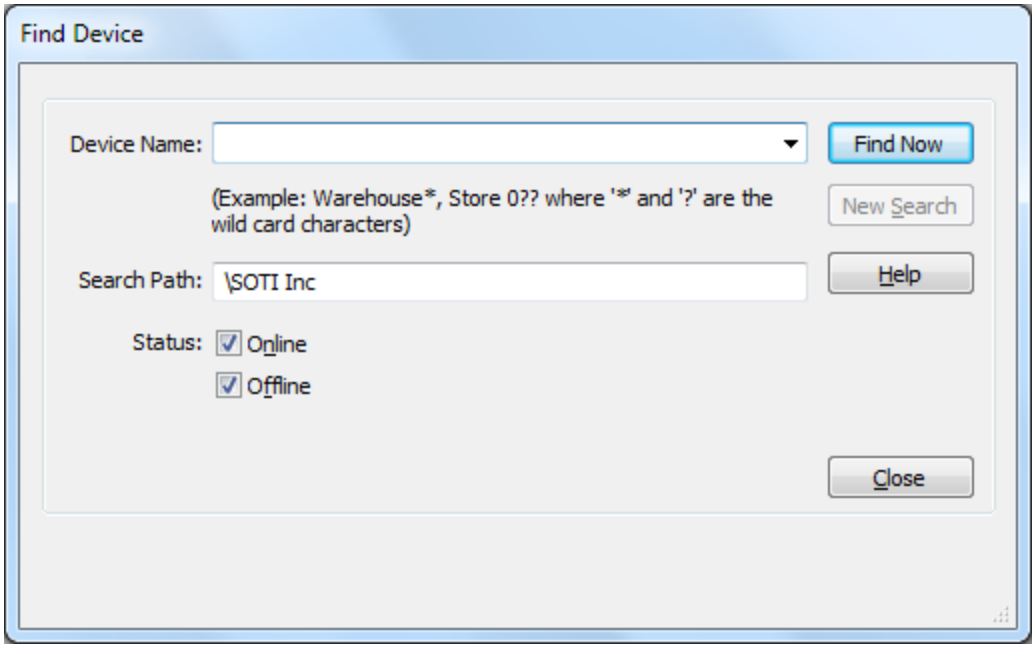
MobiControl Tutorial

This is step 2 of the MobiControl Tutorial. Please see the "Deploying Packages to Devices" topic on page 358 for the next step.

Finding Devices

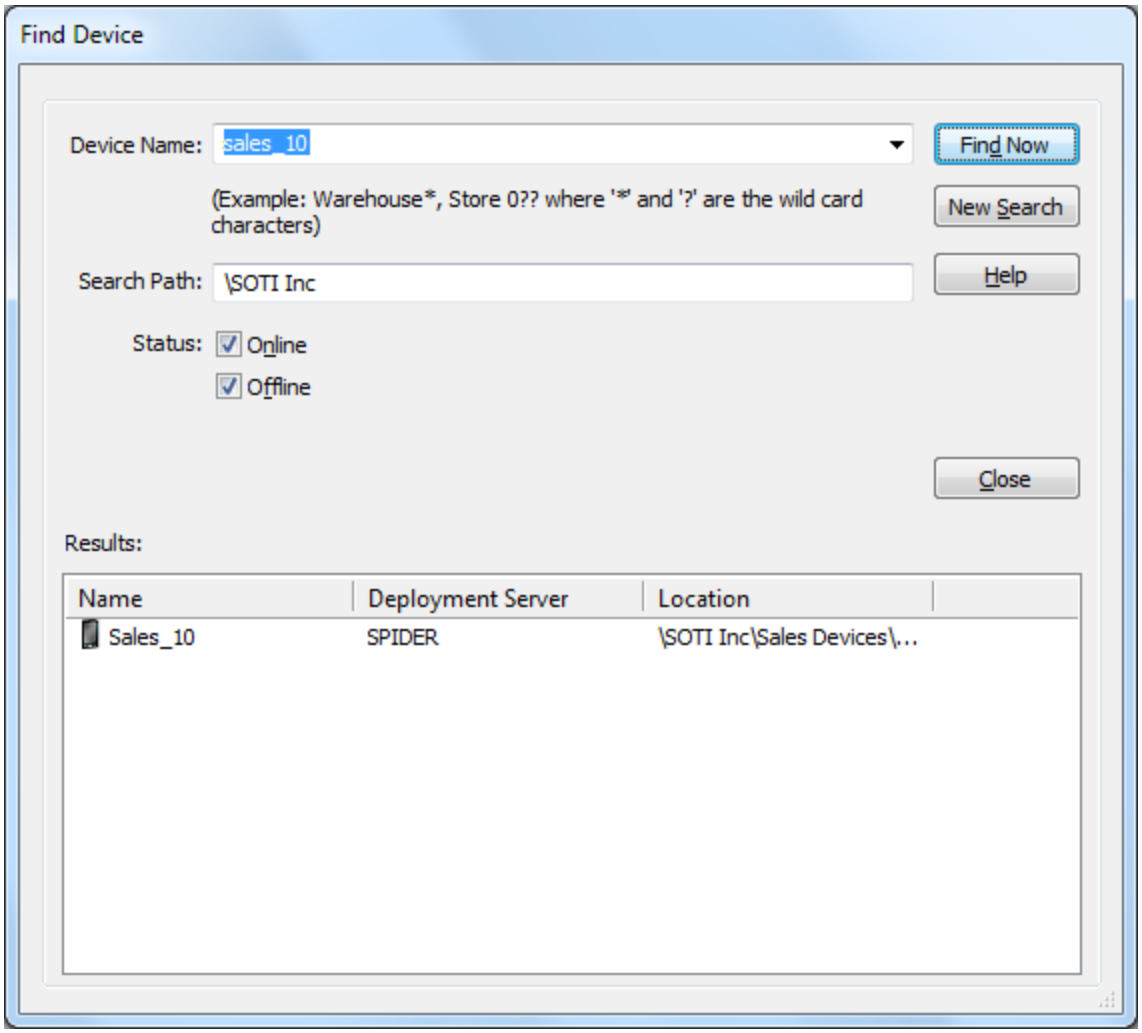
This feature allows you to quickly locate a device in the device tree by searching for the device's name.

To search for a device, click the **Find Device** icon on the MobiControl Manager **Tool** menu, or select **Find Device** from the **Device** menu, or right-click in the device tree pane on the Devices view (tab) in the MobiControl Manager.



Find Device dialog box

Upon clicking **Find Now,** the device tree will be searched for the name entered in the **Device Name** field and the search results will be displayed in the **Results** field. Wildcard characters can be used: "?" substitutes for one character and "*" substitutes for any number of characters. Selecting a device by double-clicking it in the search results also highlights it in the device tree. You can search by groups from the search path, and also search from online or offline mobile devices.



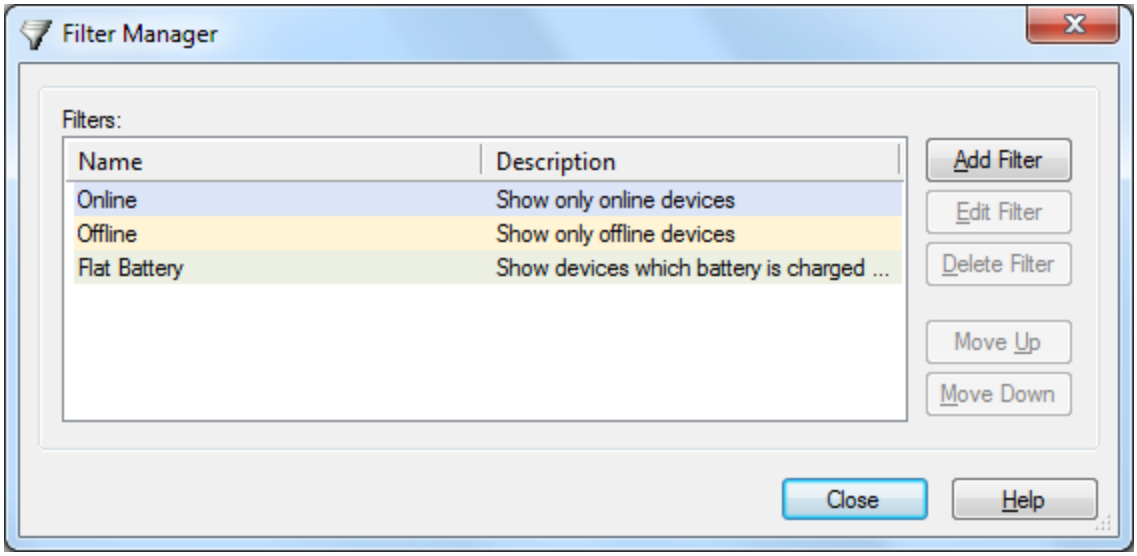
Search results in the Find Device dialog box

EXAMPLES:

- To search for devices with "`WM5`" in the name, search for "`*WM5*`."
- To search for devices with model numbers ending in "`900`," "` 960`," or "`990`," search for "`*9?0`."

Device Filters

Device filters allow you to create a customized view of the devices in your deployment. These are useful for quickly identifying sets of devices based on their status or settings. For example, the Online filter only displays the devices that are currently online.



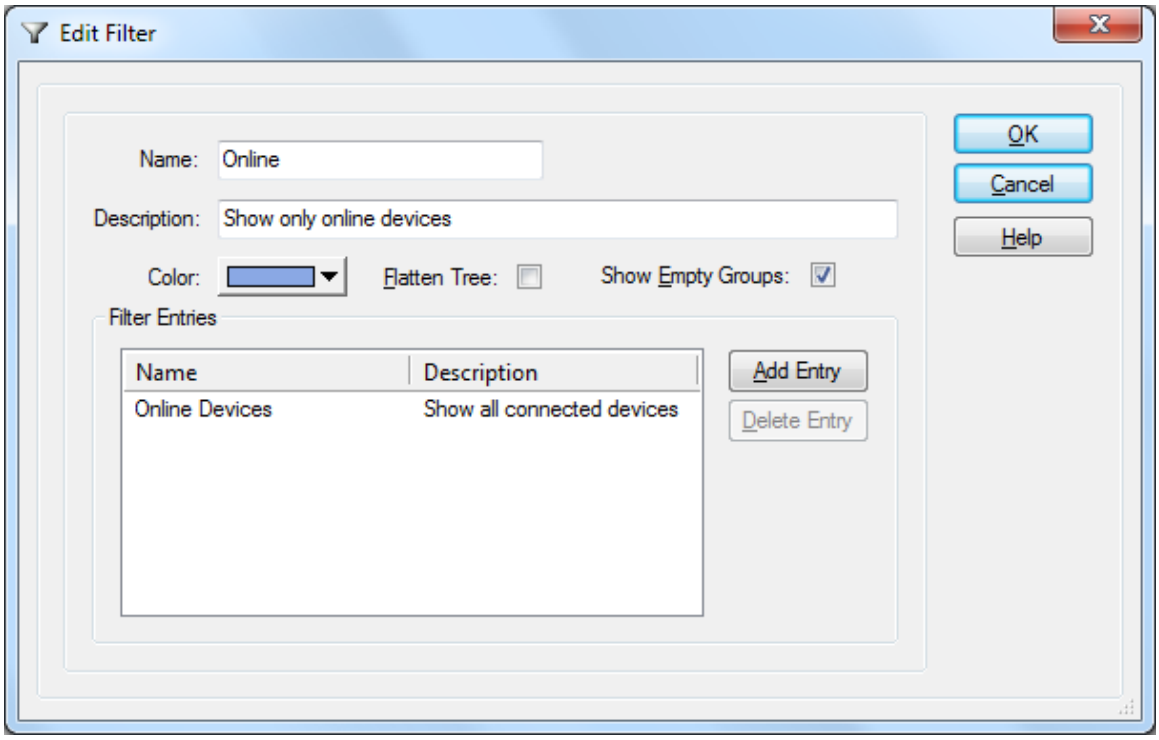
Filter Manager dialog box

To edit existing filters or add new ones select **Filter Manager** from the **Tools** menu.

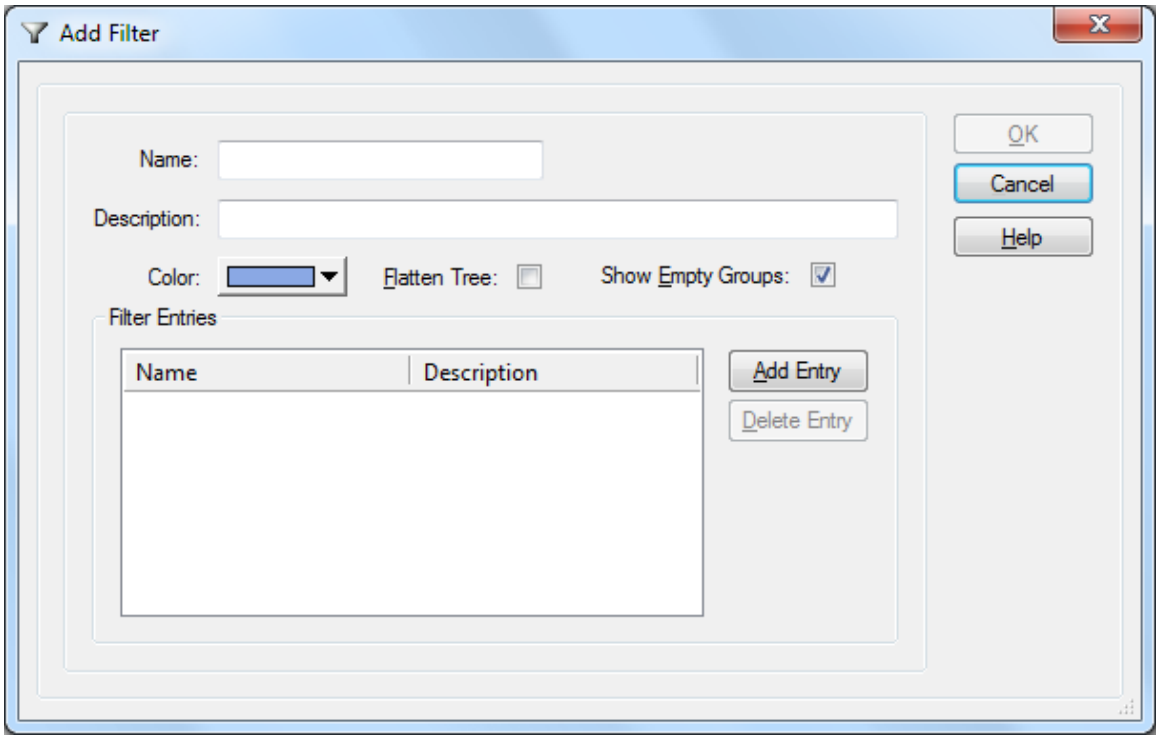
Field Name	Description
Filters	Lists the filters that are configured in the system. Filters are stored in the central database and are shared by all users of MobiControl Manager. **NOTE:** If you define multiple filter entries for 1 filter, the conditions are logical, meaning, that they're added together and **ALL** conditions must be met in order for a device to be listed in the filtered view.
Add Filter	Select this button to create a new filter. The **Edit Filter** dialog box will be displayed. Please see the Adding or Editing a Device Filter section below.

Field Name	Description
Edit Filter	Select this button to edit an existing filter. The **Edit Filter** dialog box will be displayed. Please see the Adding or Editing a Device Filter section below.
Move Up/Down	Use the **Move Up** and **Move Down** buttons to adjust the order the filter tabs appear in the Manager window.

Adding or Editing a Device Filter



Edit Filter dialog box



Add Filter dialog box

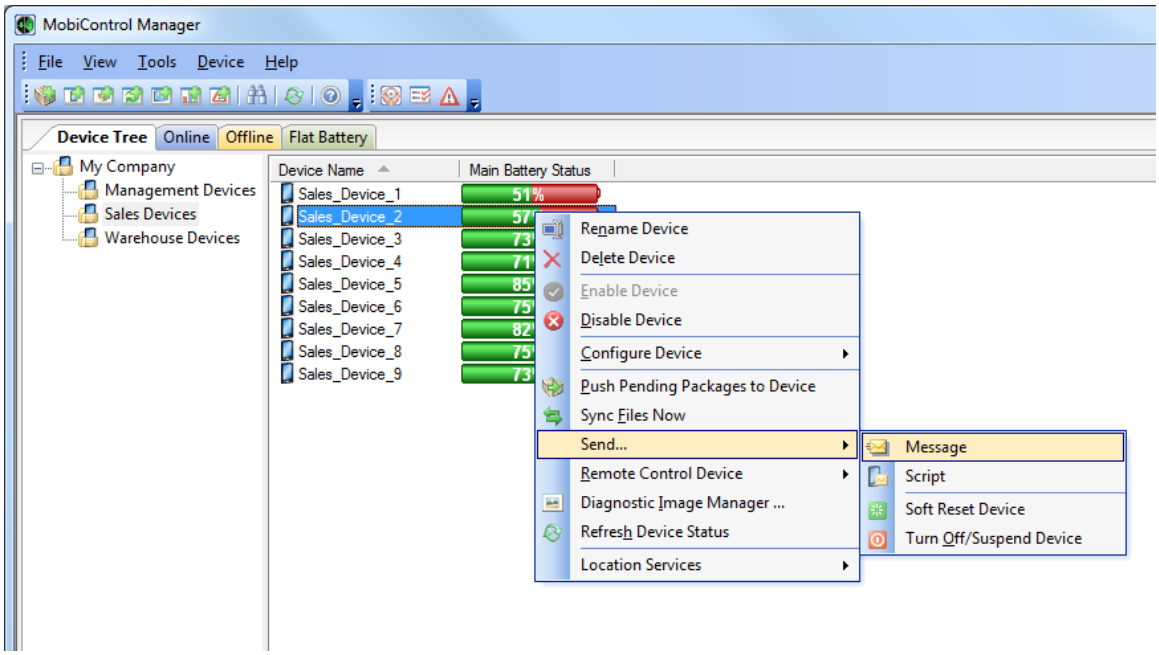
Field Name	Description
Name	Enter a descriptive name for the filter. **TIP:** Use a short name to minimize the length of the tab label, allowing for multiple tab labels to be visible without scrolling.
Description	a one-line description for the filter
Color	Colors distinguish the selected filter.
Flatten Tree	Hides the standard device tree groups and displays only a list of the devices. This is useful when you know your filter will only reveal a small set of devices and you are not interested about the group to which they belong.
Show Empty Groups	Uncheck this box to hide empty groups in the filtered view.
Filter Entries	Lists the actual filter types and parameters that constitute the filter. You can have multiple entries. For example, you can filter for all online devices in a certain IP subnet.
Add Entry	Select this button to add a filter entry. A pop-up menu is displayed with a list of filter types that can be specified. Configure the chosen filter entry and then click **OK** to return to this dialog box. The options available are:

Field Name	Description
	• The **connection status filter** which shows devices that are (or have been) online or offline, now, more than or less than a set time. **EXAMPLE:** "Show devices offline for more than 2 hours" The time parameter can be set to minutes, hours, days, or years. • The **IP sub network filter** shows devices connected to a specific subnet in the network. **EXAMPLE:** "Show devices connected to the following sub network: 192.168.100" • The **battery status filter** shows devices with battery status less than, (not) equal to, or more than a set size. **EXAMPLE:** "Show all devices with battery status less than or equal to 70%." • The **available storage filter** shows devices with available storage capacity less than, (not) equal to, or more than a set size. **EXAMPLE:** "Show devices with available storage capacity is less than 5 MB." • The **agent version filter** shows devices which have a MobiControl Device Agent whose version is less than, (not) equal to, or more than a set version. **EXAMPLE:** "Show all devices where Agent Version is v5.00" • The **custom data filter** shows devices with the specified custom data. **EXAMPLE:** "Show devices with custom data, where Field Name='CustomApp' with Value='CustomApp.exe'"
Delete Entry	Deletes a filter entry

Sending Messages and Scripts

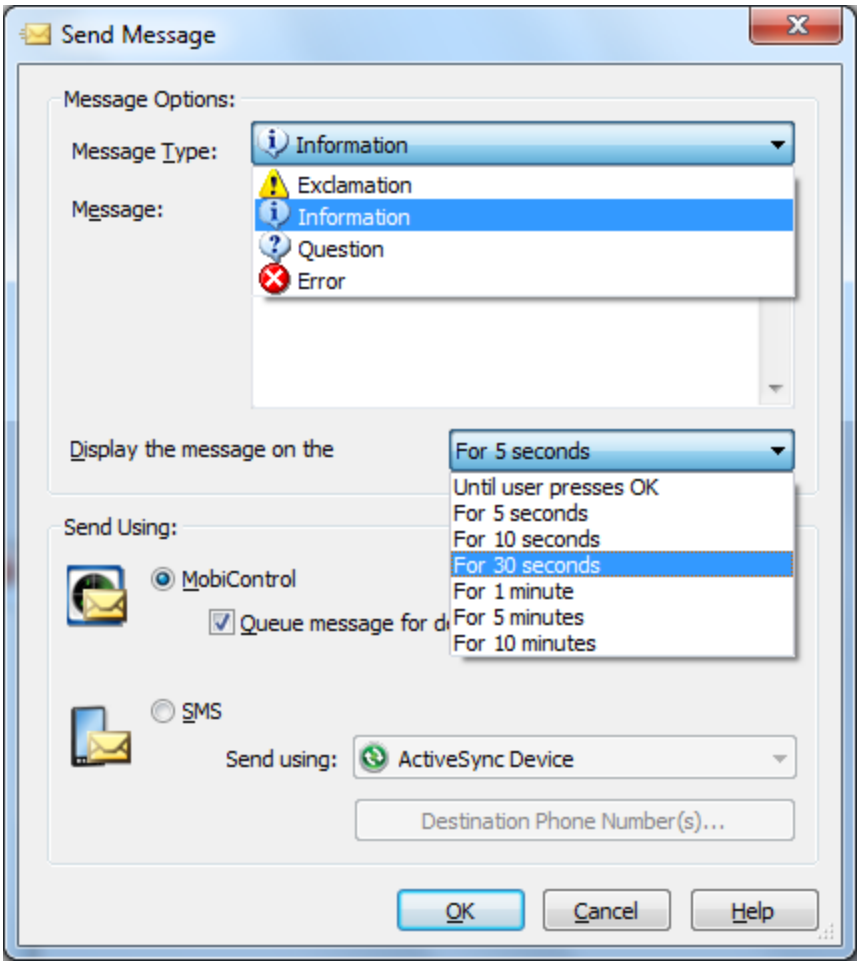
Select this option to send a message or script to one or more mobile devices. These can be sent using MobiControl or SMS (Short Message Service) from any online device or device connected via ActiveSync device. This feature can be used to keep users informed or updated remotely.

In the MobiControl Manager, right-click on a device, select **Send** and click **Message** or **Script** to start sending messages to the mobile devices. You can also choose to soft rest or turn off or suspend the device.



Send Message via MobiControl

If your mobile device can receive SMS messages, you have the option to send one and have the SMS show up as a text message. You can also initiate a connection to MobiControl or run a script on the mobile device.



Send Message dialog box displaying the different message types and durations

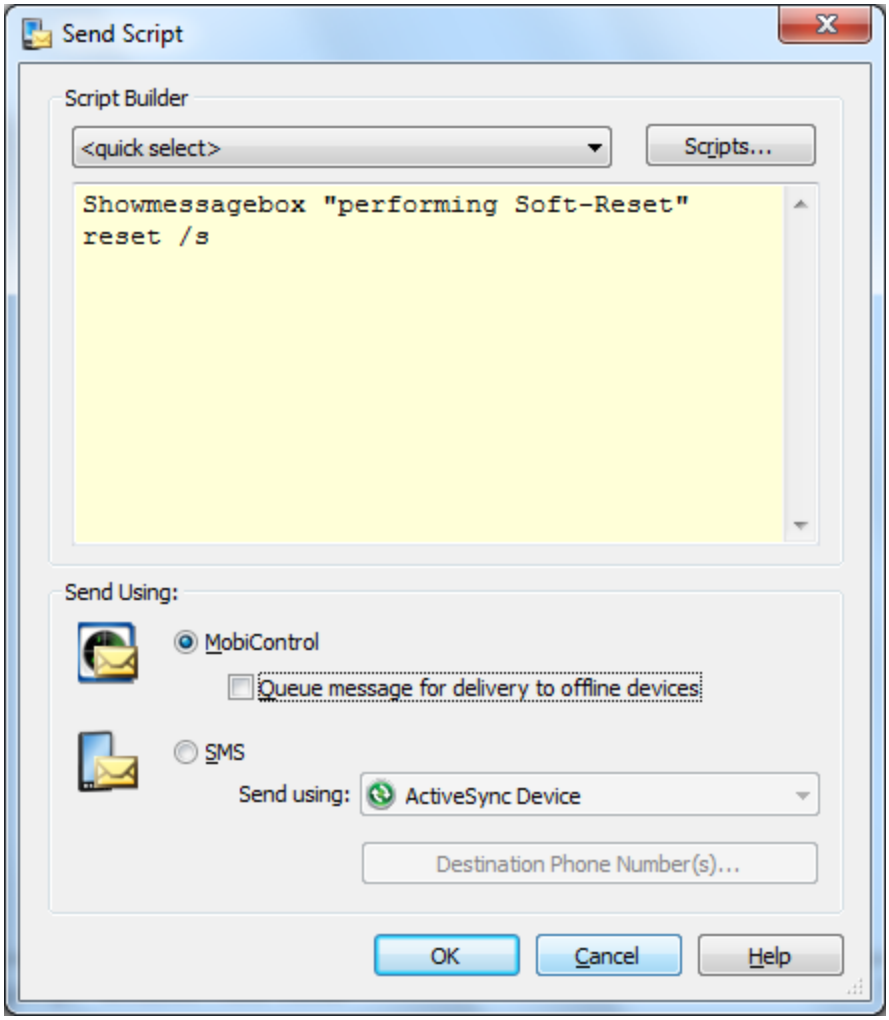
The table below describes each individual field of the **Send Message** dialog box:

Field Name	Description
Message Type	From the drop-down box, select the type of message you wish to send (information, exclamation, question, or error).
Message	A brief note to the recipient
Display the message on the device(s)	Select a time intervals for which the message can be displayed on the device.
MobiControl	Sends the messages via MobiControl. There is no character limit with this option.
Queue message for delivery to offline devices	Sends the message to devices that are offline and will receive the message when they come online. The message will be stamped with the date and time it was sent.
SMS (Short	Send the message via SMS text message. You may use a device that is connected

Field Name	Description
Message Service)	via ActiveSync, or you may select a device that is online.
Send Using	Send a message from a device connected via ActiveSync or select an online device.
Destination Phone Number(s)	This is where the message will be delivered. This area is populated with the phone number(s) of the device you selected. Multiple phone numbers need to be separated by a semi-colon ";".

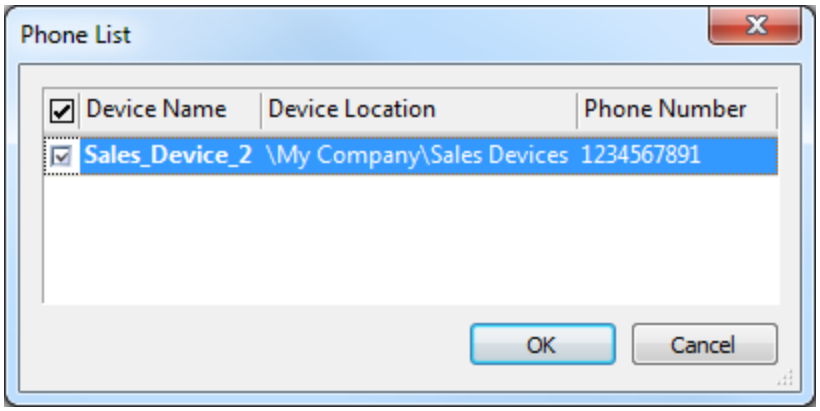
Sending Scripts to the Device

If you want to run a custom script on a mobile device, you can do so with MobiControl. In the **Script** box, you can enter the script commands and instructions that you want to run on the device. When the instructions are received by the mobile device, the script commands will be executed on the mobile device. These instructions can be sent using SMS or through MobiControl.



Send Script dialog box

A Script or Message can be sent to the mobile device by specifying the Destination Phone Number(s). When this option is selected the Phone List dialog box will be displayed that shows the Device Name, Device Location and Phone Number(s).



Phone List dialog box

The table below describes each individual field of the **Send Script** dialog box:

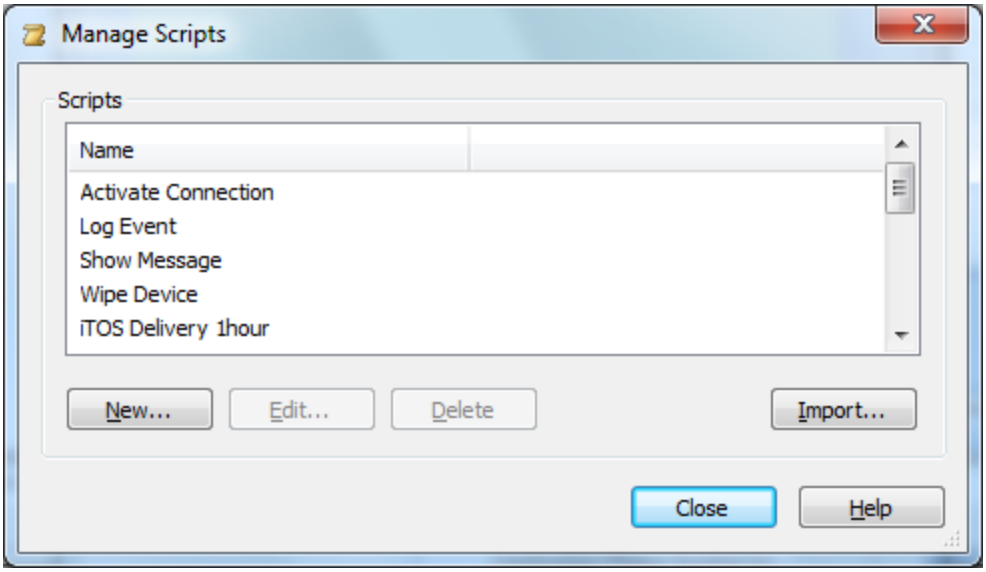
Field Name	Description
Scripts	Select a pre-built script from the drop-down menu. Clicking the **Scripts** button opens the **Manage Scripts** dialog box where you can manage scripts. Please see the "Script Manager" topic on page 141 for more information.
Queue message for delivery to offline devices	Sends the message to devices that are offline and will receive the message when they come online. The message will be stamped with the date and time it was sent.
SMS (Short Message Service)	Send the message via SMS text message. You may use a device that is connected via ActiveSync, or you may select a device that is online.
Send Using	Send a message from a device connected via ActiveSync or select an online device.
Destination Phone Number (s)	This is where the message will be delivered. This area is populated with the phone number(s) of the device you selected. Multiple phone numbers need to be separated by a semi-colon ";."

TIP:

When sending the script via SMS, hold down the CTRL key on your keyboard when clicking **OK** to view the raw text message that will be sent. You can copy this raw message into any other application or web form that facilitates SMS message delivery, for example, the website of a cellular carrier.

Script Manager

You can use the **Manage Scripts** dialog box to centrally manage all of the scripts that you are using within MobiControl. The Script Manager comes pre-built with four of the most commonly used scripts. Each one is fully customizable. The Activate Connection script connects the device to MobiControl and activates the data connection if it isn't present. The Log Event script is used to log an event with your Deployment Server. The Show Message script is used to display a message on the device, and the Wipe Device script is used to wipe the device. The scripts here are stored within the MobiControl database, and can be accessed with any MobiControl Manager console. One way to open the **Manage Scripts** dialog box is to right-click on a device or group, select **Send,** and click **Script.**

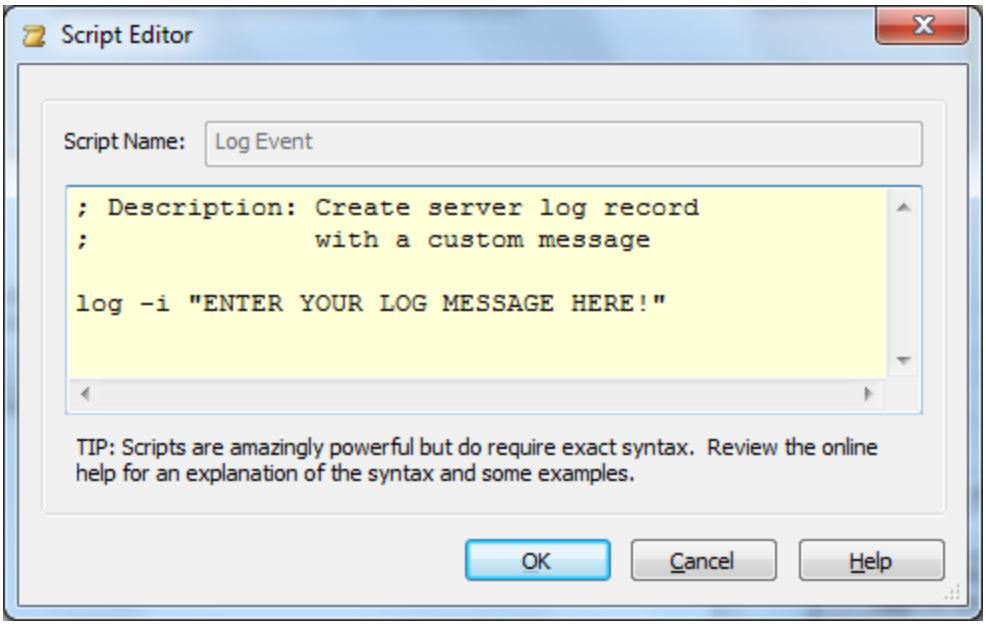


Manage Scripts dialog box

The following table describes the features of the **Manage Scripts** dialog box:

Field Name	Description
New	Creates a new script
Edit	Edits the selected script
Delete	Deletes the selected script
Import	Allows you to import a `.cmd` file containing MobiControl script commands. Please see the "Script Command Set" topic on page 72 for a full list of script commands.

Clicking the **New** button will bring up the **Script Editor** dialog box. In this window you can enter any script command that you would like to run on the device. Please see the "Script Command Set" topic on page 72 for a full list of script commands.



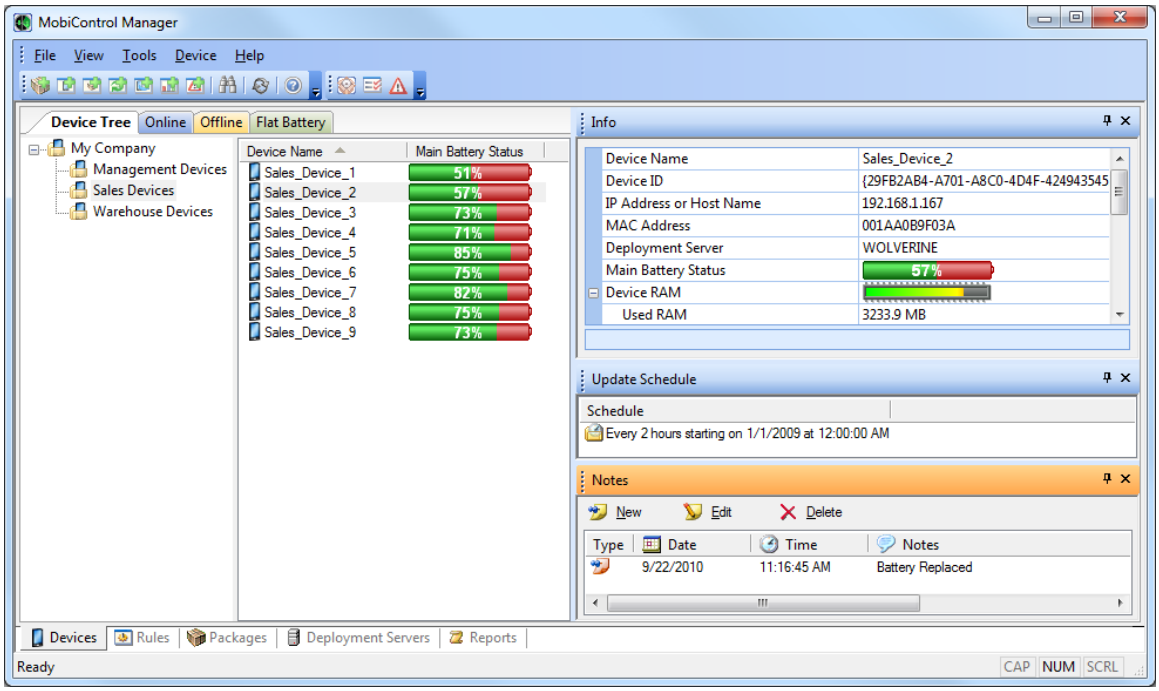
Script Editor dialog box

Device Notes

The Device Notes feature allows you to create a note for a device and archive it for future reference and tracking purposes. Each note is editable and includes the date and time when the note was added or edited. The note includes the name of the user creating the note and can be assigned different colors for color-coded categorization.

This feature is useful for creating a "trouble ticket" for help desk tracking in an end-user support or CRM (Customer Relationship Management) environment. It also allows users with access to the MobiControl Manager to document a device-specific issue and share their comments and memos related to that device with other users of the MobiControl Manager console.

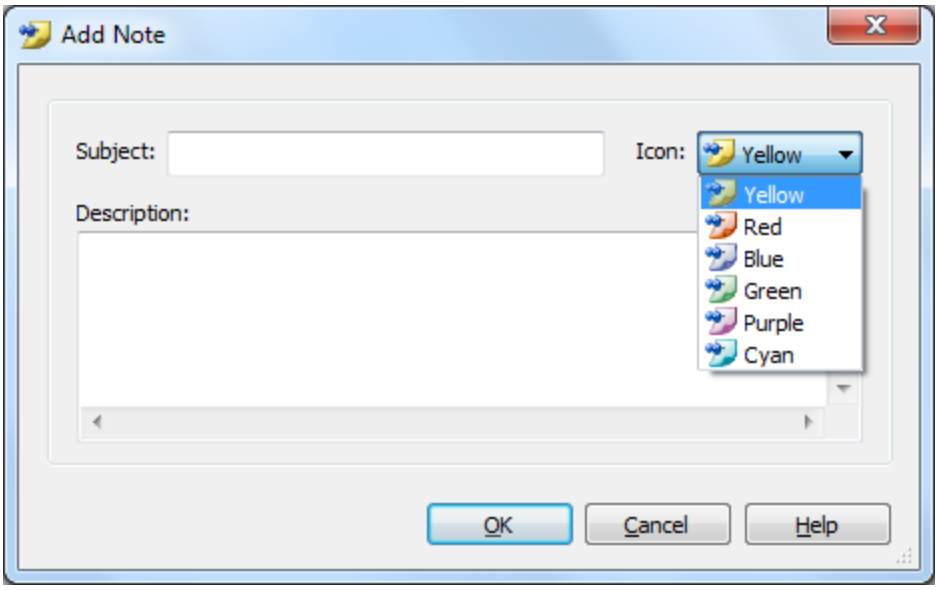
To view and edit notes for a device, select the Devices view (tab) in MobiControl Manager, and select the device. The notes for that device appear in the Notes panel.



Device Note

Adding or Editing a Note

From within the Notes panel, click **New** to add a new note for the currently selected device or click **Edit** to make changes to an existing note.



Add Note dialog box

The following table describes the fields of the **Add Note** dialog box:

Field Name	**Description**
Subject	Text entered in the subject field appears in the Notes panel as the title of the note.
Icon	You can choose different colors for the icon to adopt a color-coding to indicate different priority levels or to distinguish between different departments or users creating the note. Notes can be sorted by icon color for a categorized view.
Description	The description field is available for viewing when the note is opened. This field can contain troubleshooting notes, administrative memos or any other device-specific information.

Diagnostic Image Manager

The Diagnostic Image Manager allows you to create, view, and compare file system and registry between two previous diagnostic device images, or an online device and a previous diagnostic device image.

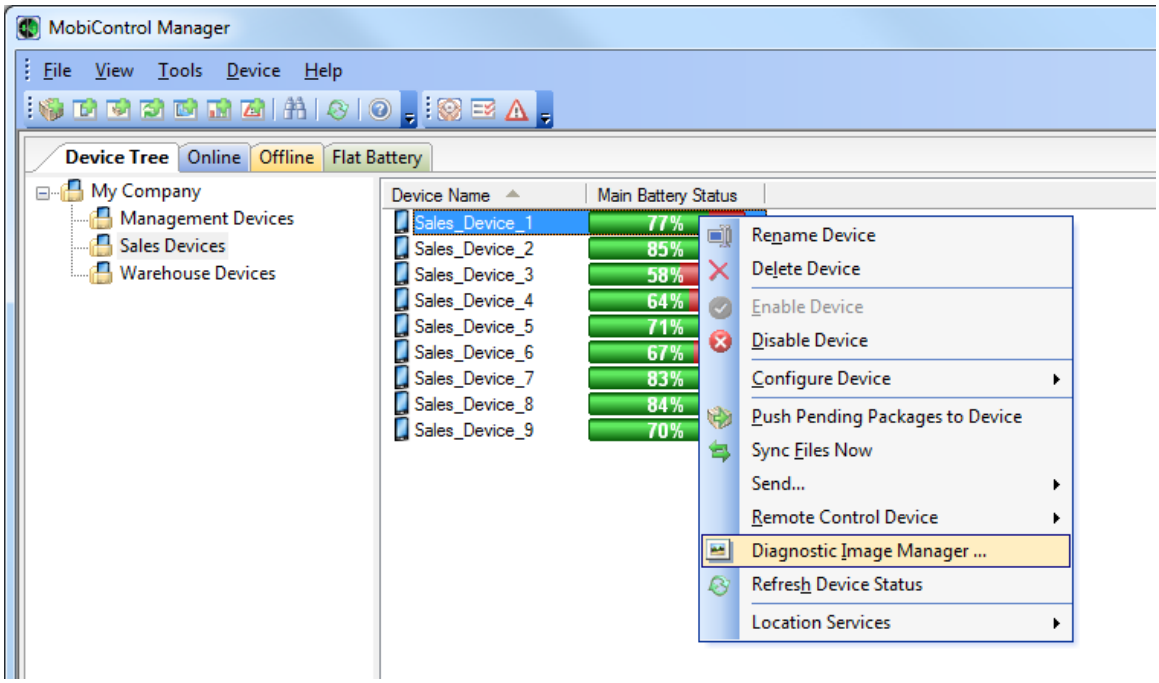
A device image is a snapshot of the mobile device's meta-data. It contains file system and registry information of the device. An image can be created when the device is online. This image is intended for diagnostic purposes and can be used to find changes in the device's file and registry structure. Once the changes are found, the necessary action can be taken and the new settings can be deployed to the devices.

The Diagnostic Image Manager can be a very useful tool which can help speed up support calls. The support personnel can use this tool to find the changes in the device in comparison to a functional device (image) and troubleshoot accordingly.

Create a Device Image

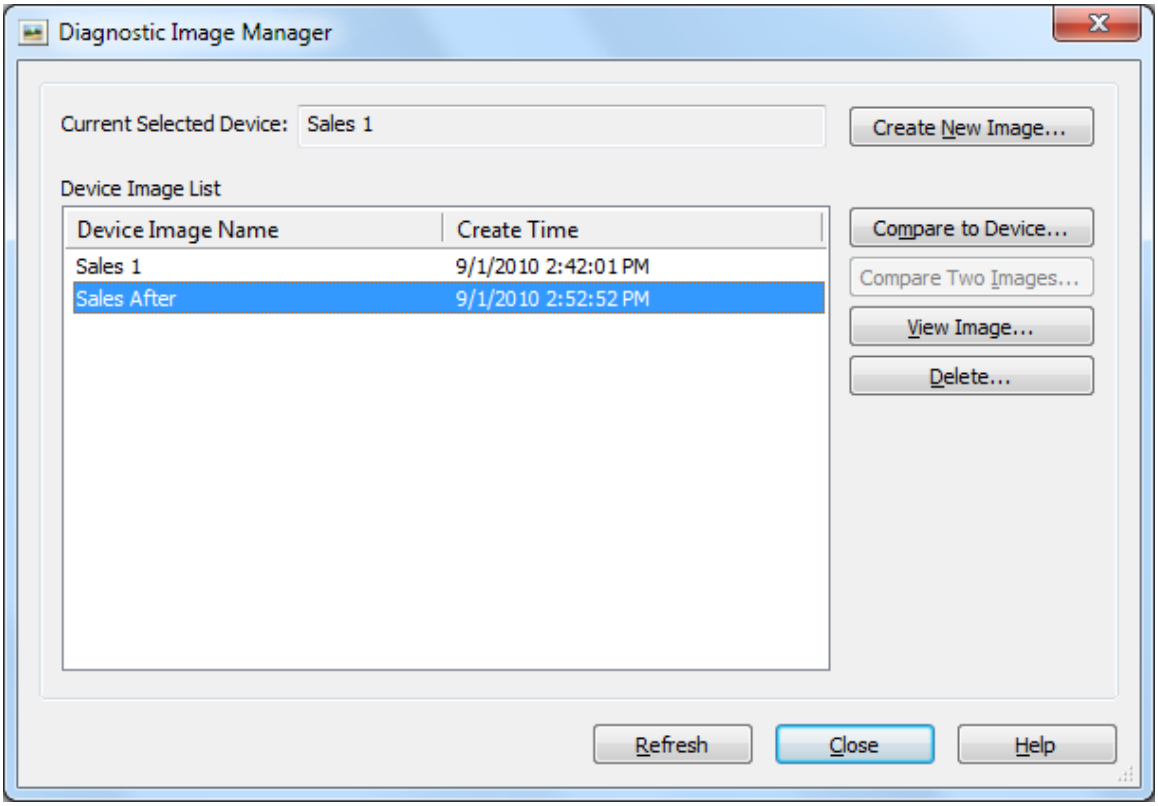
1. Open the Diagnostic Image Manager.

   Right-click an online device in the Devices view (tab), and select **Diagnostic Image Manager.**



Device menu

2. Create a device image.



Diagnostic Image Manager dialog box

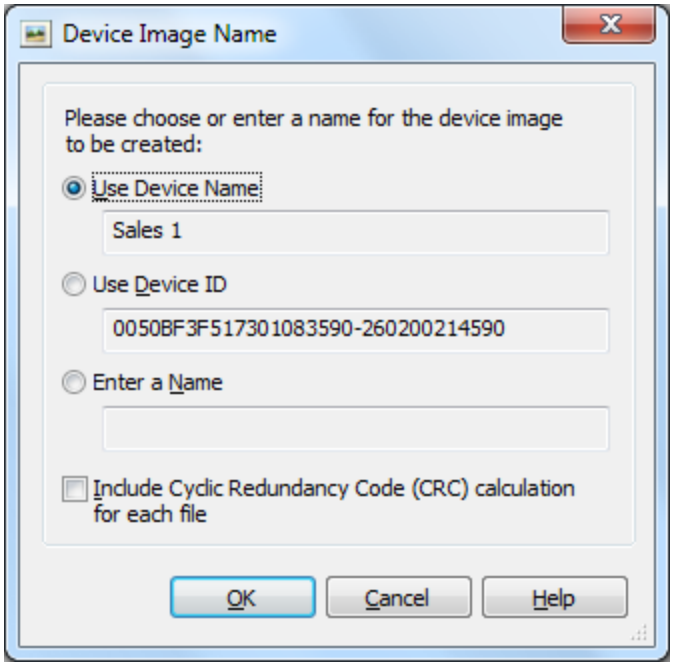
The Diagnostic Image Manager allows you to create a device image for the currently selected device and compare it with a device or a previously created device image.

Here are some common device image tasks:

- Click the **Create New Image** button to create a new device image for the currently selected device.
- Click the **Compare to Device** button to compare the selected device image with the currently selected device.
- Click the **Compare Two Images** button to compare two selected device images.
- Click the **View Image** button to view the selected device image.
- Click the **Delete** button to delete the selected device image.

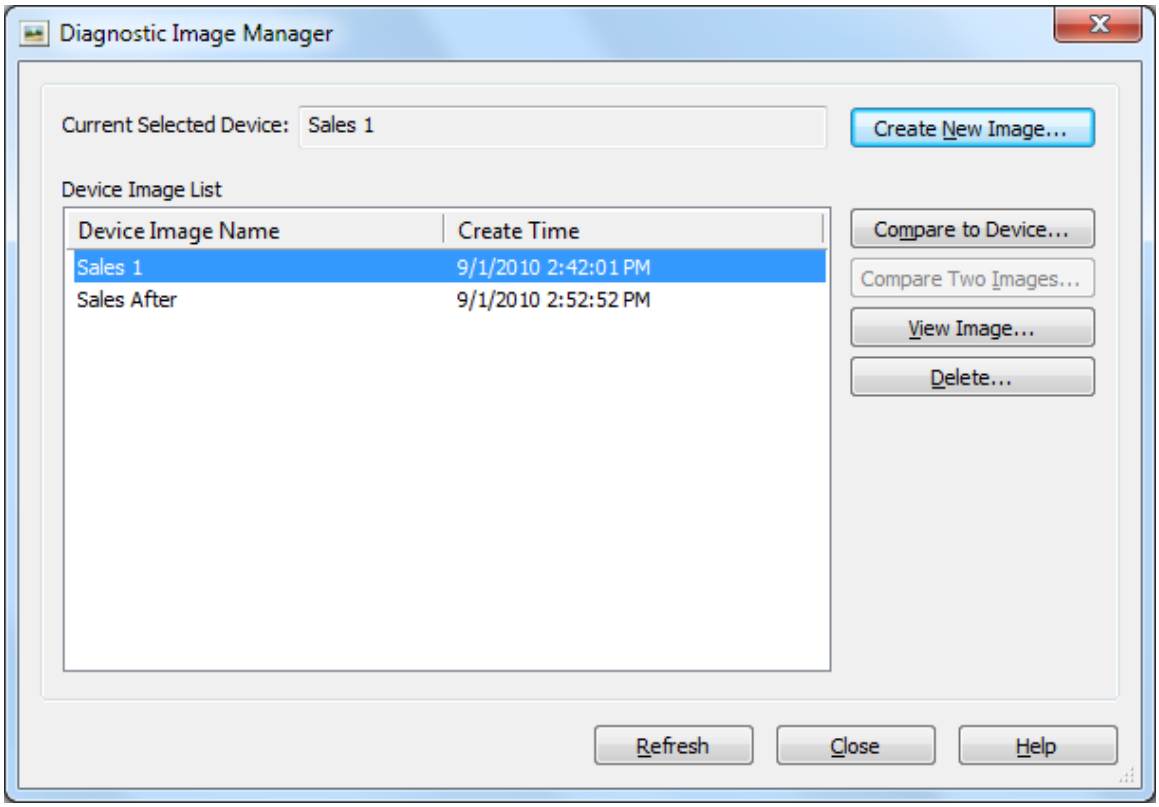
3. Choose an image name.

In the **Device Image Name** dialog box, you can choose to use the device name or device ID as the **image name**, or enter a new name.



Device Image Name dialog box

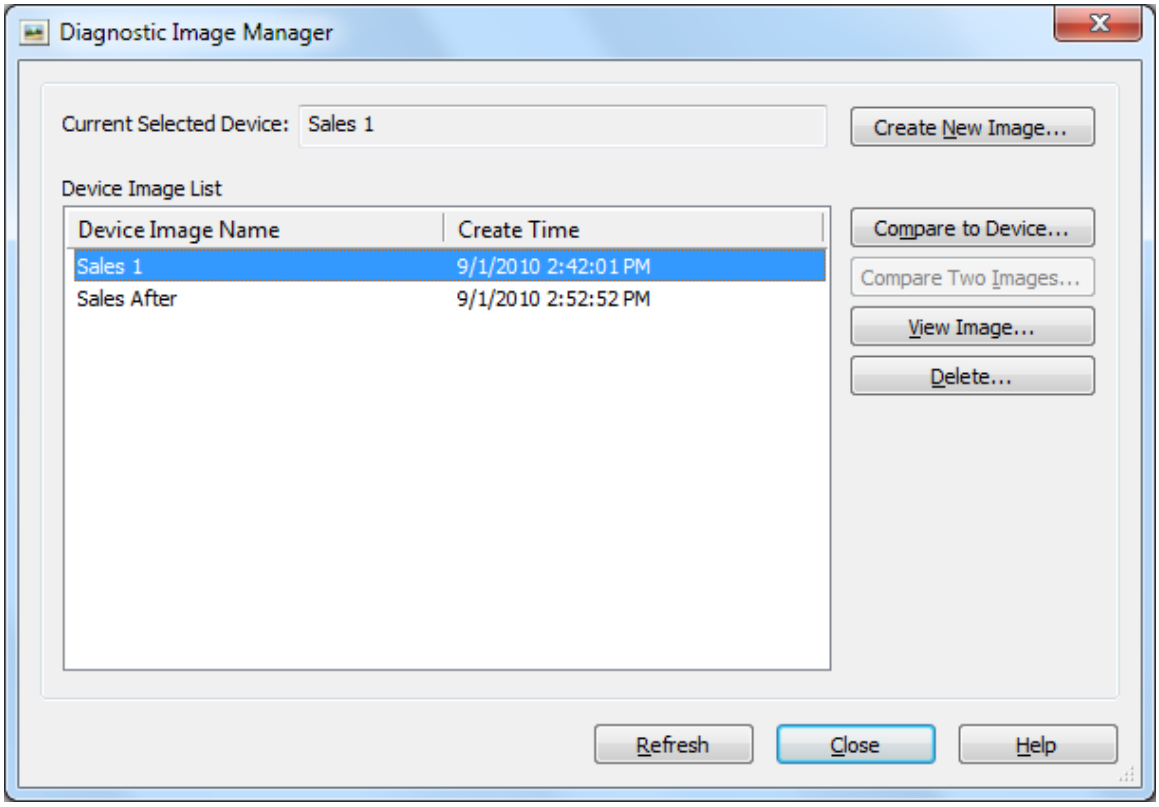
After the device image has been created, you can see it in the Device Image list in the **Diagnostic Image Manager** window.



Diagnostic Image Manager dialog box

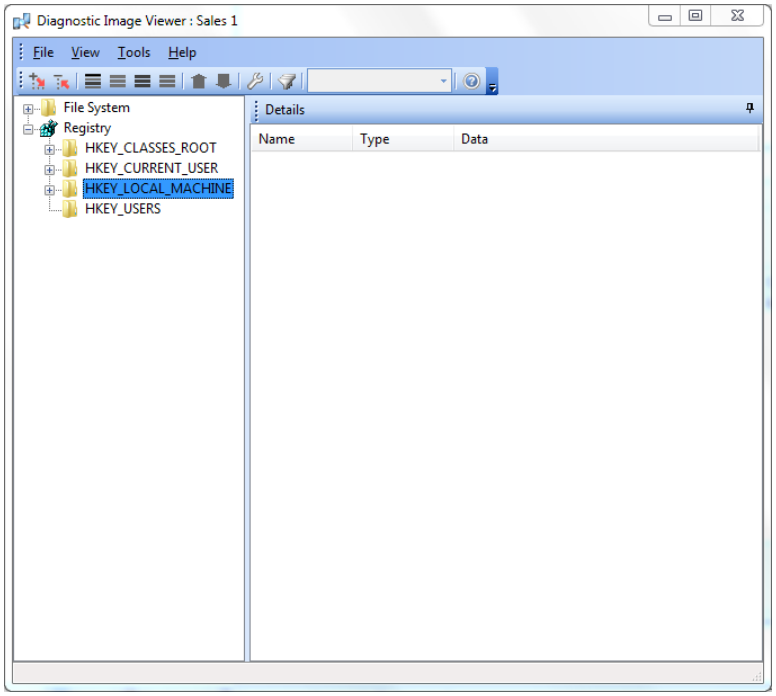
Compare a Device with a Device Image

From the Diagnostic Image Manager window, select a device image to compare, then click the **Compare to Device** button.



Diagnostic Image Manager dialog box

On the Device Image Differencing screen, you will see the resulting comparison tree. All items (files and registry keys) on the device and in the device image will be listed in the result tree. The items are displayed in different colors to differentiate them.

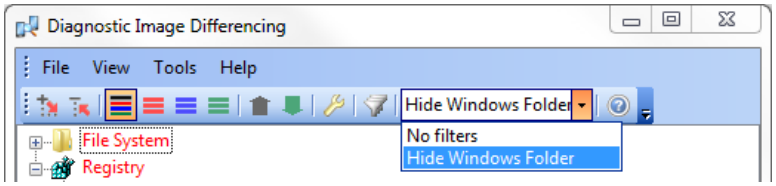


Device tree

- Items shown in red exist on both the device and in the device image, but have different attributes or properties
- Items shown in blue exist only on the device.
- Items shown in green exist only in the device image.
- Items shown in black are identical between the device and device image.

Filter Views

Custom filter views can be created in the result tree to remove common information from the comparison. This can help speed up the diagnostics as you can filter to see only the needed information only. Please see the "Diagnostic Image Comparison Filters" topic on page 153 for more information on custom filter views.

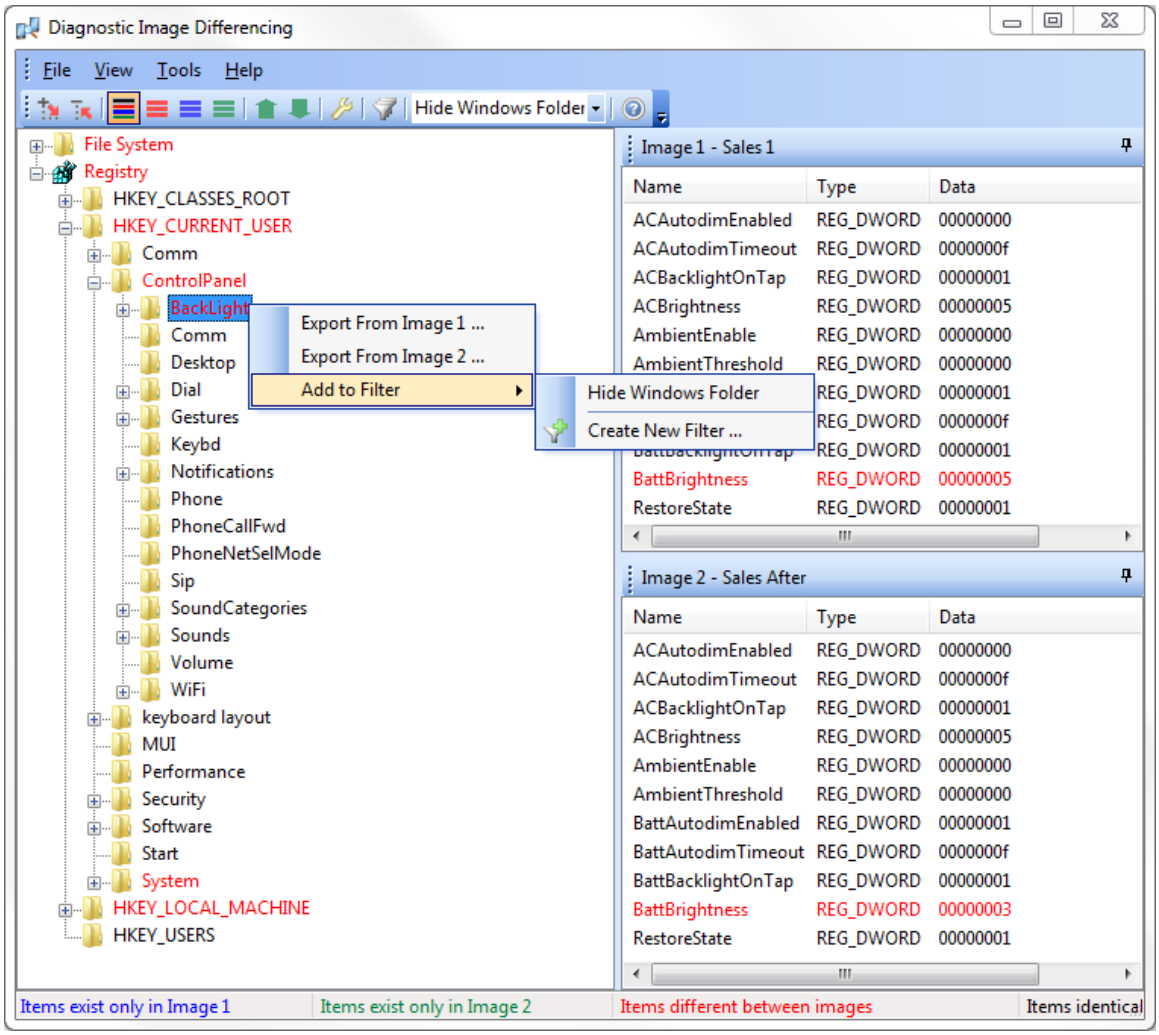


Device Image Differencing

Tree Options

There are various options available in the result tree:

- You can add files or folders from the file system and from the registry to an existing custom view filter or create a new filter.
- Under the registry tree, you have the option to export registry keys to `*.reg` files. This is the same function that is also available in the Registry Editor tool. (Please see the "Registry Tool" topic on page 44 for more information.)



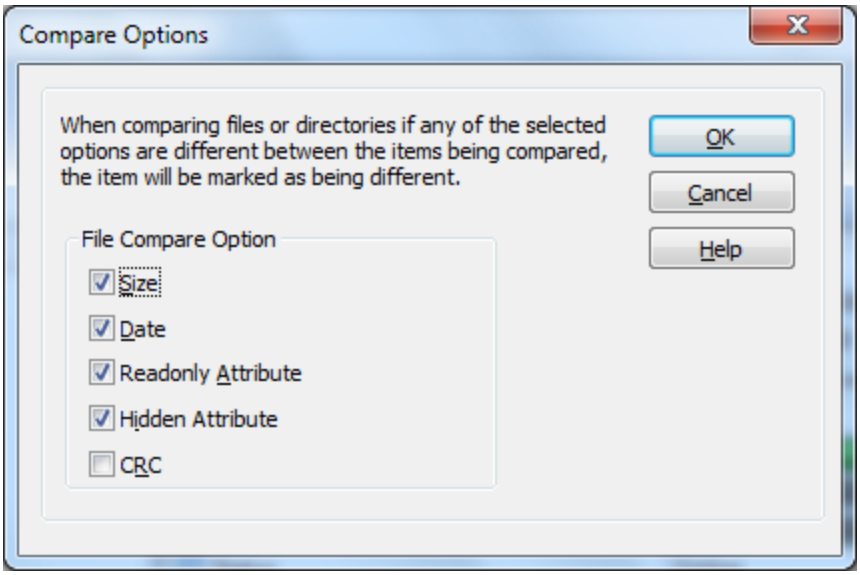
Device Image Differencing options

Comparison Options

You can choose to set options for comparisons by clicking **Tools,** and then **Options.** When comparing files and directories, there are various attributes attached to each file or directory. These attributes can now be used as parameters for comparison. Unchecking an attribute in the **Compare Options** window means ignoring it during comparison.

EXAMPLE:

If "Date" is unchecked, files that are identical except for their "Date" parameter will not appear different.



Compare Options

The following table describes the fields of the **Compare Options** dialog box:

Option	Description
Size	File size criteria will be one of the parameters used for comparison
Date	Date criteria will be one of the parameters used for comparison
Read-only Attribute	When selected, the read-only attribute criteria will be one of the parameters used for comparison.
Hidden Attribute	When selected, the hidden attribute criteria will be one of the parameters used for comparison.
CRC	A CRC (Cyclic Redundancy Check) can be used in the same way as a checksum to detect accidental alteration of data during transmission or storage. A CRC is a function that takes as input a data stream of any length and produces as output a value of a certain fixed size.

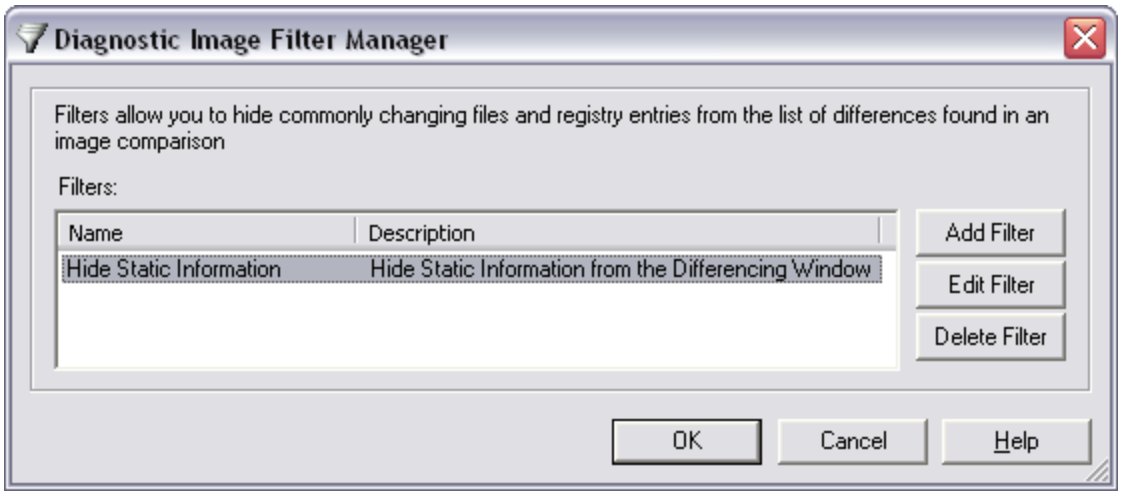
View Options

From the **View** menu, select any sub-menu item to change the current view.

- Click **Expand all** to expand all nodes in the result tree.
- Click **Collapse all** to collapse all nodes in the result tree.
- Click **Show all** to show all items in the result tree.
- Click **Show difference between device and image** to identify items existing on both, but that have different attributes or properties.
- Click **Show items existing only on device** to do so in the result tree.
- Click **Show items existing only in image** to do so in the result tree.

Diagnostic Image Comparison Filters

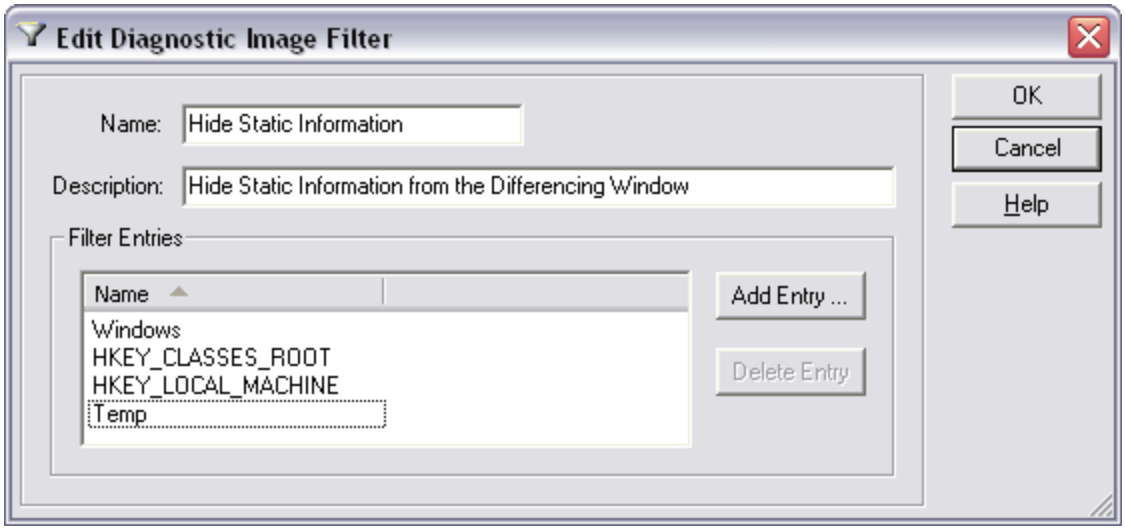
The diagnostic image comparison filter allows you to create customized filter views that can filter out information and hide information from the Diagnostic Image Differencing window. In this custom filter view, you will only see the relevant information that you want to see.



Diagnostic Image Filter Manager dialog box

To create a new filter, click **Tools,** then click **Filter Manager** in the Device Image Differencing window.

Feature	Description
Add Filter	Select this button to create a new filter. The **Edit Filter** dialog box will be displayed.
Edit Filter	Select this button to edit an existing filter. The **Edit Filter** dialog box will be displayed.
Delete Filter	Select this button to delete an existing filter.



Add Diagnostic Image Filter dialog box

Adding, Deleting, or Editing a Device Filter

In the **Diagnostic Image Filter Manager** dialog box:

- Click **Add Filter** if you wish to add a new filter.
- Click **Delete Filter** if you'd like to delete a filter.
- Click **Edit Filter** if you wish to edit an existing filter.

Adding a New Filter

Upon clicking **Add Filter,** the **Edit Diagnostic Image Filter** window will open up.

1. Give a name to this filter.
2. Enter a brief description.
3. Click **Add Entry.**
4. In the pop-up window, select the files or folders from the file system. You can also select registry keys (both individually and at group level).
5. Click **OK** once selection is complete. You will see the newly-added filter in the Filter Manager window.

Editing an Existing Filter

Upon clicking **Edit Filter,** the **Edit Diagnostic Image Filter** window will open up.

- You have the option to add a new entry in the **Filter Entries** or delete an existing entry.
- To add an entry, click **Add Entry** and follow the guidelines above.
- Select the filter from the top of the Diagnostic Image Differencing window. The data is now filtered.

Configuring Devices

There are eight main aspects to device configuration. Each of these settings can be configured for a single device or applied at the device group level thereby configuring a set of devices. When the devices are moved from one device group to another in the device tree, the settings for the new device group are applied automatically to the devices. Please see the "Device Relocation Rule" topic on page 335 for more information on automatically re-configuring devices based on their location (using IP address or other custom criteria).

Remote Control Settings

Select a device skin to display in the MobiControl Remote, and choose the connection profile to use when remote controlling the device. This allows for customized remote control settings, optimised for different types of connections, for instance, high-speed Wi-Fi or low-speed cellular connections). Please see the "Remote Control Settings" topic on page 158.

Device Update Schedule

Adjust the interval at which the mobile devices contact the Deployment Server for new updates, configuration changes and packages. Please see the "Device Update Schedule" topic on page 160.

Device Exchange ActiveSync

Configure Exchange ActiveSync settings for your mobile device. Please see the "Device Exchange ActiveSync" topic on page 163.

Deployment Server Priority

This option allows you to specify the Deployment Server preferences for the devices. When a device is configured with more than one Deployment Server, it will try to connect to highest priority one first and if this server is not accessible, then it will try to connect to the next server available. Please see the "Deployment Server Priority" topic on page 167.

Advanced Settings

This option allows you to configure advanced settings for your mobile device(s), via. configure connection security by enabling or disabling SSL, select connection mode between persistent, scheduled and manual, change connection retry interval and set log file management, among other options. Please see the "Advanced Settings" topic on page 168.

Device Time Synchronization

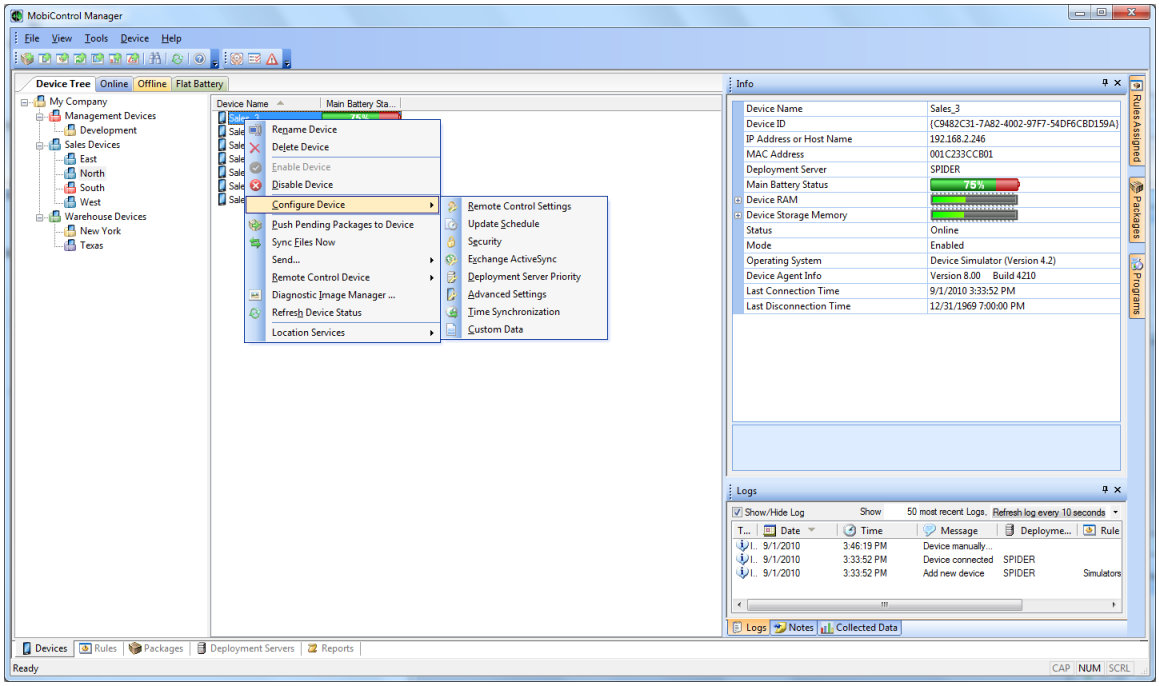
This option allows you to enable time synchronization for a mobile device, allowing the device to update its date and time settings by periodically synchronizing them with an SNTP/NTP time server or the MobiControl Deployment Server. Please see the "Device Time Synchronization" topic on page 173.

Custom Data

This option allows you to create your own monitoring fields to be shown in the Device Info window. This can be useful for monitoring various aspects of third-party applications. Please see the "Custom Data" topic on page 175.

Device Security and Control

Configure security settings for mobile devices including device lockdown for operating the devices in a kiosk mode and restricting web browsing to specific websites, user login and authentication policies, application control to restrict the applications and processes that are allowed to run on the devices, file encryption for the device and storage card file system and device-side security scripts. Please see the "Device Security and Control" topic on page 183.

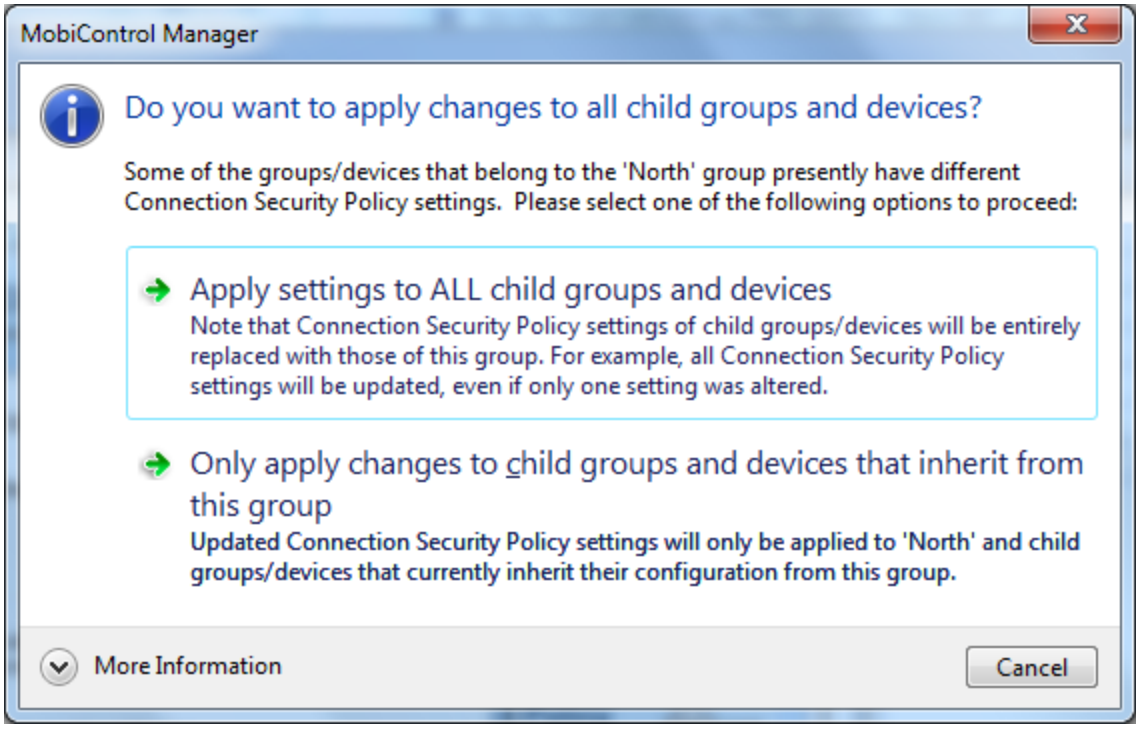


Device Configuration Menu options

Configuration Override Settings

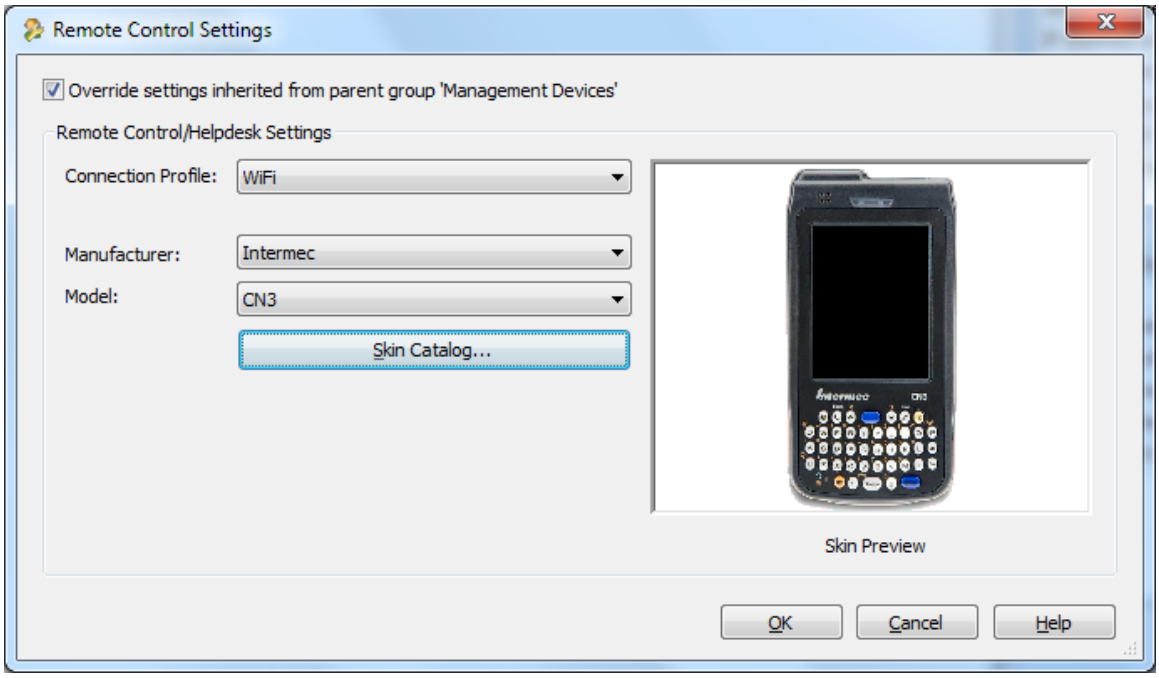
Override settings allows you to create unique configuration settings at the current level which you have selected. This will override the settings that the device or group was previously inheriting from the parent group.

If the configuration settings are different at any sublevel (be it device or subgroup) then a confirmation prompt will allow you to choose whether the current setting(s) should be applied to all sub devices and groups or only the level that inherit configurations from this group.


MobiControl Manager
Do you want to apply changes to all child groups and devices?
Some of the groups/devices that belong to the 'North' group presently have different Connection Security Policy settings. Please select one of the following options to proceed:
Apply settings to ALL child groups and devices
Note that Connection Security Policy settings of child groups/devices will be entirely replaced with those of this group. For example, all Connection Security Policy settings will be updated, even if only one setting was altered.
Only apply changes to child groups and devices that inherit from this group
Updated Connection Security Policy settings will only be applied to 'North' and child groups/devices that currently inherit their configuration from this group.
More Information
Cancel

Remote Control Settings

In the **Remote Control Settings** dialog box, it's possible to select a device skins and connection profiles.



Remote Control Settings dialog box

The following table describes fields in the **Remote Control Settings** dialog box.

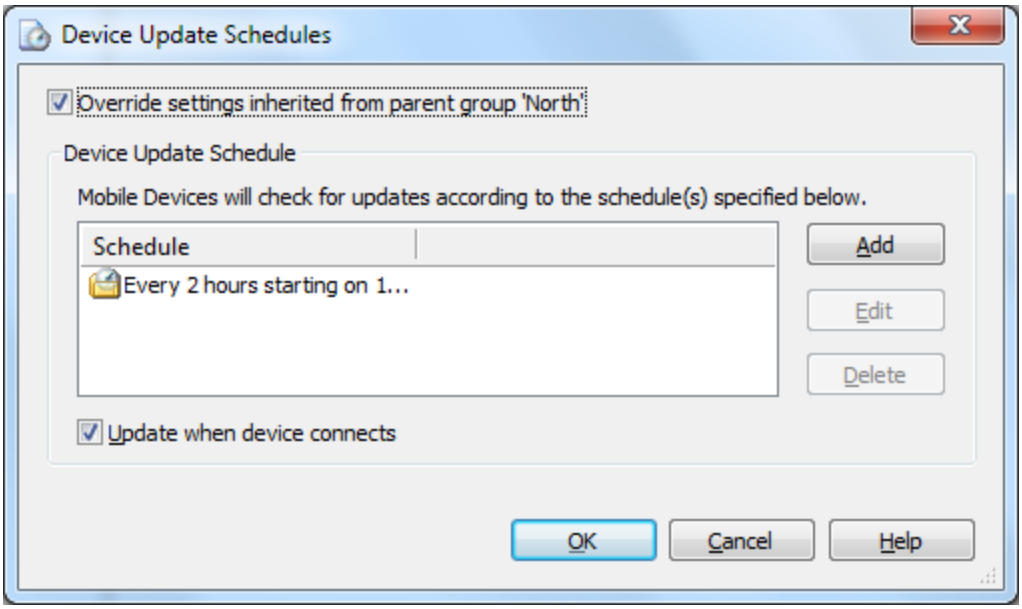
Field Name	Description
Connection Profile	This field allows the user to configure the type of connection that will be used for remote control sessions. The available connection types are TCP/IP(SERVER) **(recommended)**, TCP/IP(DIRECT), and <Prompt on Connect>. • The **TCP/IP(SERVER)** setting offers the broadest support for remote control connections. For example, situations where the mobile device does not have a public IP address. When a TCP/IP(SERVER) remote control session is established, the session is bridged through the MobiControl Deployment Server (i.e. The device connects to the MobiControl Deployment Server on TCP port 5494 and the desktop MobiControl Remote client connects to the Deployment Server on TCP port 5494). Since this connection goes through the Deployment Server the performance is generally not as fast as a direct TCP/IP connection, however, it offers improved security as it does not require the mobile Device Agent to accept unauthenticated remote control connections. An example of where this type of connection is required because of network topology is when the mobile devices are behind a firewall and do not have unique public IP addresses. • With the **TCP/IP(DIRECT)** setting, the MobiControl desktop software will open a direct Wireless/Wired TCP/IP connection to the mobile device (i.e. on TCP port 5494). A LAN-based wired/wireless TCP/IP connection generally provides the best performance, however it requires that the mobile Device Agent accept unauthenticated remote control connections unless SSL Security is enabled. Please see the "Communication and Connection Security" topic on page 411. • If you choose the **<Prompt on Connect>** option, then you will be asked to choose the connection profile you wish to use each time you initiate a TCP/IP-based remote control session.
Manufacturer, Model, and Skin Preview	A skin is an image of the body of your mobile device, which mimics the physical device on your desktop screen. Displaying your device in a skin gives you access to most of the physical buttons of the device. It can be useful in training or presentations. Select the manufacturer and model of your device to have its skin be displayed in a remote control session. If you are using MobiControl for the first time, you will need to download the skin for your device from our website. This is done by clicking the **Download Skins** button. Clicking this button will bring up the skin catalog which lists all currently available skins. (Please see the "Skin Catalog" topic on page 101.) Skins for most Windows Mobile, Pocket PC and CE .NET based mobile devices are available. We are always adding new skins to our online collection, but if your device is not listed, please contact us to let us know which device you are using.

Device Update Schedule

The device update schedule specifies when the device(s) should query the Deployment Server(s) for updates. Updates may include the addition, update, or removal of packages and modifications to device settings.

If the Deployment Server determines there are pending updates for the device, it immediately sends them to the device. The device also sends the Deployment Server a summary of its installed packages and settings. If the Deployment Server identifies an inconsistency, such as a previously-installed package that is missing on the device, the Deployment Server will re-install the package.

The initial device update schedule is specified by the add devices rule used to add the device(s) to the system. You may edit the schedule for an individual device or a group of devices that have been added to the system by selecting the target device or group in the device tree view in the main console window and selecting **Update Schedules** from the **Configure Device(s)** sub-menu.



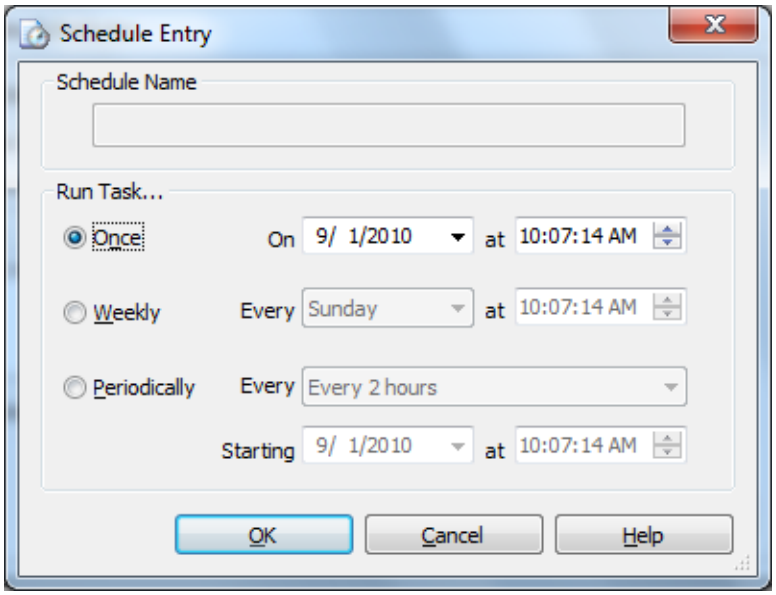
Device Update Schedules dialog box

The following table describes the **Device Update Schedules** dialog box:

Field Name	Description
Add	Select **Add** to specify additional update intervals. The **Schedule Entry** dialog box will be displayed. **EXAMPLE:** To sync a device twice a week, Monday at 06:00 and Friday at 19:00, create two weekly schedule entries.
Edit	Select **Edit** to modify an existing schedule entry. The **Schedule Entry** dialog box will be displayed.
Delete	Select **Delete** to permanently remove an update schedule entry from the dialog box.
Update when device connects	Select this check box to have the device(s) check for updates whenever they connect to a Deployment Server, that is, at every transition from offline to online. If this check box is not selected, the device(s) will only check for updates according to the schedule defined above.

Schedule Entry

The **Schedule Entry** dialog box allows you to specify schedule entries as one-time or periodic events.



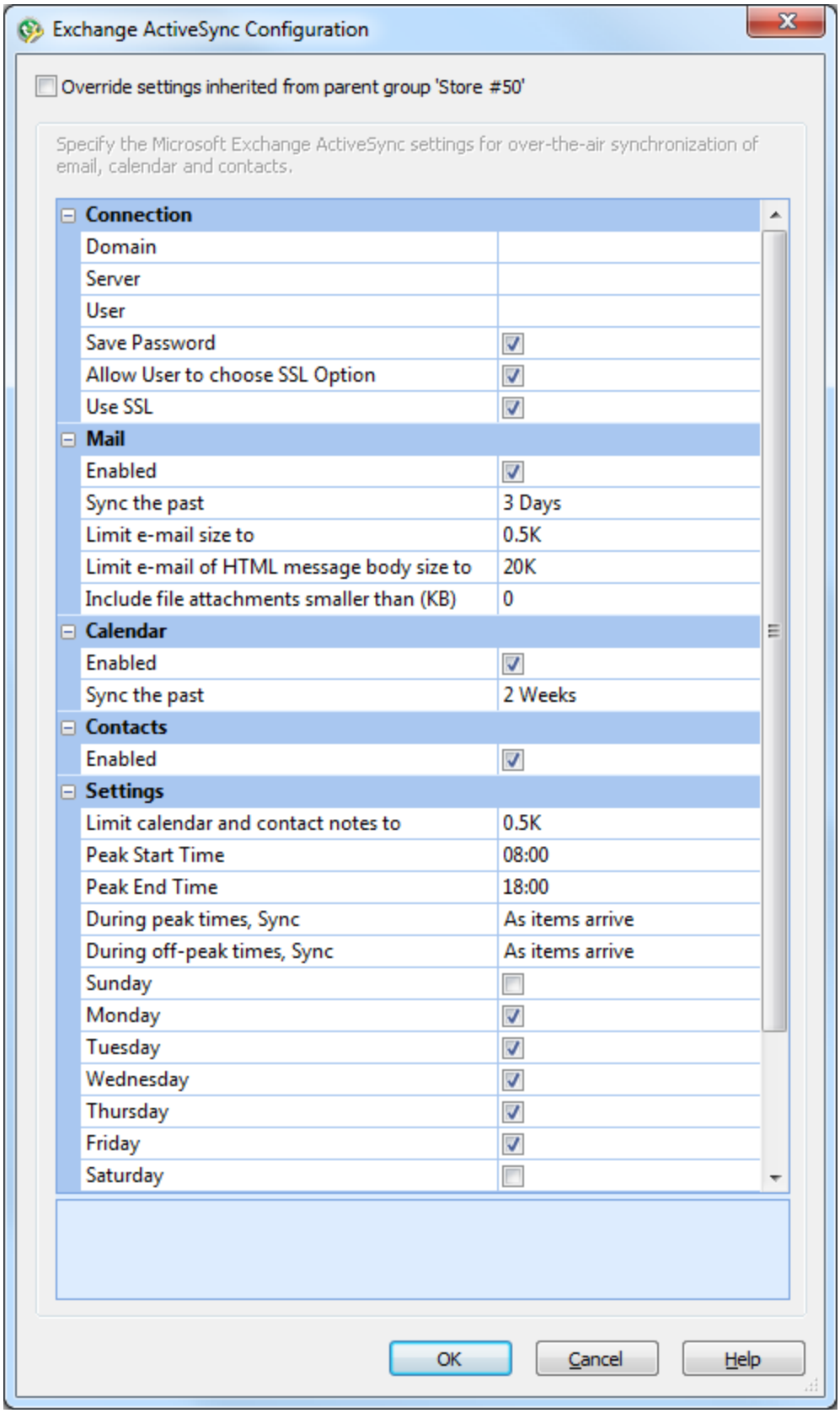
Schedule Entry dialog box

Field Name	Description
Once	The device will check for updates once at the specified date and time.
Weekly	The device will check for updates once a week, on a specific day at a specific time.

Field Name	Description
Periodically	The device will check for updates periodically, at the specified interval from the set start date and time.

Device Exchange ActiveSync

With MobiControl, you can now configure Microsoft Exchange ActiveSync settings for your mobile device. To arrive at this configuration menu, select the device or the group, right-click, select **Configure Device(s)**, and click **Exchange ActiveSync**.


Exchange ActiveSync Configuration
Override settings inherited from parent group 'Store #50'
Specify the Microsoft Exchange ActiveSync settings for over-the-air synchronization of email, calendar and contacts.
Connection
Domain
Server
User
Save Password
Allow User to choose SSL Option
Use SSL
Mail
Enabled
Sync the past
3 Days
Limit e-mail size to
0.5K
Limit e-mail of HTML message body size to
20K
Include file attachments smaller than (KB)
0
Calendar
Enabled
Sync the past
2 Weeks
Contacts
Enabled
Settings
Limit calendar and contact notes to
0.5K
Peak Start Time
08:00
Peak End Time
18:00
During peak times, Sync
As items arrive
During off-peak times, Sync
As items arrive
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
OK
Cancel
Help

Connection Options

Field Name	Description
Domain	Enter the domain name of your organization.
Server	Enter the server address of your organization.
User	Enter the user name for your Exchange email account.
Save Password	Check this box if you wish to have your password saved. If this box is unchecked, you will be asked to enter the password each time you perform synchronization. Also, this box must be checked for push email synchronization.
Allow User to use SSL Option	This option allows the end user to select whether or not SSL is used for communication with the Exchange server.
Use SSL	This option enables the SSL protection on the connection.

Mail Options

Field Name	Description
Enabled	This option will enable email synchronization.
Sync the past	This option will synchronize all email entries for the past up to the specified number of days.
Limit e-mail size to	This option will control the maximum amount of data in the email message that can be used during email synchronization.
Include file attachment size smaller than (KB)	Any email with attachments smaller than the specified size, will be downloaded to the device upon synchronization.

Calendar Options

Field Name	Description
Enabled	This option will enable calendar synchronization.
Sync the past	This option will synchronize all calendar entries for the past up to the specified number of days.

Contacts Options

Field Name	Description
Enabled	This option will enable synchronization of contacts.

Settings Options

Field Name	Description
Limit Calendar and Contact Notes to	This option will control the maximum amount of data that can be used during calendar notes and contacts notes synchronization.

Field Name	Description
Peak Start Time	This time specifies the beginning of the peak service for peak days.
Peak End Time	This time specifies the end of the peak service for peak days.
During Peak Times, Sync	This option specifies how frequently synchronization should occur during peak times.
During Off-Peak Times, sync	This option specifies how frequently synchronization should occur during off-peak times.
Sun / Mon / Tue / Wed / Thu / Fri / Sat	Select the days you want to include in your peak-time synchronization schedule
Sync when roaming	This option will allow automatic synchronization for the mobile device even when it is using a roaming data service.
Send outgoing items immediately	When sending items from the mobile device, you have a choice to send it immediately or after a delay. This option controls this setting to send items immediately or after a delay.
Delay sending messages (seconds)	This option specifies the time interval for the delay when sending an email from the mobile device

Tasks Options

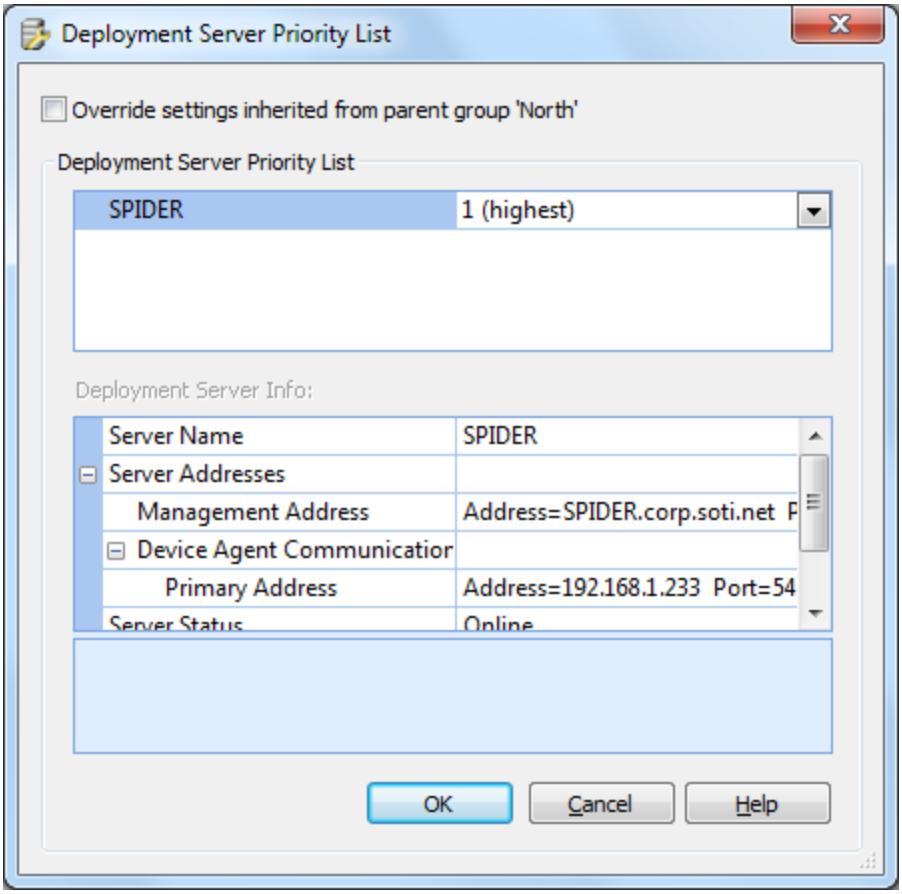
Field Name	Description
Enabled	This option will enable synchronization of tasks.

NOTES:

- It is recommended that you set up an authentication policy using Active Directory-based user authentication prior to using this feature. MobiControl will automatically set the user name when the Exchange settings are pushed down. You should leave the user name field below blank in this case, and MobiControl will automatically fill it in.
- If you need to deploy a certificate to the device (because the Root Certificate Authority certificate is not already in the devices certificate store), then you should do so using a package that includes a script to install it. Please see the "Script Command Set" topic on page 75.

Deployment Server Priority

The **Deployment Server Priority List** dialog box allows you to specify the Deployment Server preferences for the devices. Priority one is the highest and five is the lowest. When a device is configured with more than one Deployment Server, it will try to connect to highest priority one first. If this server is not accessible, then it will try to connect to the next server available.



Deployment Server Priority List dialog box

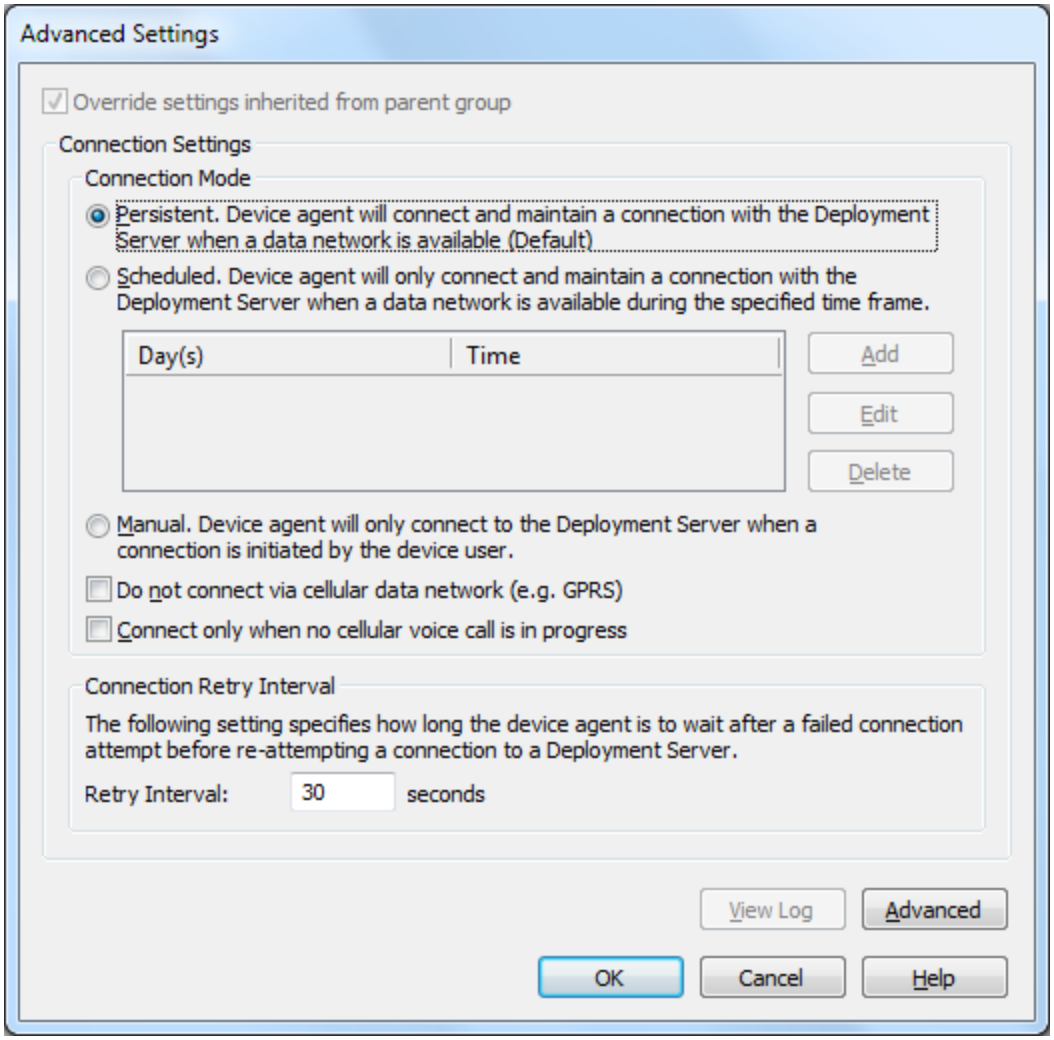
Multiple servers may be assigned the same priority level to establish a pool of Deployment Servers to balance the load of a large number of devices.

If you select "Not used," the selected devices will not connect to that Deployment Server.

Deployment Server priority is only applicable when you have installed multiple Deployment Servers using the same site name. Please see the "Configuring MobiControl Manager" topic on page 399 for more information.

Advanced Settings

To access the **Advanced Settings** dialog box, right-click on a device or device group, point to **Configure Device(s),** and select **Advanced Settings.**



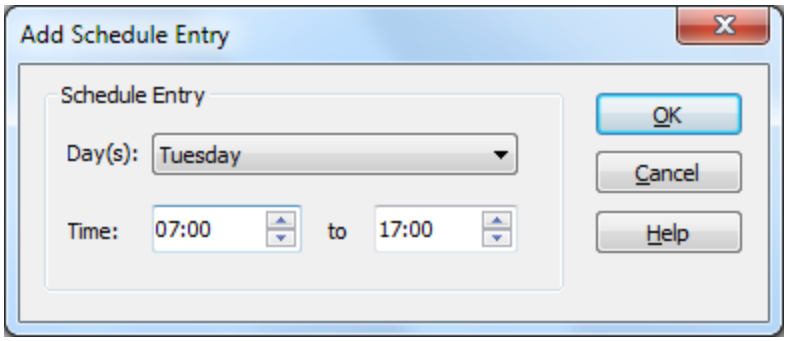
Advanced Settings Connection Settings tab

Connection Mode

In any connection mode, the Device Agent does not force the mobile device to establish a network connection; it only takes advantage of an existing network connection.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Persistent</td><td>In this mode of operation the Device Agent will persistently try to establish and maintain a TCP/IP connection with the Deployment Server. This maximizes the amount of time the device is connected to MobiControl, ensuring that it is able to quickly receive updates and available for remote control.
This is the recommended mode of operation for most installations.</td></tr>
<tr><td>Scheduled</td><td>In this mode of operation the Device Agent will only attempt to establish and maintain a TCP/IP connection with the Deployment Server during the defined time periods. Within the set time periods, the Device Agent operates in a "persistent" mode. Outside of the set time periods, the Device Agent will remain disconnected from the Deployment Server unless a connection is manually initiated by the device user.
This is the recommended mode of operation for installations where it is not necessary for the device to always be connected to the Deployment Server.
It is important that the time frame configured takes into consideration the device update schedule, and file synchronization schedules. These schedules can only be executed when the device is connected to the Deployment Server.
TIP:
If you are experiencing aggressive battery consumption with the persistent connection mode, switch to the Scheduled mode, and specify a narrow time frame (e.g. 1–2 hours)</td></tr>
<tr><td>Manual</td><td>In this mode of operation the Device Agent will never automatically attempt to establish a connection to the Deployment Server. Connections must be initiated by the device user via the device configuration applet.
This is the recommended mode of operation for installations where only the remote help desk facilities of MobiControl are being used (not using deployment rules or file sync rules), and it is acceptable and/or required that the device user initiate the connection to the Deployment Server.
NOTE:
The device must be connected to the Deployment Server in order for a remote help desk session to be established via the "TCP/IP(SERVER)" profile.</td></tr>
<tr><td>Do not connect via cellular data network</td><td>This option prevents the MobiControl Agent from connecting to the server via a data network on the device, e.g. GPRS. It can still connect using any other connection, e.g. Wi-Fi.
Don't use the Connect button on the Device Agent to test the device connection, since the MobiControl Manager (when the setting is implemented) will always allow a connection through GPRS. Instead you can use Disable device then Enable device on the MobiControl Manager to see if the device can connect through GPRS.</td></tr>
</table>

Option	Description
Only connect when no voice call in progress	When a voice call is in progress on a cellular phone device, the data service may or may not be available. To prevent the Device Agent from attempting to establish a connection while a voice call is in progress select this checkbox.

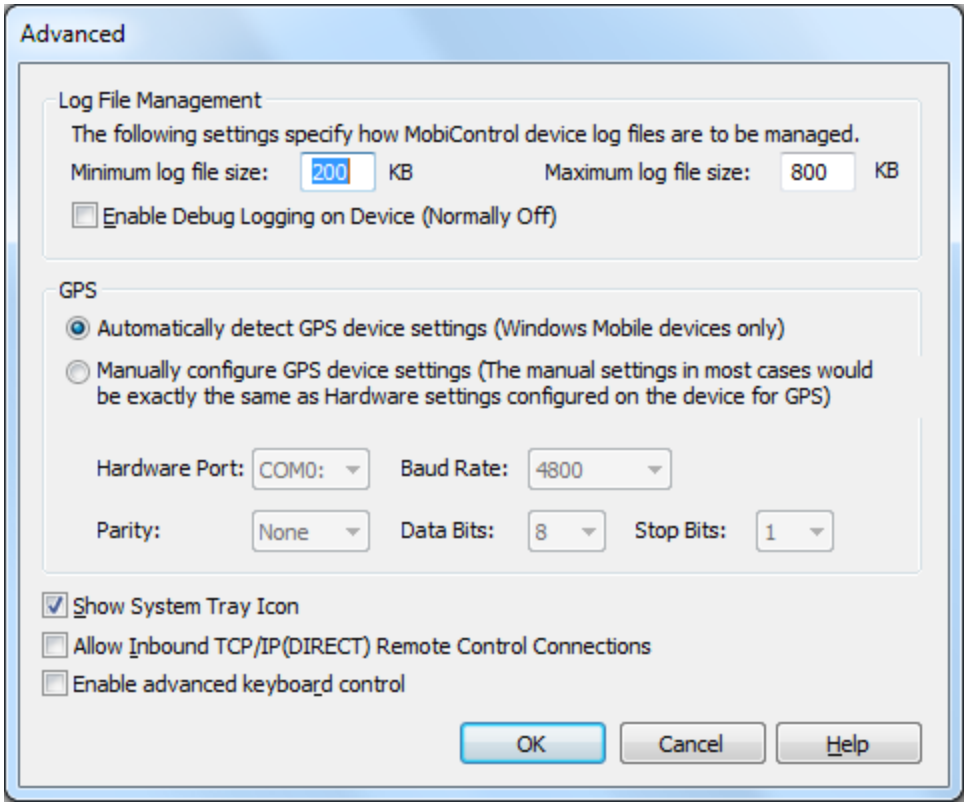


Add Schedule Entry settings dialog box

Connection Retry Interval

This setting determines how long the Device Agent should wait before trying to contact the Deployment Server again after a failed attempt. If your device will experience long periods disconnected from the Deployment Server, you should set this value high in order to prevent battery drain.

Option	Description
Allow Inbound TCP/IP(DIRECT) Remote Control Connections	This box needs to be checked if you intend to connect to your mobile device using the **TCP/IP (DIRECT)** connection mode. This option will enable the **Allow Inbound TCP/IP Connections** option in the Device Agent on the mobile device.



Advanced Settings Advanced tab

Advanced Device Agent Configuration

This set of options allows you to tune how the debug log files are managed on the device. Log management works by waiting for the log file to grow to a maximum threshold. Once the given threshold is met, the log file size is reduced down to the given minimum threshold by purging all the older entries.

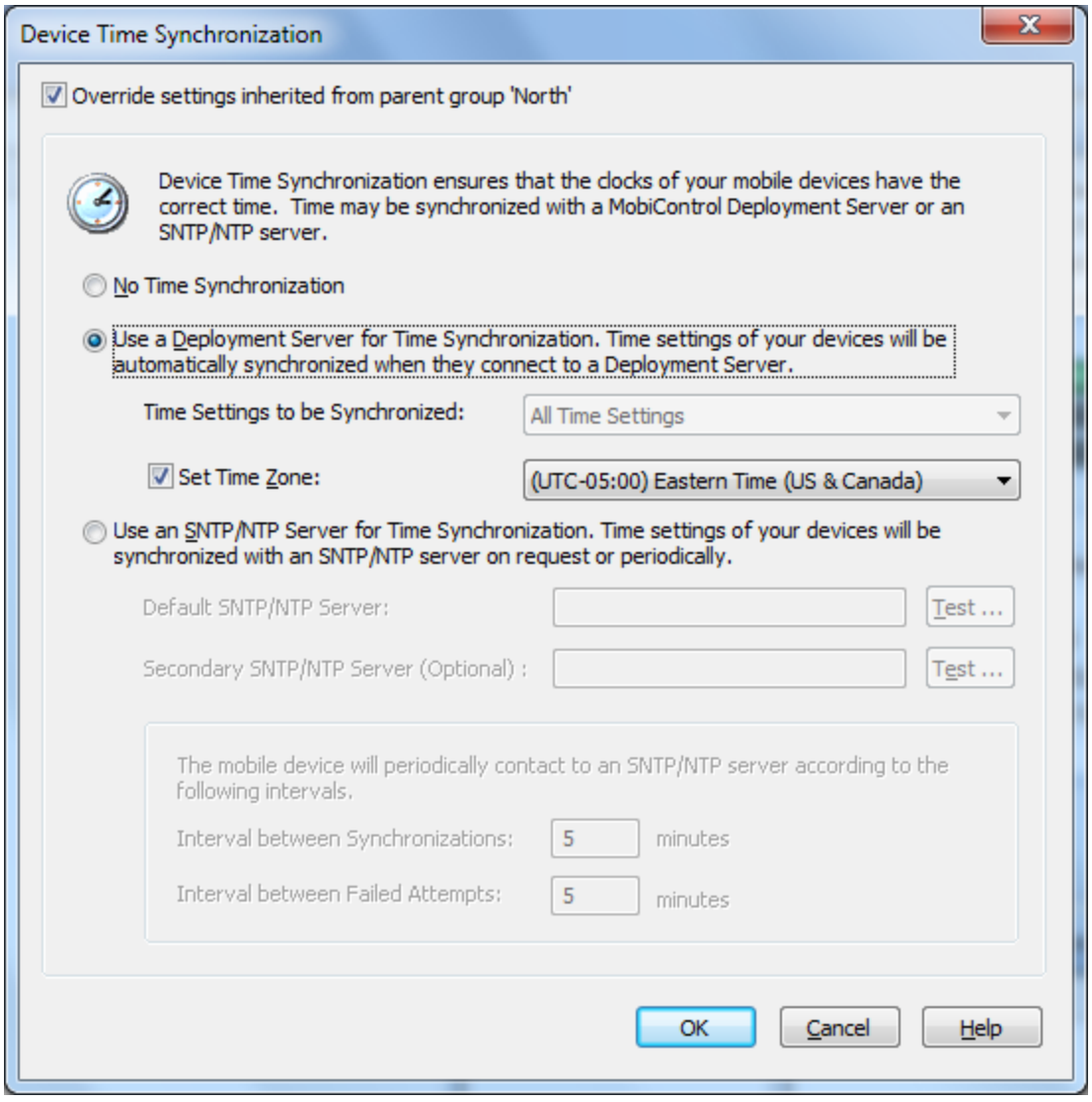
Option	Description
Minimum Log File Size	Threshold size up to which the log file will be purged.
Maximum Log File Size	Threshold size, reaching which will trigger the log file to be purged to the minimum log file size
Enable Debug Logging (Normally Off)	Enables event logging on the mobile device. All MobiControl-related activity and events will be logged to a log file.The log file can provide vital information to IT support staff in diagnostics and resolving any issues that might have been reported for the mobile device with respect to MobiControl. The mobile device may operate more slowly with this option checked. **IMPORTANT:**

Option	Description
	Debug logs generate a large amount of file system traffic and as such, should only be enabled when you are debugging a problem. In particular, on Windows Mobile 5 devices, this intense logging activity can reduce the life of your flash memory if left on indefinitely.
Automatically Detect GPS Device	Automatically Detects the devices GPS settings, and uses those to locate the Device.
Manually Configure GPS Device	Enter the GPS Configuration settings for your specific devices. These settings can be obtained from the device manufacturer if you are un aware of them.
Show System Tray Icon	Enables the MobiControl Agent icon to be displayed on the device's system tray
Allow Inbound TCP/IP Connections	Enable the agent to listen and accept inbound TCP/IP remote control connections. When unchecked, you can remote control this device through "Remote Control Device via TCP/IP (SERVER)," but you cannot remote control this device by through "Remote Control Device via TCP/IP (DIRECT)."
Enable Advanced Keyboard Control	Enables the hardware keys on the device to be used by third party applications when the lockdown is engaged.

Device Time Synchronization

This feature allows you to enable time synchronization for a mobile device, allowing the device to update its date and time settings by periodically synchronizing them with an SNTP/NTP time server or the MobiControl Deployment Server.

To configure the time synchronization settings for a device or device group, select the device or group in the device tree and click **Device,** click **Configure Device(s),** and click **Time Synchronization.**



Device Time Synchronization dialog box

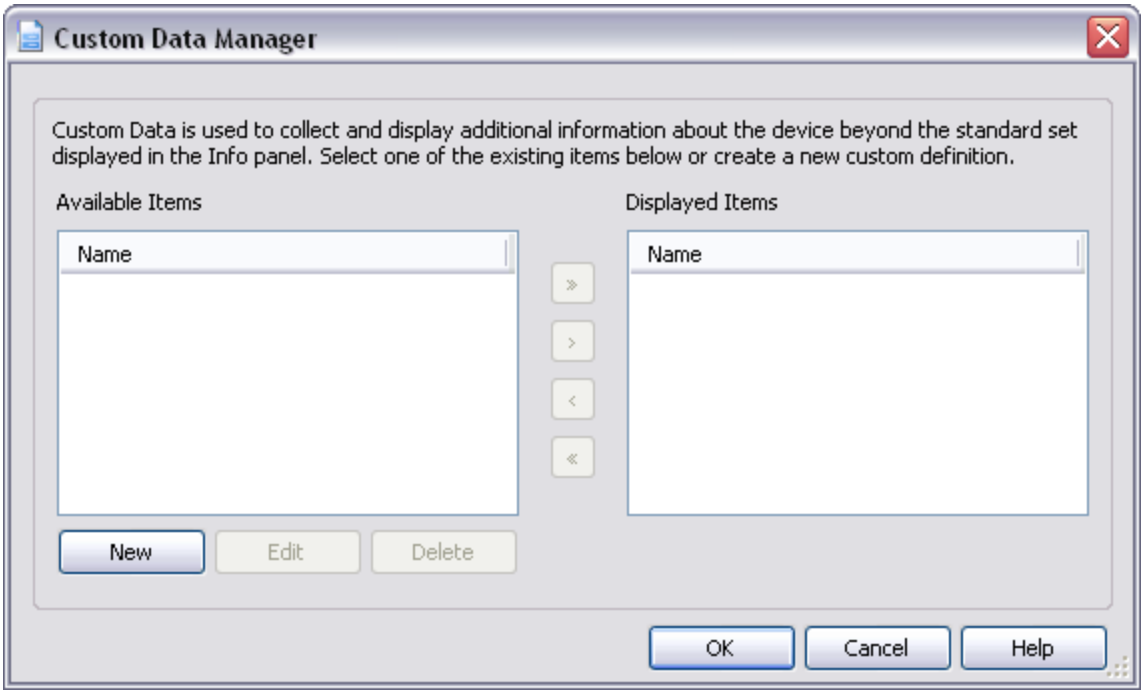
Time Synchronization Settings

There are three different modes available for time synchronization:

Option	Description
No Time Synchronization	The device time is not synchronized with any server.
Use a Deployment Server for Time Synchronization	The device will synchronize its time with a MobiControl Deployment Server when it connects to it. The time settings available for synchronization include Time Only, and All Time settings: • The **Time Only** option will result in the date and time being synchronized (but not the time zone) • The **All Time Settings** option will sync all of the time settings including DST, time zone, date, and time. • The **Set Time Zone** option to set the time zone for mobile devices which are in a different time zone than the Deployment Server. You can use this on device level or group level.
Use an SNTP/NTP server for Time Synchronization	The device will synchronize its time with the SNTP/NTP server(s) specified in the **Default SNTP/NTP Server** and **Secondary SNTP/NTP Server** fields. When this mode is selected, the option to synchronize automatically becomes available. With automatic synchronization enabled, the device will synchronize its time according to the interval specified in the **Interval between Synchronizations** field. If an automatic synchronization fails, the device will retry after the time interval specified in **Interval between Failed Attempts** has elapsed. **NOTE:** SNTP/NTP Server does not synchronize DST settings. It's similar to time only.

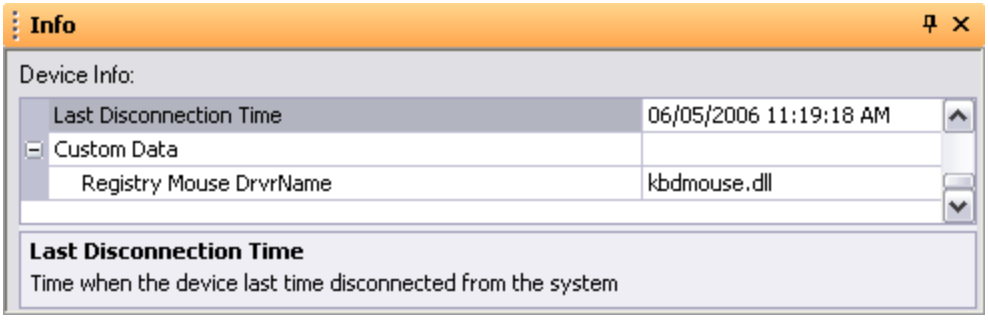
Custom Data

The custom data feature in MobiControl allows users to create their own monitoring fields to be shown in the **Device Info** window. This can be useful for monitoring various aspects of third-party applications. Custom data values are refreshed from the device when the device reconnects to the MobiControl Deployment Server and periodically, while the device status is Online, based on the device update schedule.



Custom Data Manager

The Custom Data Manager is accessible by right-clicking on a device or group, then selecting **Configure Device(s)** and clicking **Custom Data**.



The Device Info panel in MobiControl Manager

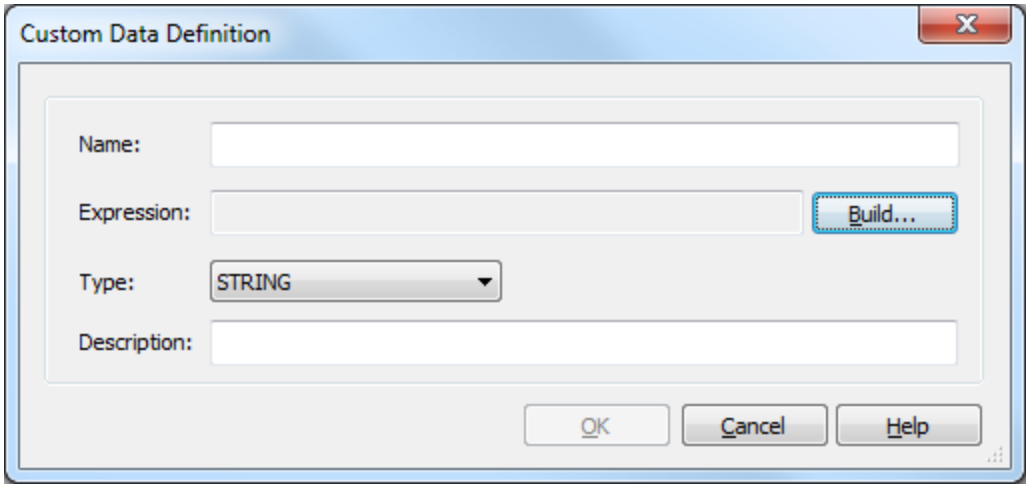
The following custom data types are available:

Type	Format and Description	Example
Text File	<Key>=TXT://\<FileName>?LN=<Value Number> Get the content of specified line of the text file (if LN is not specified, it assumes the first line)	TXT://\Device.log?LN=1
Registry	<Key>=REG://<GlobalKeyName>\<RegistryKey>?VN=<ValueName> Get a value from the registry. <GlobalKeyName> can be one of: • HKEY_CLASSES_ROOT • HKEY_CURRENT_USER • HKEY_LOCAL_MACHINE • HKEY_USERS	REG://HKEY_LOCAL_MACHINE\Software\Apps\SOTI\MobiControl?VN=Version
.INI File	<Key>=INI://\<FileName>?SC=<SectionName>&NM=<ValueName> Get a value from a Section in an .ini file.	INI://\SOTI\pdb.ini?SC=Device&NM=DeviceName
Exit Code	<Key>=EXE://\<Executable> [<ArgumentList>] Get the exit code of the executable	EXE://\windows\system32\calc.exe
STDOUT	<Key>=STDOUT://<Executable> [<ArgumentList>] Get the first line of STDOUT output of the executable.	STDOUT://cmd.exe /c dir
Static	<Key>=Text Enter the static value to display in the device info pane. This information is not based on any value on the device but based on user input.	OwnerName="X & Y Corporation, SalesDepartment"

Editing Custom Data

Configuration of custom data entries is performed through the Custom Data Manager which can be accessed by highlighting the device or the device group and selecting **Custom Data** from the **Configure Device(s)** option in the **Device** menu.

You can use the buttons in the **Custom Data Setting Manager** dialog box to add new entries, edit existing entries and change the order position of the custom data entries as displayed in the **Info** window.



Custom Data Definitions window

The following table describes the fields in the **Custom Data Definition** dialog box.

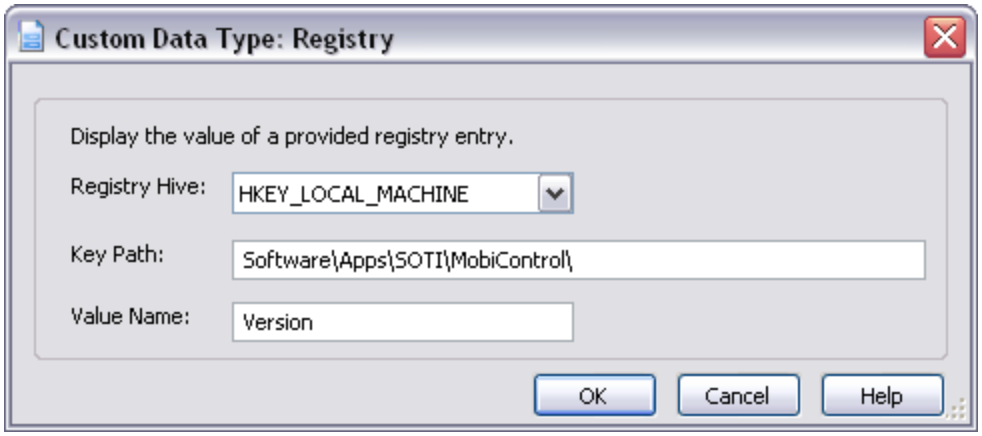
Field Name	Description
Name	Name of the custom data field that you want to show in the device info pane
Expression	The build button can be used to create a definition which will be used to collect the custom data values.
Type	Default is set to "String." This setting is only recommended when doing custom data collection. Other options are "Float" and "Integer."
Description	A brief note describing the nature of the custom data query and its purpose. This description is shown in the device info pane when the custom data field is selected.

Custom Data: Text Files

The following table describes the fields in the **Custom Data Type: Text File** dialog box.

Field Name	Description
Text File Name	Specify the location of the text file on the mobile device.
Line Number	Specify the line number that should be read from the text file and displayed in the device info pane.

Custom Data: Registry



The following table describes the fields in the **Custom Data Type: Registry** dialog box.

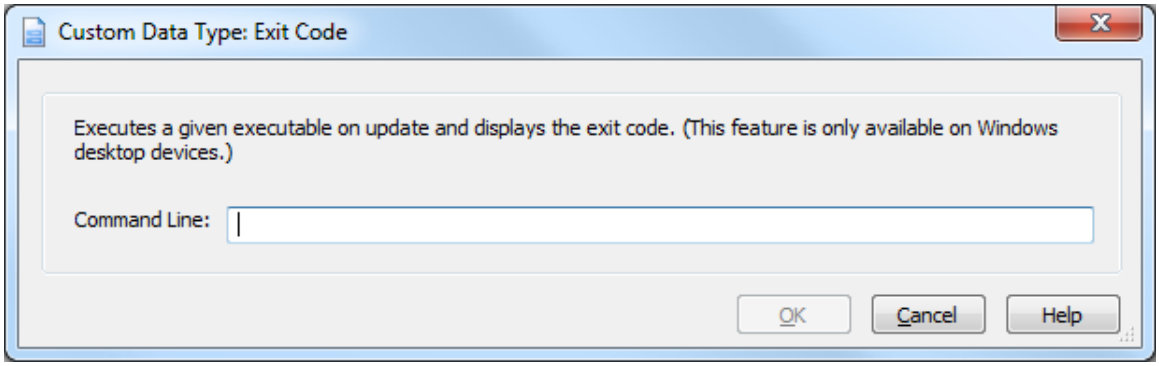
Field Name	Description
Registry Hive	Specify the registry hive where the information is located.
Key Path	Specify the exact path of the value that needs to be read.
Value Name	Specify the name of the value that should be ready and displayed in the device info pane. **NOTE:** Only `REG_SZ` and `REG_DWORD` value types are supported.

Custom Data: .Ini File

The following table describes the fields in the **Custom Data Type: INI File** dialog box.

Field Name	Description
INI File Name	Location of the `.ini` file on the mobile device
Section Name	Section from which the value should be read
Value Name	Value that should be read from the `.ini` file and displayed in the custom data field in the Device Info panel

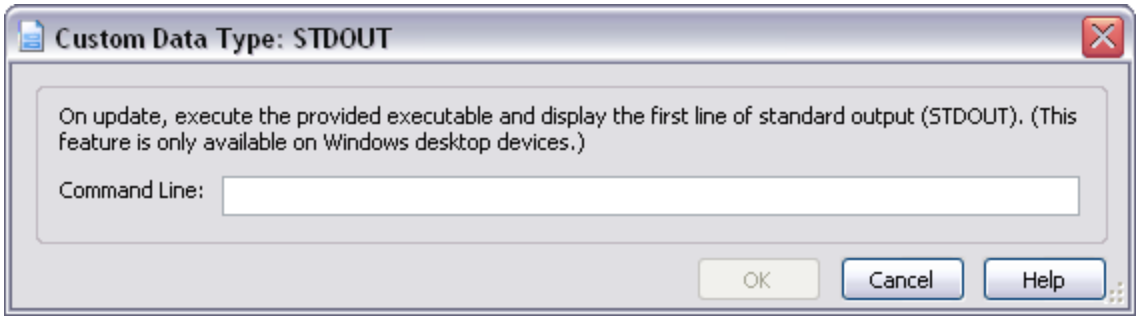
Custom Data: Exit Code



The following table describes the field in the **Custom Data Type: Exit Code** dialog box.

Field Name	Description
Command Line	Display the exit code of the application or command line instructions once they are executed.

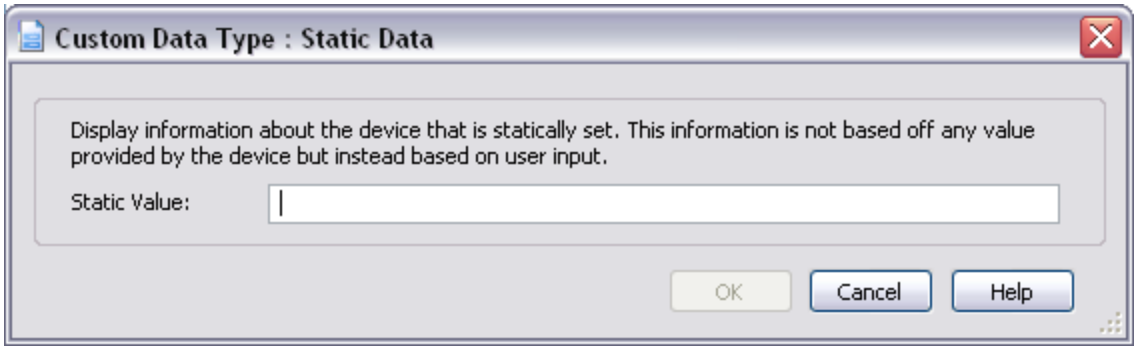
Custom Data: STDOUT



The following table describes the field in the **Custom Data Type: STDOUT** dialog box.

Field Name	Description
Command Line	Enter the command line instructions that should be executed and the first line of the return is displayed in the device info pane.

Custom Data: Static Data



The following table describes the fields in the **Custom Data: Static Data** dialog box.

Field Name	Description
Static Value	Enter the static value here to display in the device info pane. This information is not based on any value on the device but based on user input.

Embedded Query

A query string can be in another query string by using the format `%<KeyName>%`. The embedded query must be defined before the query. It works only in static type query and there has to be one static custom data type for every embedded query.

EXAMPLE:

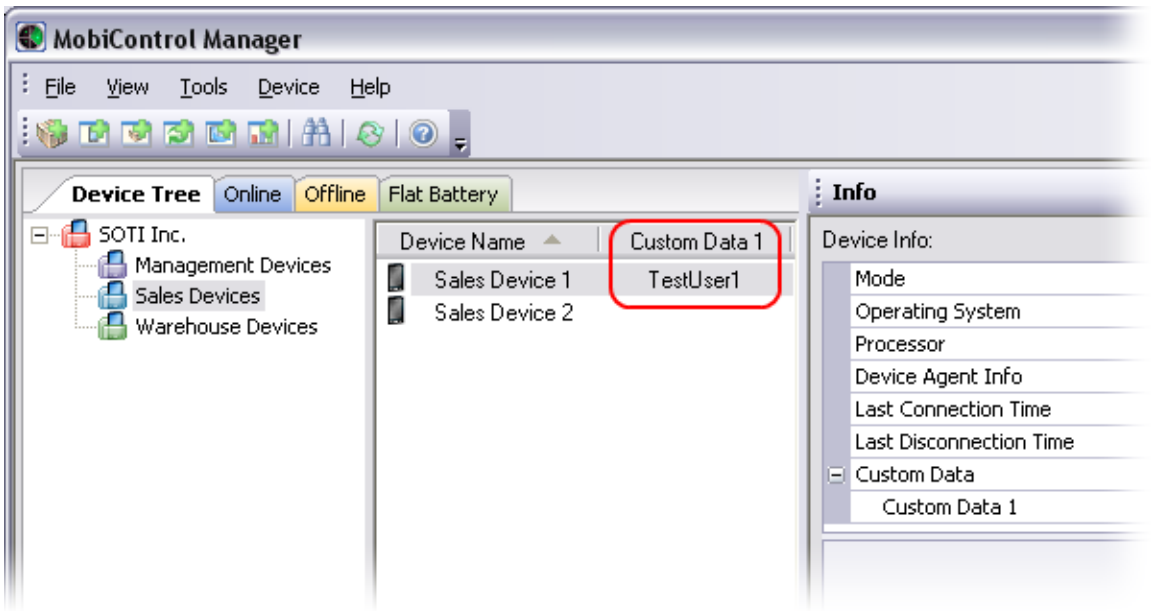
```
Key1=TXT://\RegLocationSSID.txt?LN=1
Key2=REG://%Key1%
```

Limitations

- All result values are limited to 250 characters. They will be truncated if this limit is exceeded.
- All Query Key Names are limited to 80 characters.
- All query strings (URLs) are limited to 250 characters.
- Typing "`STDOUT`" works on DOS and Desktop Agent. It doesn't work on CE and Pocket PC Agent.

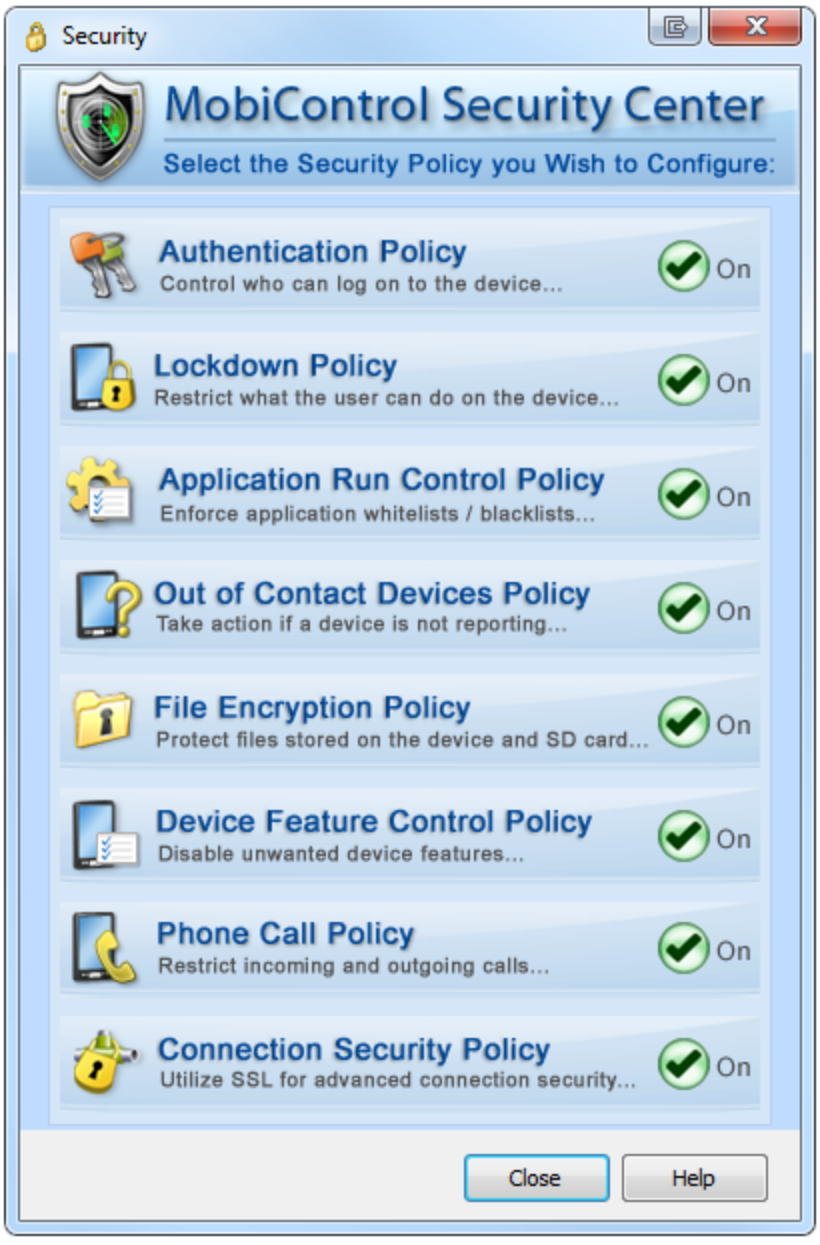
Custom Data Device Column

Once custom data has been configured, you can display or hide these custom data. Right-click on the device tree header or white space in the device tree and select **Custom Data**. You can also choose to display or hide the predefined data values displayed in the list.



Device Security and Control

MobiControl offers several device security options ranging from password authentication, user interface lockdown (also known as "kiosk"), and the ability to configure the device to automatically react to security threats such as repeated failed login attempts, even if the device is out-of-contact or in an offline state.



MobiControl Security Center dialog box

MobiControl's security provides powerful features for securing devices and mobile data, while maximizing usability and making security implementation easy, efficient and cost-effective. Salient features of MobiControl's security include:

- Over-the-Air (OTA) security policy distribution
- Policies can be assigned at the individual device, group or global level
- Security managed for both online (connected) and offline (disconnected) devices

To access MobiControl's Security Center, select the device or group of devices for which you want to configure security and then click **Device,** click **Configure Devices,** and click **Security.**

Authentication Policy

You can configure administrator passwords, and optionally, user passwords, to control access to the mobile device. The passwords are centrally managed via the **Authentication** tab. The option to use Windows Active Directory credentials is available. Please see the "Authentication Security" topic on page 186 for more information on configuring device-side user authentication.

Lockdown Policy

MobiControl allows administrators to operate mobile devices in a lockdown or kiosk mode by providing them with a specialized interface that strictly provides the device user with access to approved applications and websites only. Integrated locked-down or industrial web browser allows restricting browsing to specific Internet or Intranet sites only. Please see the "Device Lockdown" topic on page 201 for more information on configuring lockdown.

Application Run Control Policy

Control application infrastructure so you can easily manage, secure, and improve application service across the extended network of your mobile devices. Anti-virus like functionality allows better memory management and tighter monitoring of unauthorized applications on the device. MobiControl's application control engine delivers scalability, availability, breakthrough application security, and a way to simplify the application infrastructure overall within the network of your mobile devices.Please see the "Application Run Control" topic on page 227 for more information on configuring application run control.

Out-of-Contact Devices Policy

Time-based protection is now available for mobile devices to add an extra layer of security for mobile devices. The MobiControl Agent can be configured so that if the device has been lost or stolen and is out of contact (i.e. not connected to the network or the Deployment Server) for a defined time period, it will automatically take action to secure itself. For example, if the agent detects that the device has not connected for 24 hours, then it will wipe all data stored on the device. Please see the "Out-of-Contact Devices" topic on page 236 for more information on configuring out-of-contact device security.

File Encryption Policy

On-the-fly FIPS validated file encryption helps secure mobile data stored on the mobile device and media (flash storage or SD memory cards). File encryption allows only authenticated users to access the encrypted files, thus safeguarding sensitive business data and information on the mobile device, and helping mobile enterprise administrators meet their goals for complying with regulations. Please see the "File Encryption" topic on page 238 for more information on configuring file encryption.

Device Feature Control Policy

MobiControl provides various on-device feature controls including the capability to block various device communications and communication ports, similar to firewall functionality. Administrators can now

disable Bluetooth, IR Beam, SD-card auto-execute, ActiveSync connection and other features including the phone and camera functionality available on the PDAs. Please see the "Device Feature Control" topic on page 241 for more information on configuring feature control on the devices.

Phone Call Policy

MobiControl will allow or deny a predefined set of phone numbers that the device will be able to receive a call from, or make a call to. Please see the Phone Call Policy page for more information on configuring the phone call policy.

Connection Security Policy

To protect the integrity of the corporate firewall and to secure communication and data flowing from the mobile devices to the server across public unsecured networks, MobiControl allows the use of SSL Mode for encrypting communication using SSL certificate-based communication security. Please see the "Connection Security" topic on page 248 for more information on configuring connection security.

NOTE:

Due to a limitation in the way Windows CE 6.0 handles the pkfsh.log file - The following Device Security and Control Policies will not function properly:

- Application Run Control Policy
- Taskbar Lockdown
- Device Feature Control Policy
- File Encryption
- Phone Call Policy

NOTE:

Device security and control policies will apply to only mobile devices, and do not apply to Windows 2000/XP/Vista/7, with the exception of the connection security policy.

Authentication

The Authentication Policy option in the **MobiControl Security Center** dialog box allows administrators to set up device-side, password-based user authentication. This tab also allows administrators to create authentication actions, device-side scripts that execute when user authentication either succeeds or fails. For example, an administrator might create a script that locks the device for 30 minutes if authentication fails three times in a row.

To enable Authentication Security for a device or group of devices, select **Authentication Policy** from the MobiControl Security Center. (Please see the "Device Security and Control" topic on page 183.)

Device Authentication Configuration dialog box

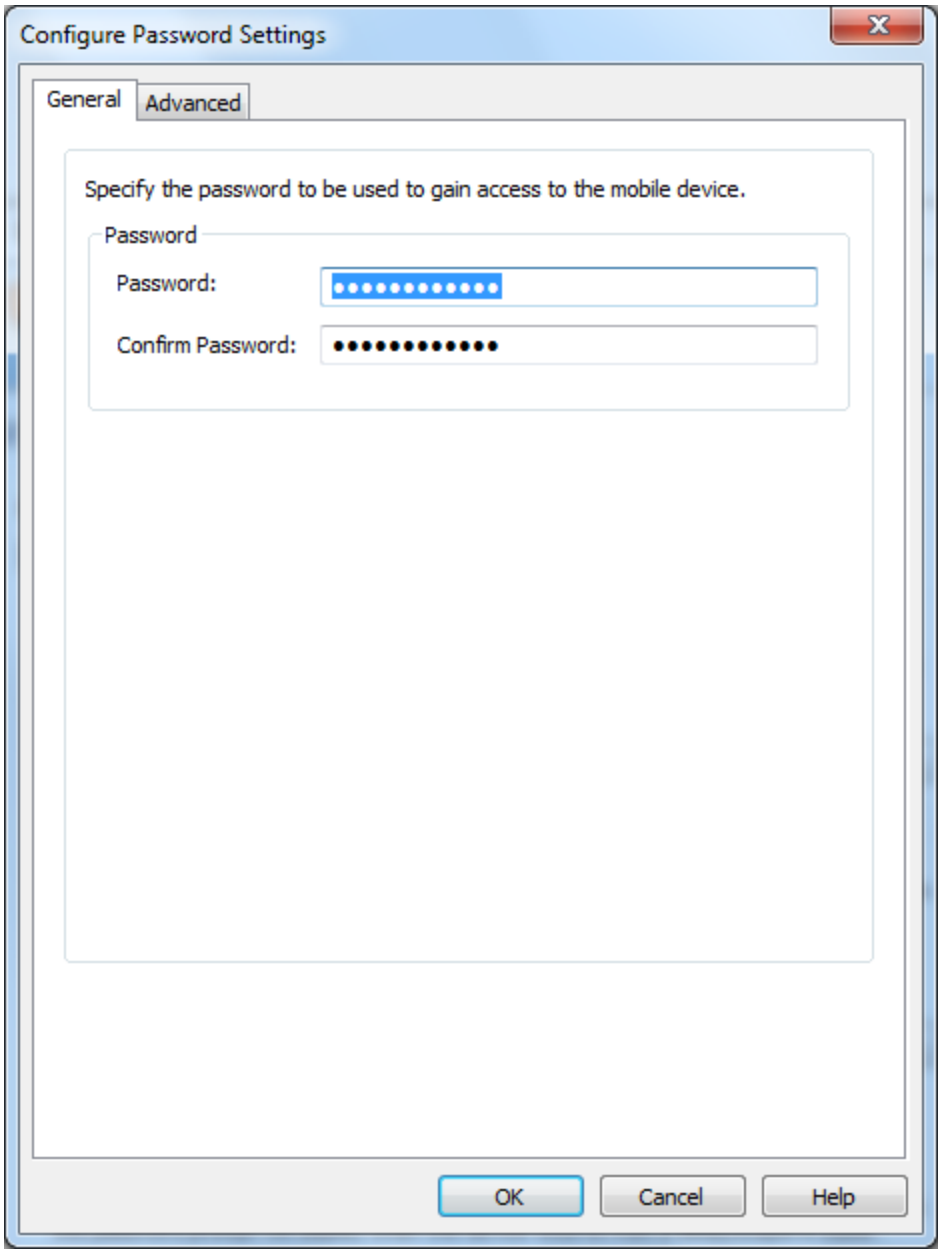
For assistance with Override Settings Click Here.

Administrators can configure an administrator password and a user password. When the administrator password is entered, the device is unlocked so that the administrator has complete access to the device. When a user password is entered, the user will have access to only those programs that the administrator has configured. An administrator can allow users to run all programs or only specific programs. Please see the "Device Lockdown" topic on page 201 and "Application Run Control" topic on page 227 for more details.

Administrator Password

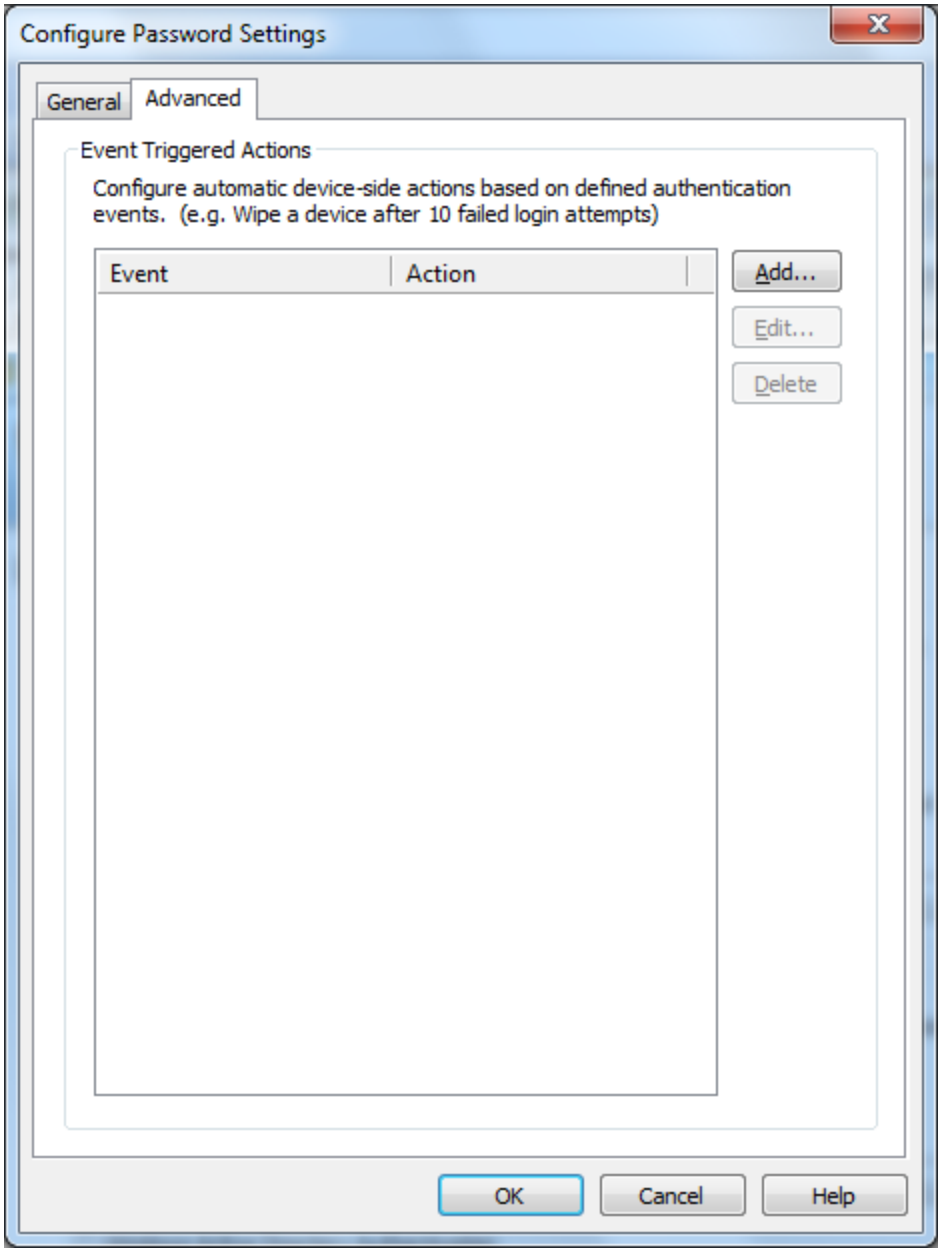
To specify an administrator password, first ensure that the **Enable Password Authentication** box is checked, and then click the **Configure** button in the administrator password section. This will bring up the dialog box below. Enter the desired password in the two provided text boxes and click **OK.** The configuration of the Administrator password is a prerequisite for all the other security configurations. To get to this screen you must click on the **Options** button, then select **Administrator** and click **OK.**

Administrator Device Password prompt



General tab of the Configure Password Settings dialog box

Administrator Authentication Events and Actions



Advanced tab of the Configure Password Settings dialog box

You can specify actions for administrator events. For example, you may wish to wipe all the data on the device if there are 10 consecutive failed log-in attempts. To create, edit, or remove an action, click on the **Advanced** tab of the **Configure Password Settings** dialog box. To add an action, click the **Add** button.

MobiControl will prompt you for the event that will trigger the new action. This event can be either a successful login or a certain number of failed attempts. After you have made your selection, click **OK** to bring up the **Action Configuration** dialog box. Please see the "Configuring Event Scripts" topic on page 251 for more details. To edit an existing action, select the action from the list and click **Edit.** This will bring up a small menu that lets you choose whether to edit the event that triggers the action or the action itself. To delete an action, select it from the list and click **Delete.**

User Password and Policy

To specify a user password, first ensure that the **Enable Password Authentication** box is checked, and then click the **Configure** button in the user password section. You must specify an administrator password before you can specify a user password. MobiControl provides a dialog box similar to that used for administrator passwords. The **User Password** dialog box also allows you to specify a password policy.

When you have configured a password or chosen Active Directory-based authentication, MobiControl will queue up the delivery of packages and settings targeted to the device, and only install the packages and settings once the user has been authenticated.

There are four options with regard to user authentication:

Field Name	Description
No Authentication	No user authentication is set. Any user can access the mobile device without any authentication.
Standard User Authentication	The administrator must specify a password for the user to enter to access the mobile device. This password is unique to MobiControl and can be controlled only with MobiControl.
Windows Active Directory Authentication	MobiControl now enforces Active Directory authentication for the users on their mobile devices. The end-user must enter their Active Directory credentials when trying to logon to the device. If the administrator changes their Active Directory profile, the changes are propagated down to the mobile device with MobiControl.
Prompt for password if device is unused for	This option can be used with both Standard and Windows Active Directory Authentication. When this option is enabled, if the mobile device is unused for the specified period of time, then the user will be prompted to enter the password again and authenticate their identity. The time value only works with Windows Mobile 5 (or greater) devices. On all other platforms, enabling this setting will cause the device to prompt for a password after device emerges from sleep mode. **NOTE:** It is necessary for the device to be soft reset (i.e. powered off and back on) for the change to take effect.

A user password policy specifies whether or not users can change their passwords and what minimum complexity requirements those passwords must meet (if any). Complexity requirements can include minimum length and uppercase, lowercase, numeric, and special character requirements.

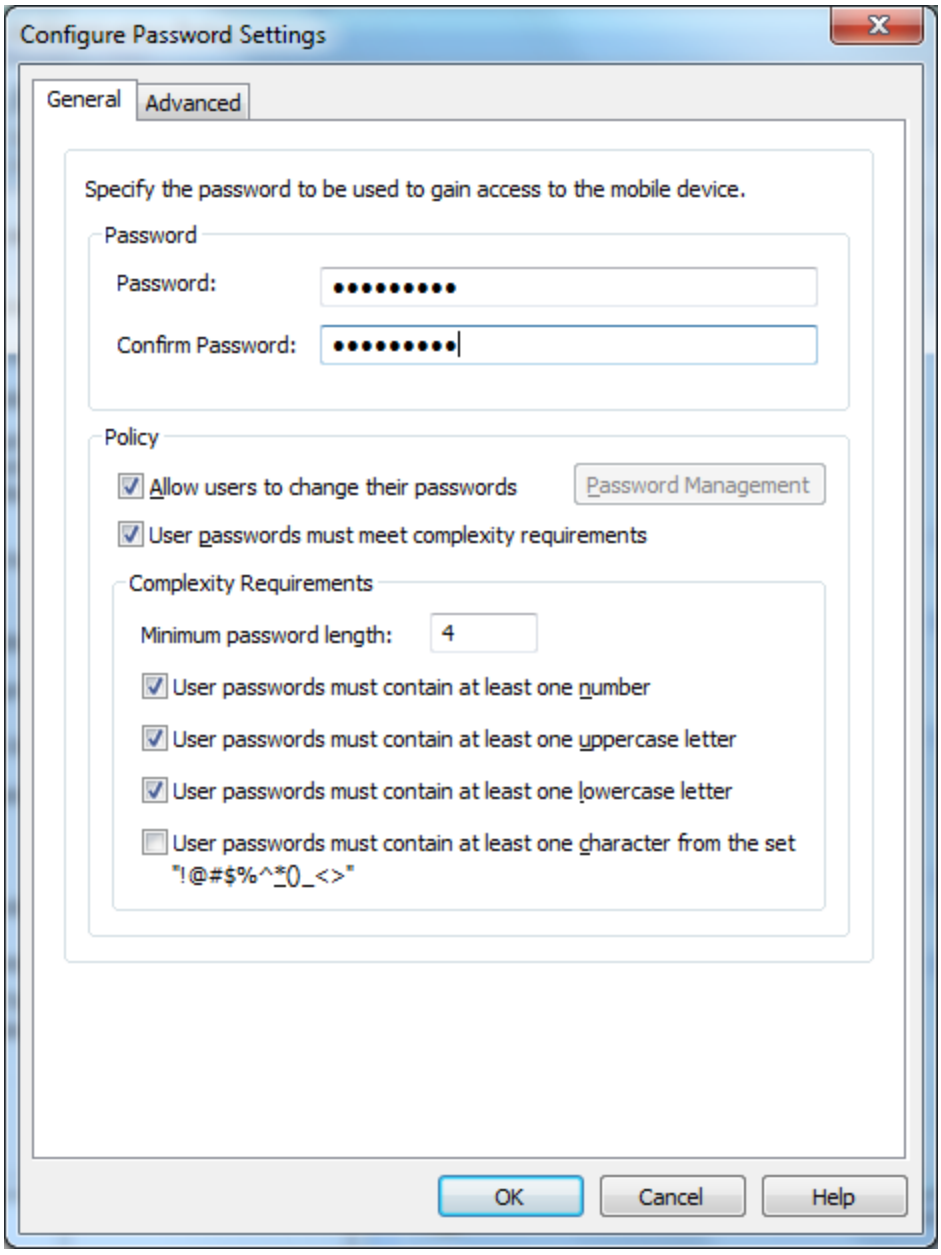
User Password Settings

When Standard Authentication is selected, a password is specified for the user and complexity requirements for the user password is enforced, if the user password does not meet the complexity requirements, MobiControl will prompt you to change the user password within MobiControl Manager.

User Device Password prompt

NOTE:

When you click the **Reset Password** button, it will reset the password instantly, so there is no need to click the **OK** button. Please see the "Device Lockdown" topic on page 209 if you would like to add a custom bitmap background image to your password prompt banner.



User Password Settings dialog box

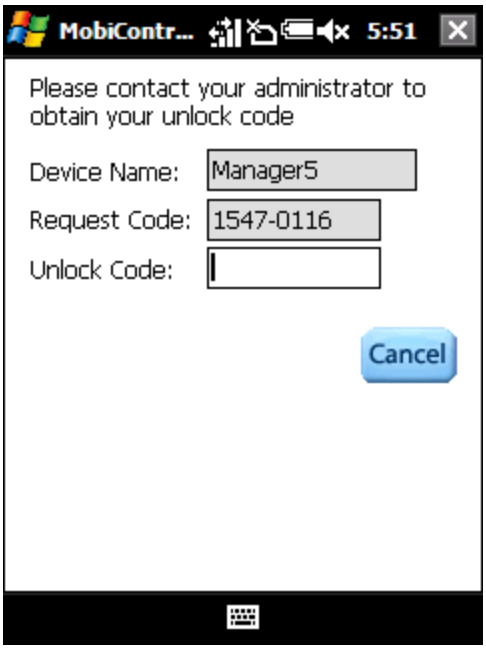
Offline User Password Reset

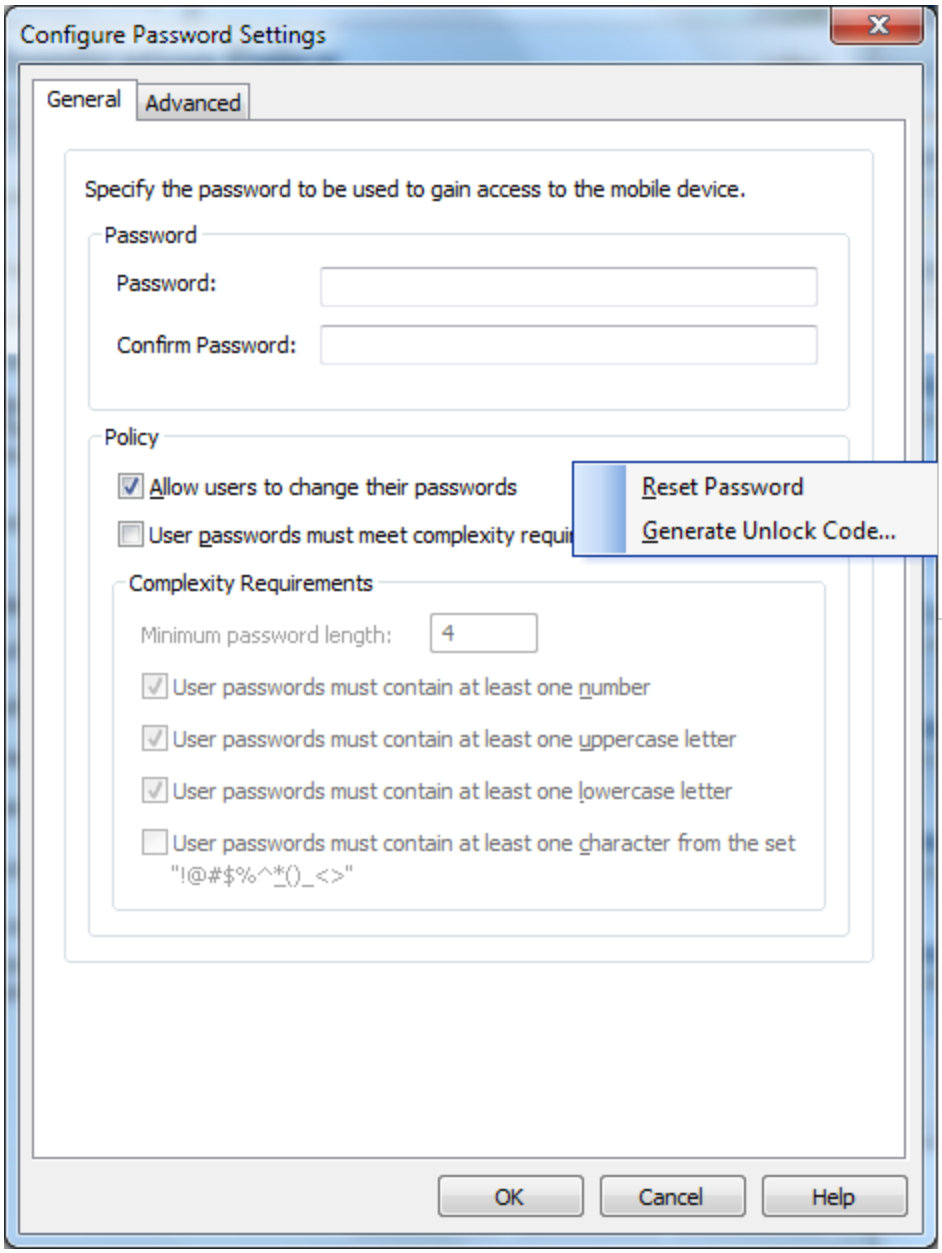
If a user has forgotten his or her password and cannot connect to the Deployment Server, an offline user password reset may be used to change the user password. This feature is only available for standard user authentication.

To do an offline password reset, the user must click the **Options** button from the password entry screen and select **Forgot Password?** The user will then be provided with a request code. This code is required to obtain the unlock code.

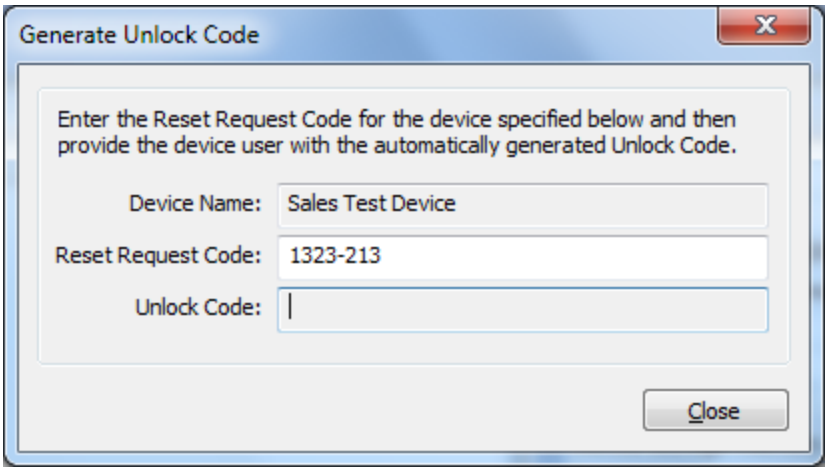
In order to generate an unlock code within the MobiControl Manager, use the following steps:

1. Right-click on the device that requires the unlock code.
2. Click **Configure Device** and then click **Security.**
3. Select **Authentication Policy.**
4. Select **Configure** from the **User Authentication** section.
5. Click on the **Password Management** button.
6. Select **Generate Unlock Code.**

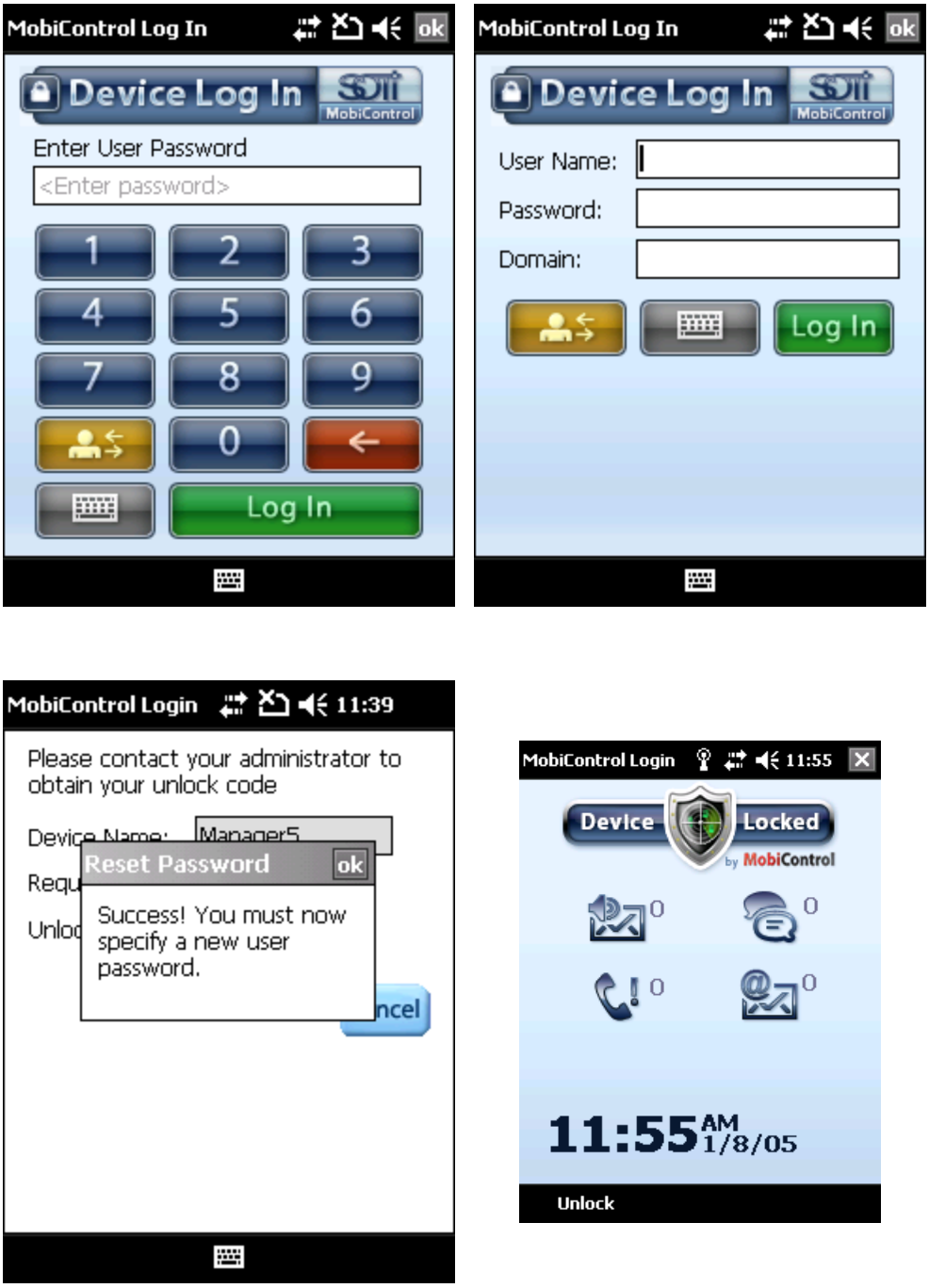




When the request code has been entered, an unlock code is automatically generated. This code can then be provided to the user of the device.


Generate Unlock Code
Enter the Reset Request Code for the device specified below and then provide the device user with the automatically generated Unlock Code.
Device Name:
Sales Test Device
Reset Request Code:
1323-213
Unlock Code:
Close

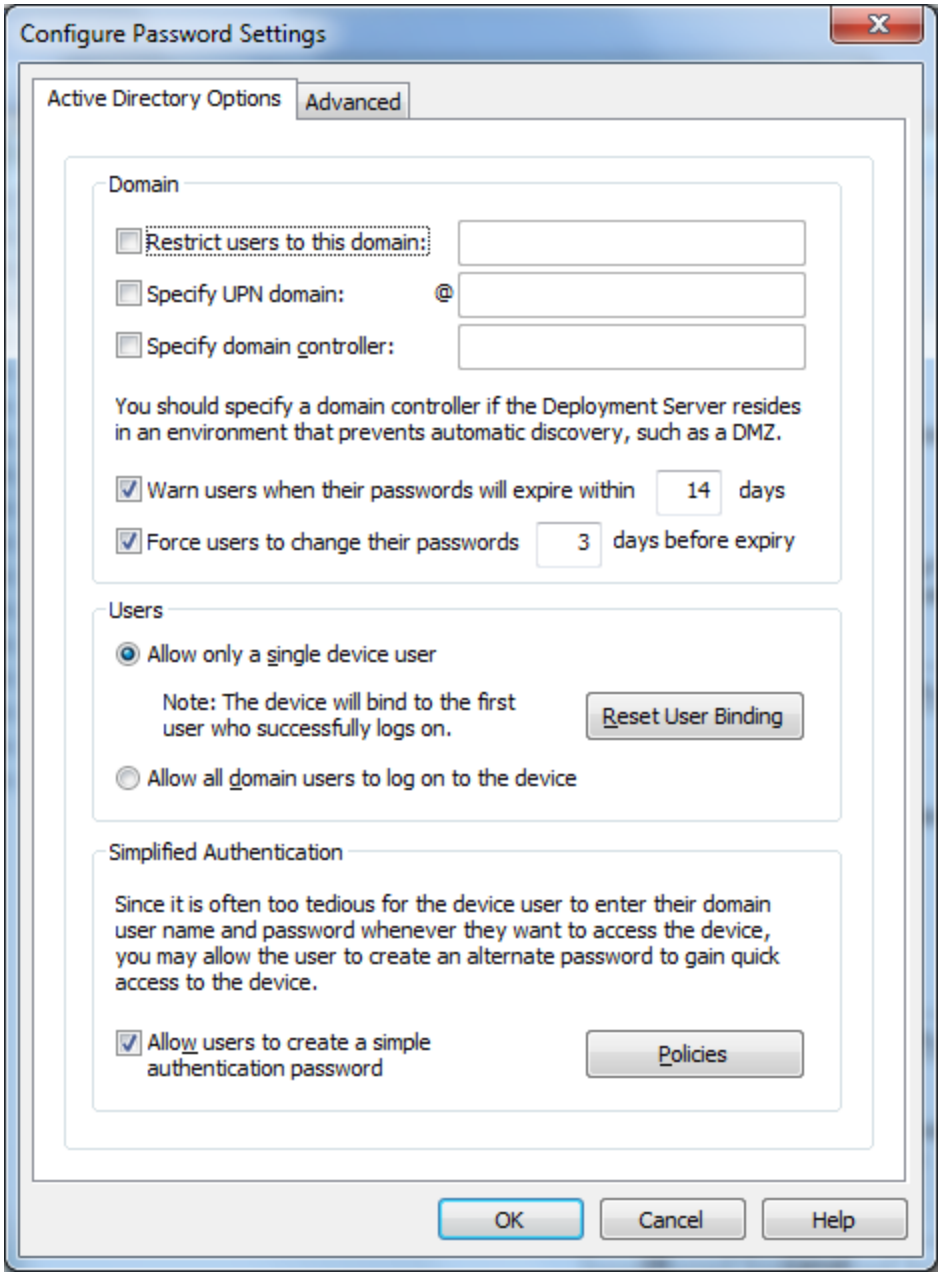
Once the user enters the unlock code, they will be prompted to enter a new user password. The new password cannot match the old password.



Entering a new password, notification that setting the new password was successful, and the Active Directory login prompt

Windows Active Directory Authentication

When you choose Windows Active Directory-based authentication, the MobiControl Agent will directly authenticate the user's credentials with the Active Directory server associated with the configured domain. The Active Directory Server requires SSL security to be enabled, and ports 636 and 443 to be open between the Deployment Server and Active Directory Server. If your organization is using a non-standard port to communicate over SSL with your Active Directory Server, then a colon ":" must be used to indicate the port being used in the **Specify domain controller** field (i.e. `Mydomain.com:1234`). If no other connections are available, the MobiControl agent will attempt to initiate a data connection if one has already been configured.

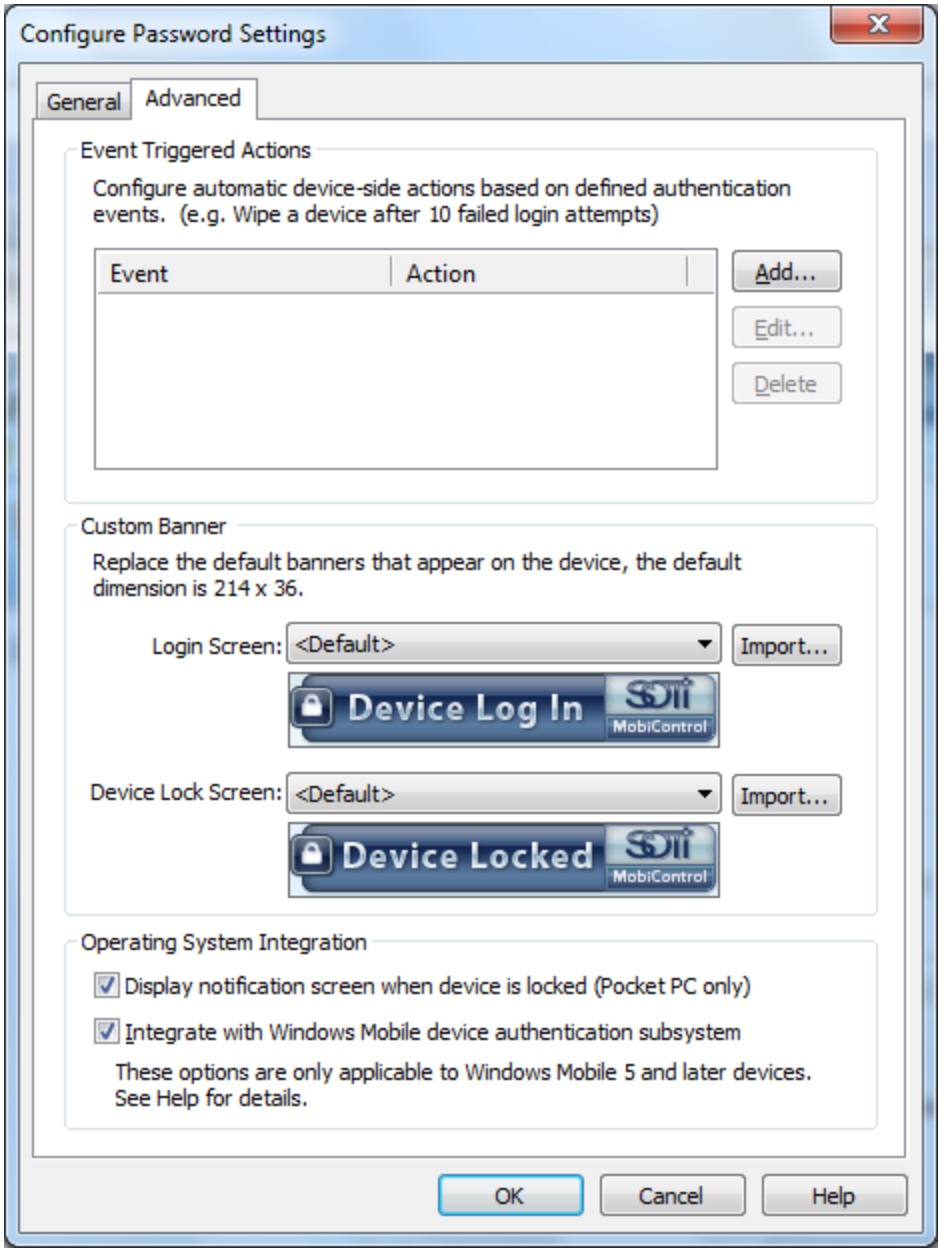


Configure Active Directory Settings dialog box

Field Name	Description
Restrict users to this domain	Select this option to force the user to be authenticated against a particular domain controller. When the domain is known ahead of time this option is recommended as it requires the device user to enter less information.
Specify UPN domain	Select this option to specify the domain portion of the UPN (User Principal Name) that should be used to identify users in the Active Directory system. This name typically takes the form of `domain.corp.mycompany.com` or simply `@mycompany.com`.
Specify Domain Controller	This is where you can specify a domain controller to use when your Deployment Server resides in a DMZ (Demilitarized Zone). This is also useful if you have more than one Domain Controller and want to specify a single one.
Warn Users when their password will expire	Advises the user that his or her password is about to expire, and requests that he or she changes it
Force Users to change their password	Forces the users to change their password before it expires in the Active Directory. This option is especially helpful in case your Deployment Server is located within a DMZ since in that configuration, the Deployment Server is unable to facilitate the password change if the password has already expired.
Allow only a single device user	This option will lock the device to the first user that successfully logs on to the device. Another user will be unable to login and use the device. This option must be selected if you are using Microsoft Exchange ActiveSync, since a Windows Mobile device is only capable of synchronizing with the account of a single user. If you wish to reset which device user is bound to a given device: While the device is online, right-click on it in the device tree, and click **Configure Devices**, then click **Security**, click **Authentication Policy** and click **Configure** to get to the dialog box displayed above. Then, click the **Reset User Binding** button. **NOTE:** When you click the **Reset User Binding** button it will reset the binding instantly, so there is no need to click the **OK** button.
Allow all domain users to log on to the device	Allows for all domain users to log on to the device and use the device This option is suitable only for environments where devices are shared amongst a group of people, and there are no personal settings stored on the device.
Allow users to create a simple authentication password	This option will allow the user to create a simplified password and use this password when trying to log on to the device instead of using their Active Directory password. This option is handy when the Active Directory password for the user is very complex and it is too tedious to enter on the device. Although called "simple," you may force the user to use a password of a given complexity by clicking on the **Policies** button.

User Authentication Events and Actions

You can specify actions for user authentication events. For example, you may wish to wipe all the data on the device if there are 10 consecutive failed log-in attempts. To create, edit, or remove an action, click the **Advanced** tab of the **Configure Password Settings** dialog box. This will bring up the following screen:



Password Settings (Advanced)

To add an action, click the **Add** button. MobiControl will prompt you for the event that will trigger the new action. This event can be either a successful login or a certain number of failed attempts. After you have made your selection, click **OK** to bring up the **Action Configuration** dialog box. Please see the "Configuring Event Scripts" topic on page 251 for further details. To edit an existing action, select the

action from the list and click **Edit.** This will bring up a small menu that lets you choose whether to edit the event that triggers the action or the action itself. To delete an action, select it from the list and click **Delete.**

Custom Banner

You have the option of replacing the default banners that appear on your device with custom images (The default dimension is **214x36 Pixels** and the image file must be of .BMP format.). Next to the **Login Screen** drop-down menu, click on the **Import** button to browse to the desired .BMP file that you'd like to replace the default banner with. For the **Device Lock Screen** drop-down menu you can do the same. Simply click on the **Import** button to browse to your .BMP file and -once selected- it will be available as an option in the drop-down menu for the **Device Lock Screen** feature.

Operating System Integration

The **Display notification screen when device is locked(Pocket PC only)** check box option configures the device to present clear indication of the device's locked status to users.

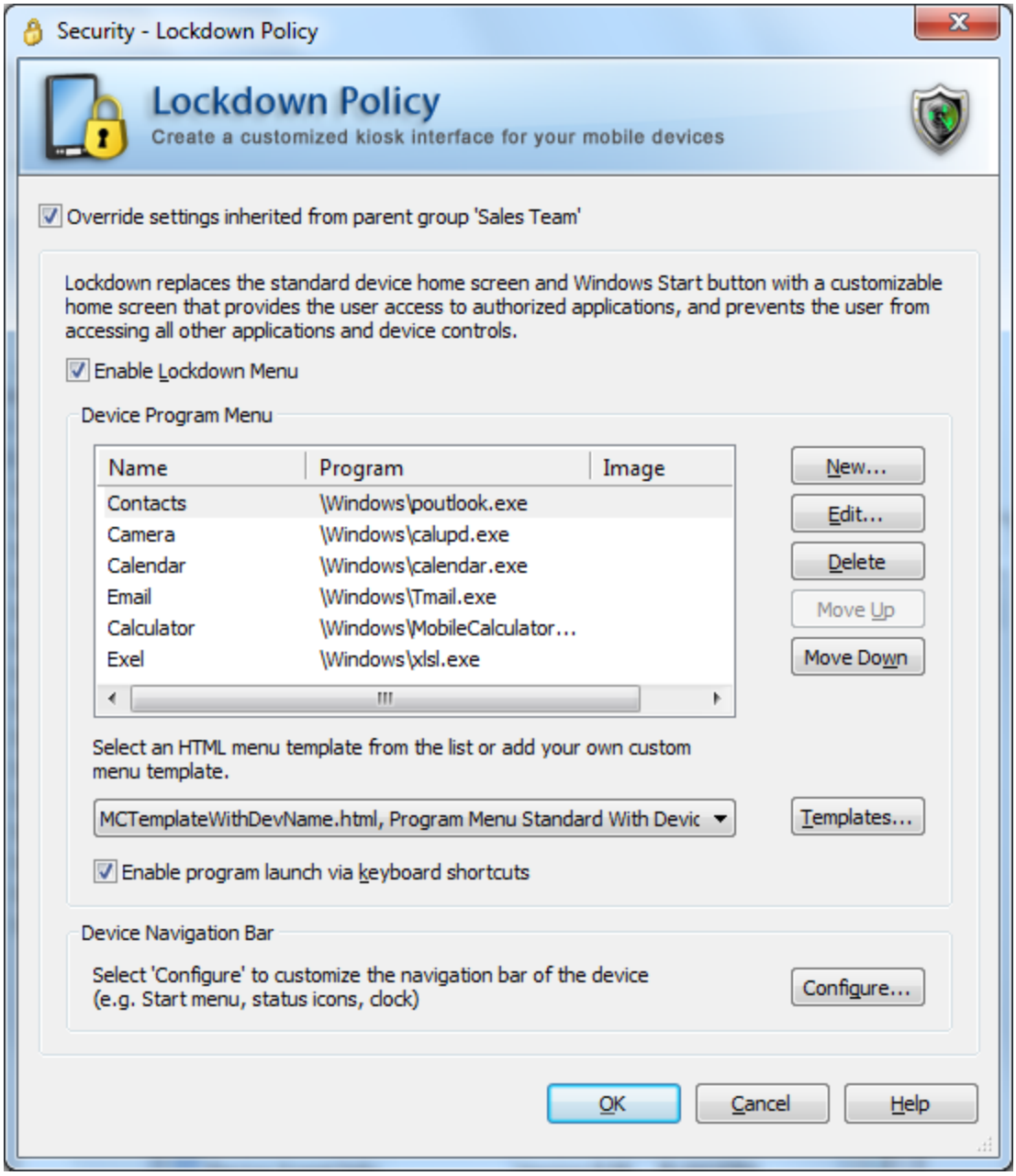
Windows Mobile Authentication Plug-in

When the **Integrate with Windows Mobile device authentication subsystem** option is selected, the MobiControl agent is registered with the operating system authentication subsystem, and replaces the standard password prompt with its custom password prompt. This provides maximum security for the device because the password prompt engages immediately on device startup, ensuring the device cannot be accessed without the user first providing the user or administrator password. With this option, the password prompt is automatically re-engaged when the operating system dictates the idle timeout has expired.

This option is only applicable when both an administrator and a user password have been configured and the device is running the Windows Mobile 5 or later operating system. For devices running other operating systems, the password prompt is handled at the application layer and is not driven directly by the operating system. In some cases you may wish to disable this option to avoid the authentication plug-in from conflicting with other third-party security solutions that may be running on the mobile device.

Device Lockdown

Device lockdown replaces the standard device home screen and Windows **Start** button with a customizable home screen. Users have access only to authorized applications and websites, and are prevented from accessing all other applications and device controls.



Lockdown Policy dialog box

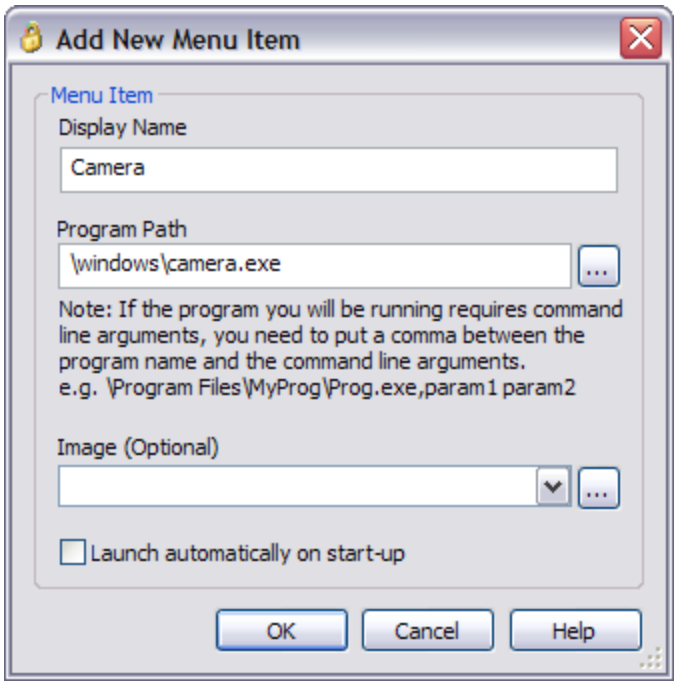
For assistance with Override Settings Click Here.

By locking down devices, organizations can minimize the risk of unauthorized persons accessing information on their mobile devices. Administrators can control exactly which programs users are allowed to run, and which websites they are allowed to visit. This decreases the amount of down-time caused by users changing settings that may adversely affect the operation of the device or application software, and also decreases support costs. MobiControl allows running the mobile devices in a kiosk mode with a read-only access to provide critical information to the end users, without giving them access to change the settings.

The lockdown menu can only be dismissed by an administrator. Specification of a user password is optional. If not configured the device user can access the lockdown menu directly after turning on the device. If a user password is defined, then the password must be entered in order to access the lockdown menu.

To configure lockdown settings for a device or group of devices, select the target device or group in the device tree view in the main console window and select **Security** from the **Configure Device(s)** submenu.

Field Name	Description
Enable lockdown menu	Use this checkbox to enable or disable the device lockdown menu.
Device Program Menu	The device program menu is a list of programs and websites to which the user has access. There are pre-configured HTML menu templates that can be edited or applied to the menu, and an option to enable or disable the launching of a menu item with keyboard shortcuts. Please see the Device Program Menu section below for details.
HTML menu template	Select a menu template from the drop-down list. Please see the Templates section below or the "Customizing Lockdown Program Menu Templates" topic on page 217 for more information.
Enable program launch via keyboard shortcuts	Keyboard shortcuts such as numeric keys can be used to launch lockdown menu items. See the Shortcuts section below.
Device Navigation Bar	The device navigation bar, commonly referred to as the task bar, contains the **Start** button and small icons for quick access to device status and settings such as the time, date, wireless status, or volume control. By default, when lockdown is enabled, the standard operating system navigation bar is replaced with a customizable navigation bar. **NOTE:** This applies to only Pocket PC and CE devices; it does not apply to Smartphone devices. Select the **Configure** button to specify which icons in the custom navigation bar are to be made available to the device user. Please see the Navigation Bar Configuration section below for details.



Add New Menu Item dialog box

TIP:

- To provide the device users with access to specific websites and prevent access to other websites, provide the URL in the **Program Path** of the **Add New Menu Item** line.
- If you link to a search engine the end user will gain full access to the Internet.

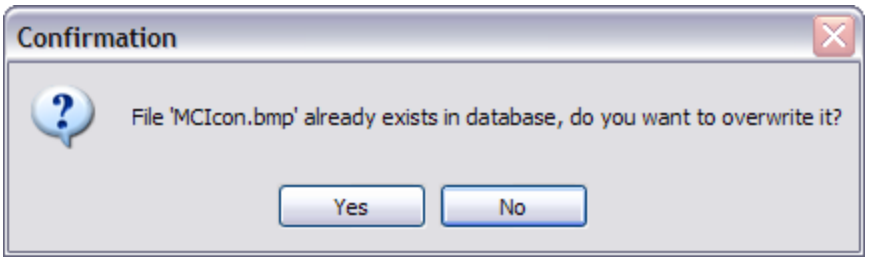
Device Program Menu

Use the **New** button to add menu items. Each entry consists of a user-friendly name and a complete file path to the executable, `.lnk` shortcut file, `.cmd` script file, or website address (URL). To adjust the position of the menu items, use the **Move Up** and **Move Down** buttons.

Field Name	Description
Display Name	This is the displayed name of the menu item which will appear on the device.
Program Path	This is the path for the web address, or executable file on the device. You can either type in the path or you can browse the file using the browse button [...]. You can only browse the files if the device is connected to the desktop via ActiveSync. For instance, the program path for Pocket Word is `\windows\pword.exe`. The path will not be displayed on the Menu page.

NOTES:

- For command line parameters, a comma must be used to separate the program path from the parameter. For example, write `\windows\poutlook.exe,contacts` **without spaces**.
- Incase a " character is required for paths including spaces in them, in place of double quotes, %22 MUST be used.

Field Name	Description
Image (optional)	This is the name of the image file that you want to display in the lockdown menu with this menu entry. By selecting the image in this dialog box, it will be automatically delivered to the device along with the lockdown configuration. Select an image from the drop-down list, or click the browse button ... to select an image from your desktop computer. In order to display this image in the lockdown menu, it is necessary for the HTML template to have a special `<MCDispImgN>` tag. Please see the "Customizing Lockdown Program Menu Templates" topic on page 217 for instructions on how to make this image appear in the Lockdown menu. **NOTE:** If you wish to replace an image that had been previously imported, upload the new graphic file, maintaining the same file name as the old one. You will be asked to confirm the overwrite of the old file. Click **Yes,** and the new image will be in effect.  *Lockdown Menu Image Overwrite Confirmation dialog box*
Launch automatically on startup	When this option is checked, the selected program will be automatically executed on startup (i.e. after a soft reset, or restart of the lockdown process).

TIP:

On devices that feature a numeric keypad, an alternative to tapping the screen to launch the menu entries is entering the number that corresponds to the menu item. For example, press 2 to launch the second menu item.

Templates

The lockdown program menu is displayed as an HTML web page to the user. The Template drop-down box allows you to select an HTML template from a list of built in templates and your own customized templates.

You can easily create a customized lockdown template by copying an existing template and directly modifying HTML code in the built-in Lockdown Menu Template Editor available in MobiControl. (Please see the "Customizing Lockdown Program Menu Templates" topic on page 217.) You can also use your favorite HTML editor. When editing the HTML file, be sure to preserve the special MobiControl Menu tags. These special tags are automatically replaced with the appropriate Program Menu entries by MobiControl.

Once you have selected the desired template and clicked the **OK** button, MobiControl will merge the menu items that you have configured with the selected template and generate a custom HTML menu page.

Device lockdown page

Keyboard Shortcuts

If the checkbox next to **Enable program launch via keyboard shortcuts** is selected, program menu items may launch in a few additional ways: pressing a numeric key on the device or using a scanner will launch the program menu item corresponding to the value of the numeric key or barcode. To prevent this, clear the checkbox next to **Enable program launch via keyboard shortcuts**.

Navigating Device Lockdown

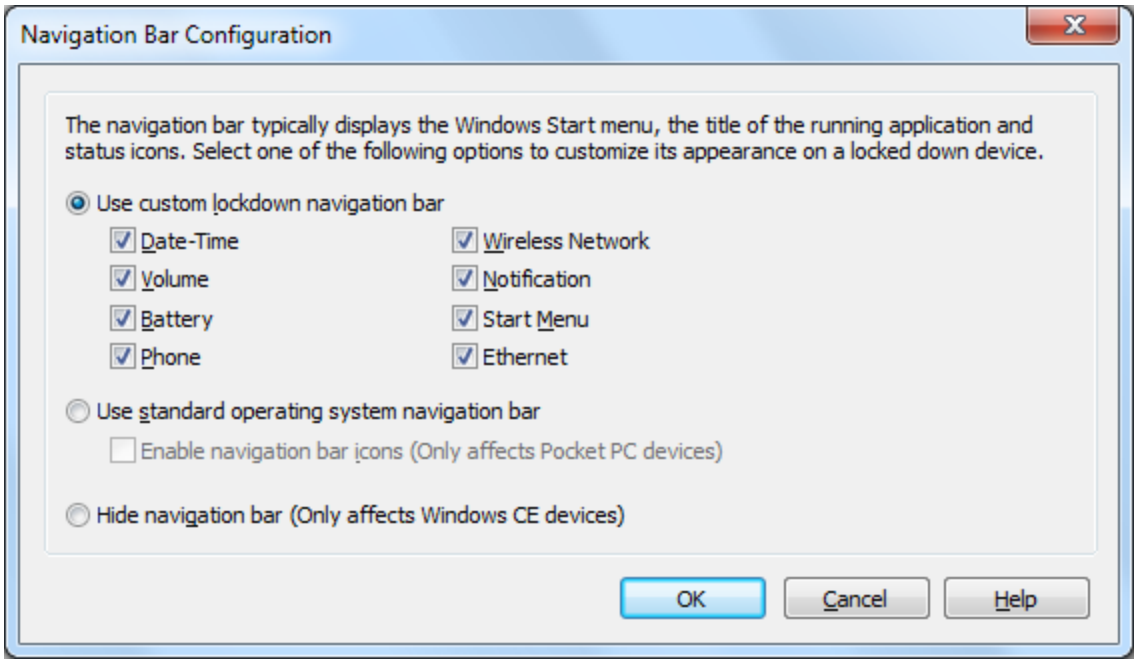
Back Button:
While you are navigating a web page within the lockdown, the back button will allow you to return to the previous page.

Right Click Option:
Click and hold on the device screen to bring up the "Right Click" menu. This allows you to copy and paste contents from within the lockdown.

NOTE:

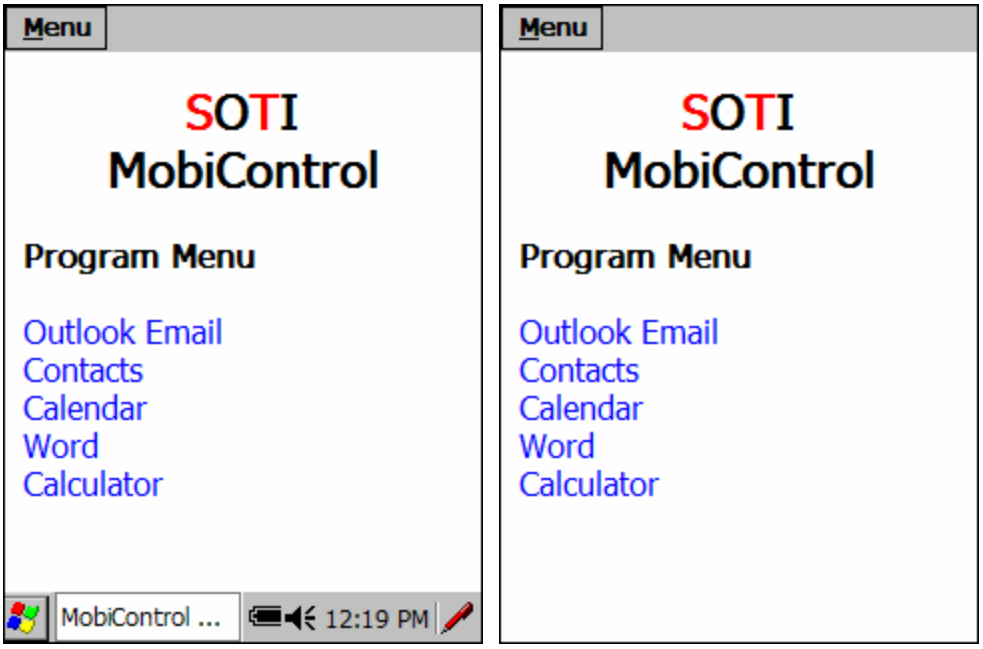
This feature is only supported on Windows Mobile 5.0 or later devices.

Navigation Bar Configuration



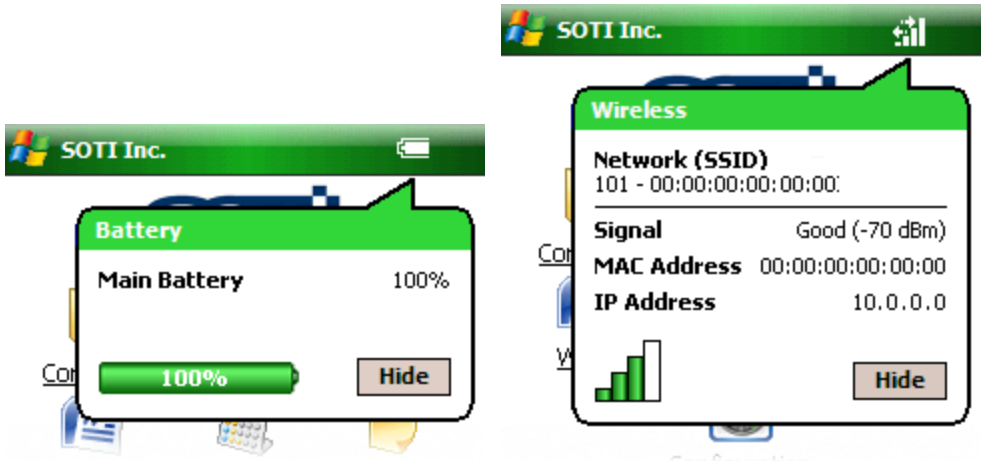
Navigation Bar Configuration dialog box

Field Name	Description
Use custom lockdown navigator	This option will only allow the selected icons to show up in a custom navigation bar. The user will have the ability to click on the icons and have view-only access. The user will not be allowed to make any configuration changes using the icons on the navigation bar. Please see the descriptions of the six options following this table.  *Enabled custom lockdown navigation bar displaying all the available icons*

Field Name	Description
	NOTE: The icons of the lockdown custom navigation bar are non-responsive on Windows CE 6.0 devices due to a current limitation. This will be addressed in a later version.
Use standard operating system navigation bar	This option will display the standard operating system's navigation bar. This option is recommended if there are specific icons that appear in the standard navigation bar that are not available in the custom navigation bar.  *Enabled Windows navigation bar* In order to prevent the user from accessing Programs listed in the Start menu and links to Settings from popup balloons accessed through the navigation bar icons, the navigation bar is disabled by default. For only Pocket PC devices, it is possible to enable the navigation bar icons. This option will allow the user unrestricted access to the Windows navigation bar.
Hide navigation bar	For only Windows CE.NET devices, this option will hide the navigation bar completely.  *Disabled and enabled "Hide navigation bar"*

Enabled custom lockdown navigation bars with date-time and volume

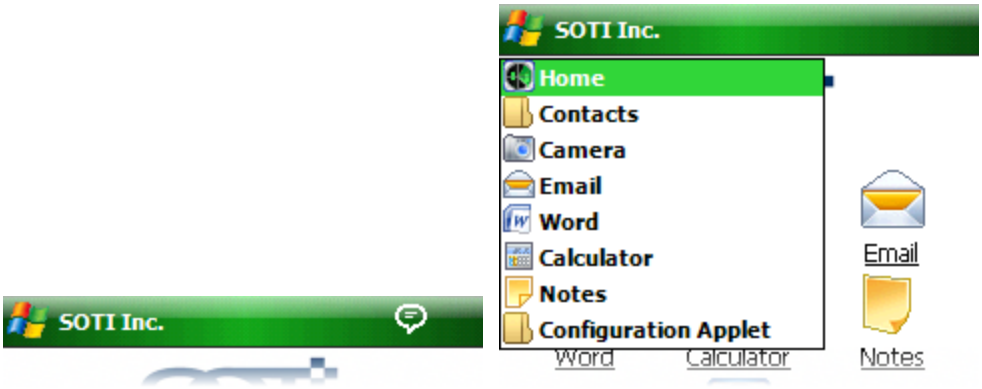
- The **Date-Time** option will display the time on the custom lockdown navigation bar. When the time is selected, a window will display the date, time and user's appointments.
- The **Volume** option will cause the volume icon to be displayed on the custom lockdown navigation bar. When the volume icon is selected, the volume window will open and the user will be able to adjust the mobile device's sound and volume, change it to vibrate or turn off the sound completely.



Enabled custom lockdown navigation bars with battery and wireless network

- The **Battery** option will cause the battery icon to be displayed on the custom lockdown navigation bar. When the battery icon is selected, a window will display the percentage of the battery charge.

- The **Wireless Network** option will cause the wireless bar icon to be displayed on the custom lockdown navigation bar. When the wireless bar icon is selected, a window will display the mobile device's wireless settings such as the signal strength, MAC address and IP address.



Enabled custom lockdown navigation bar notification and Start menu

- The **Notification** option will cause the Notification icon to appear in the custom lockdown navigation bar when there is an unacknowledged notification on the device. When the notification icon is selected, a pop-up menu will display, from which the user can select the notification to be displayed. This option also controls the display of the Notification menu entry in the Lockdown window.
- The **Start Menu** option allows the custom navigation bar to replace the standard Start menu with a listing of the programs specified in the Program Menu. This allows the Start menu to be used as an "application switcher" to move quickly from one application to another.

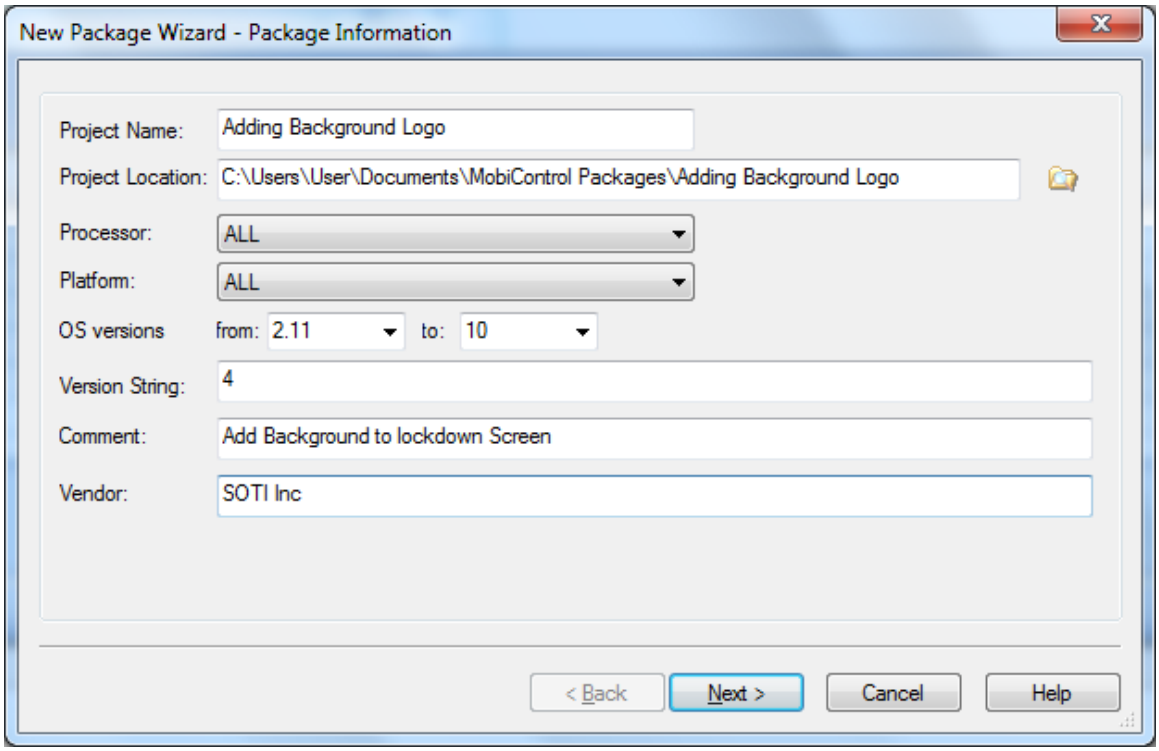
Customizing Lockdown

The lockdown program menu can be customized a number of different ways. You have the ability to change the lockdown password banner, as well as add your own notification icons. This section will explain how to edit your lockdown using MobiControl Package Studio.

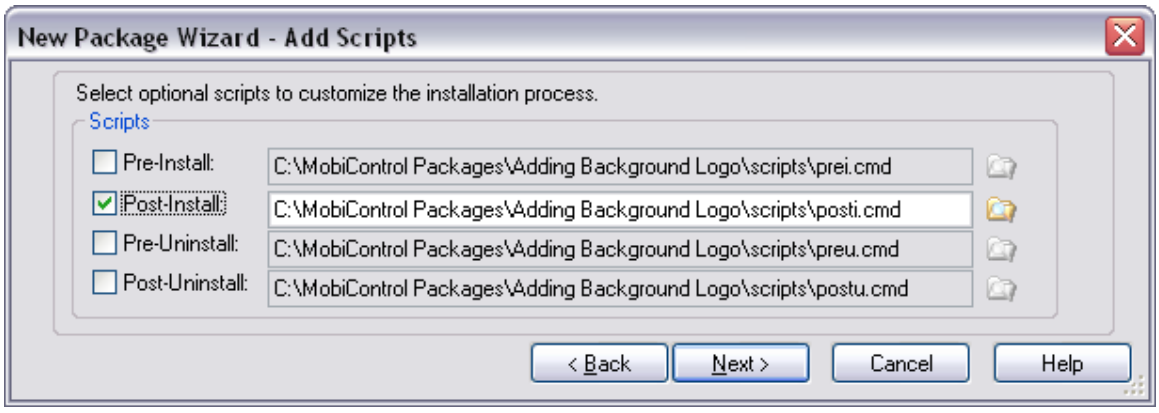
Custom Password Prompt Banner

If you would like to add a custom bitmap background image to your password prompt banner follow the steps outlined below:

1. Create a new package using Package Studio.
   Please see the "MobiControl Package Studio" topic on page 413.

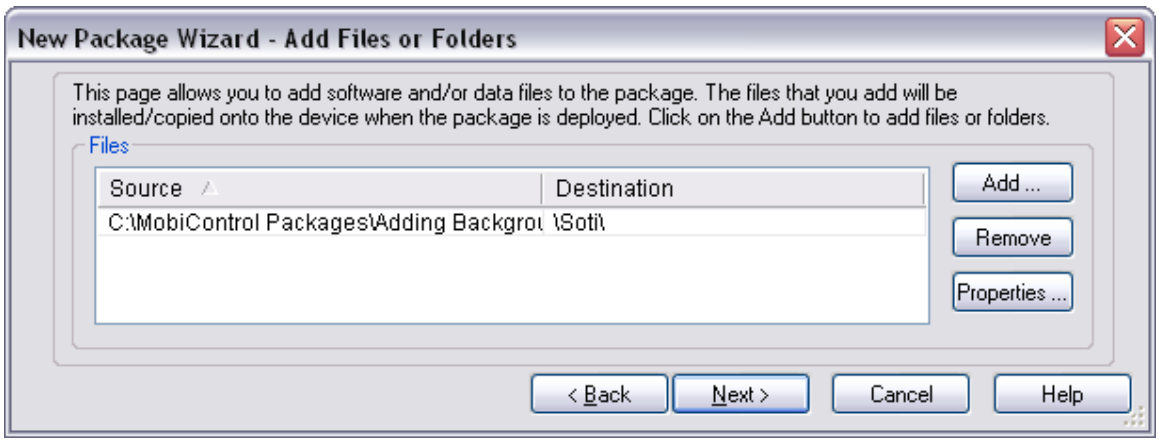


2. Add a post-install script.



3. Add files to the package.

   Add a `.bmp` file that is 225 by 32 pixels, and tell the package editor where on the device the `.bmp` image will be stored. In this example, it will be stored on the device in the `\SOTI\` folder.

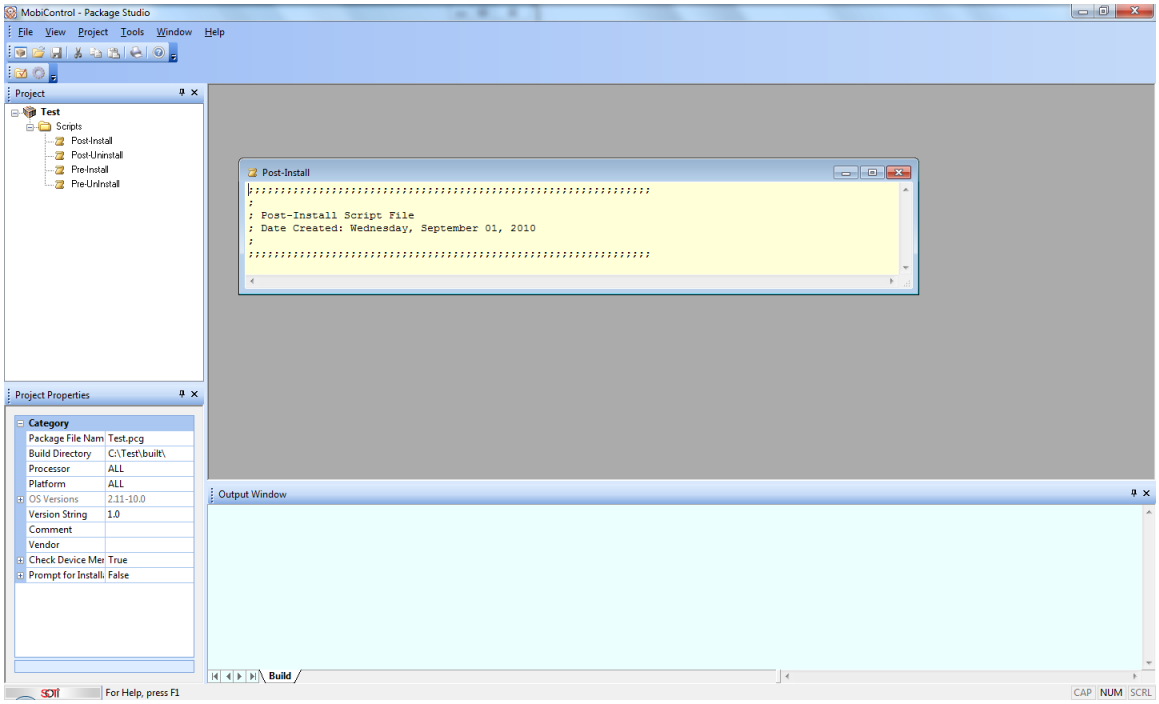


4. Edit the post-install script.

   Add one line:

   ```
   writeprivateprofstring Kiosk LoginBanner
   "\FOLDERNAME\FILENAME.bmp"
   ```

   Replace "`FOLDERNAME`" and "`FILENAME`" with the correct folder and file names.



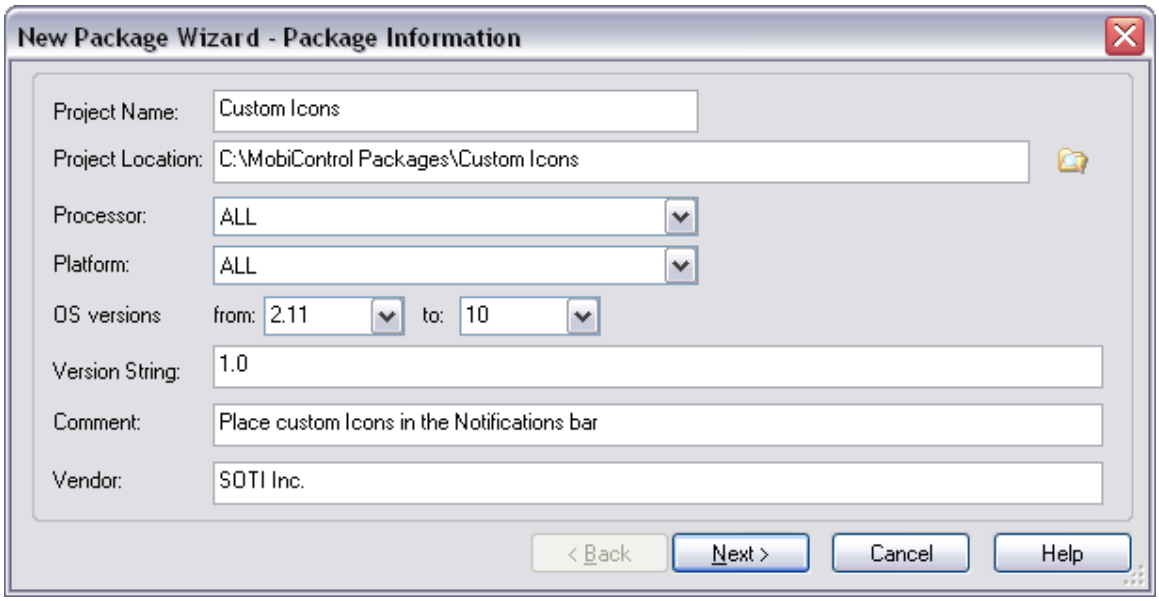
5. Build the project.

   Once you have completed editing the post-install script, you should be able to build the project and deploy it to devices.

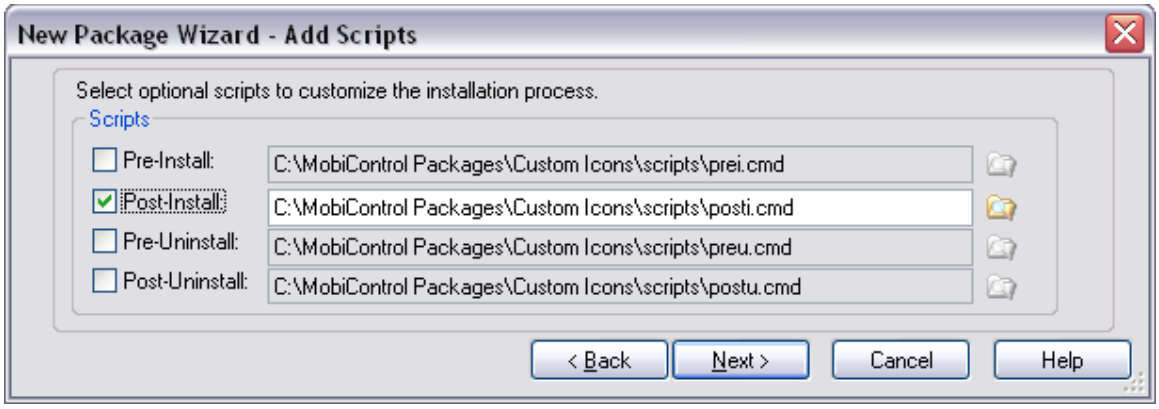
Custom Notification Icons

If you would like to add a custom notification icons to your lockdown follow the steps outlined below:

1. Create a new package using Package Studio.



2. Add a post-install script.

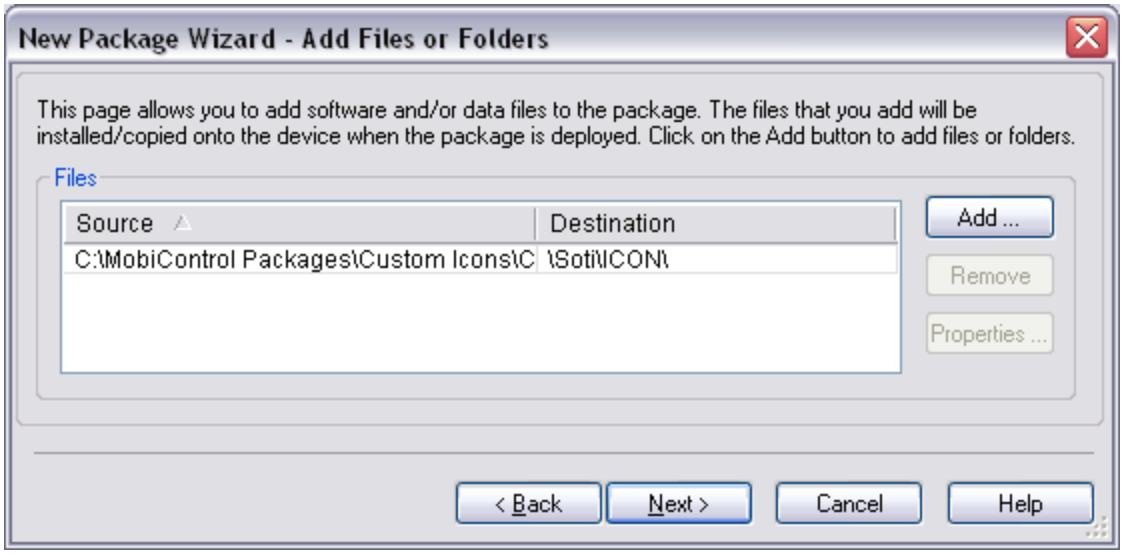


3. Add files to the package.

The image file must be 16 pixels in height and the width must be an integer multiple of 16. Each multiple of 16 pixels will determine how many icons are available for use. Now, decide where on the device the image is going to be stored. For example, I have chosen to store it on the device in the `\SOTI\ICONS\` folder. The example image is 48 pixels wide by 16 pixels high, which will make 3 icons available for display.

NOTE:

The first pixel in the top left corner of the image will set which color is transparent when the icons are displayed.



Once you have selected the location to store the file, finish the New Package Wizard.

4. Edit the Post-Install script.

   This script will contain different registry settings and commands to install the icon and display it.

   First, prepare the registry for the new settings.

   ```
   regset HKLM\Software\Apps\SOTI\MobiControl LockdownNotifications
   regset HKLM\Software\Apps\SOTI\MobiControl\LockdownNotifications
   001_IMAGE \SOTI\ICON\CustIconExample.bmp
   regset HKLM\Software\Apps\SOTI\MobiControl\LockdownNotifications
   001_STATE dword:0
   ```

   The first line in the script creates a new folder, "`LockdownNotifications`." The second line creates an entry in the `LockdownNotifications` folder called `XXX_IMAGE` with a value of `\SOTI\ICON\CustIconExample.bmp`. This is the location of the image file on the device. The third line creates a `dword` value, and this will tell the kiosk which icon in the image to display. Going to the example image above, when we give a `dword` value of `0`, nothing will be displayed. However, if we give a `dword` value of `2` the MobiControl icon will be displayed.

   The very first time you create these entries in the registry, or if the image location gets changed, you must restart MCKiosk. This can be done with the script below. It will cause MCKiosk to reload with a delay of half a second:

   ```
   Start /wait MCKiosk -Quit
   Sleepex 500
   Start MCKiosk
   ```

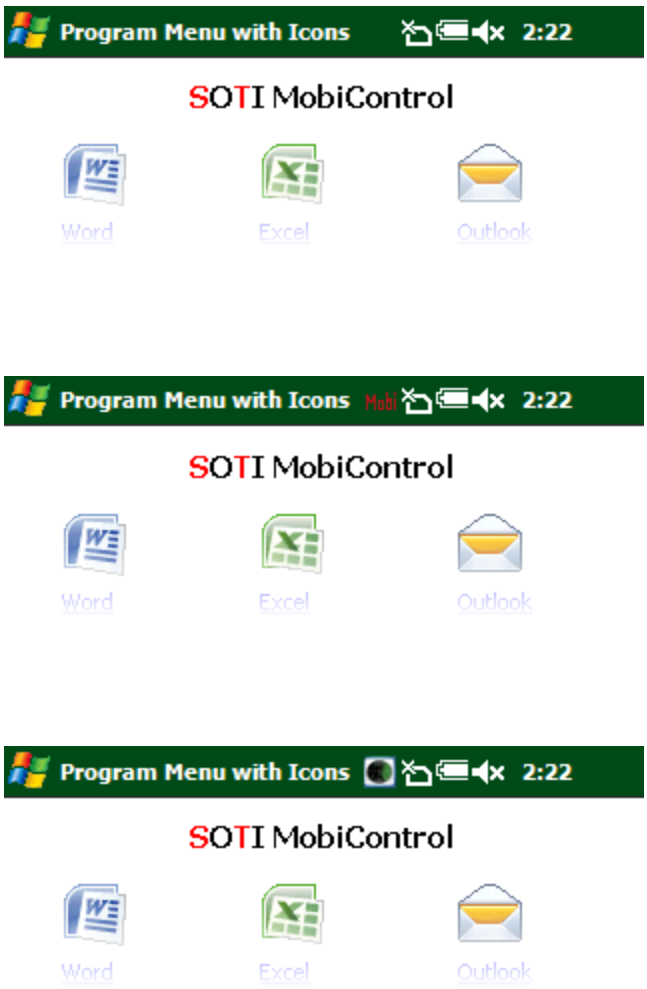
5. Switch to the correct icon.

   Now that you have successfully edited the registry, only one registry change is required to switch between the different icons. This is done by using the following command:

   ```
   regset HKLM\Software\Apps\SOTI\MobiControl\LockdownNotifications
   001_STATE dword:#
   ```

   where "`#`" is the index of icon you would like. If the number being entered is not valid, no icon will be displayed. When changing the `dword` value, the icon will change instantly. This line can be placed anywhere, in any script, to display or change the icon.

6. Deploy the package.
   Once you finish editing the script, and you are ready to deploy the package to the devices.



Navigation bars with no icon, "Mobi" text custom notification icon, and world custom notification icon

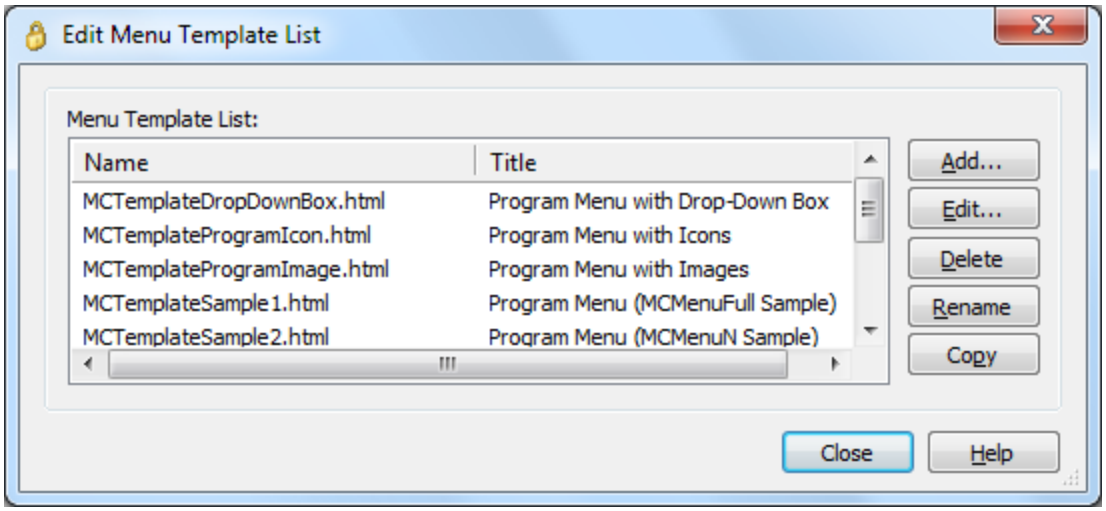
For further assistance, please contact us.

Customizing Lockdown Menu Templates

MobiControl allows you to modify pre-configured HTML menu templates or to build your own HTML menu templates. A menu template is an HTML file with special menu tags that get replaced by MobiControl when it generates the menu. Essentially, the menu tags get replaced by the menu item links that you configure for your program menu. The table below describes the special menu tags that get replaced in the HTML file.

The easiest way to create a custom program menu template is to make a copy of one of the default templates, customize it, and then add it to the list of available templates:

1. Select **Edit** in the **Lockdown Configuration** dialog box.
2. Create a copy of one of the default templates listed in the **Templates** dialog box. (Copy and paste it into another folder, e.g. My Documents.)
3. Edit the copied file according to the guidelines below and name the file appropriately.
4. Add the new template by selecting the **Add** button in the **Templates** dialog box.



Edit Menu Template List dialog box

The following table describes menu tags:

<table>
<tr><th>Tag Name</th><th>Description</th></tr>
<tr><td><MCMenuFull></td><td>This tag gets replaced with the full menu list that the user has configured. The menu items are separated by carriage returns.

Sample Menu Entries:
Pocket Word (\windows\pword.exe)
Pocket Excel (\windows\pxl.exe)
My Website (mywebsite.com)

Template:
<html>
<body>
<MCMenuFull>
</body>
</html>

Resultant Menu:
<html>
<body>
Pocket Word

Pocket Excel

My Website

</body>
</html></td></tr>
<tr><td><MCMenuN>
where "N" is the menu item number</td><td>This tag allows you to place each complete menu item where you want it in the HTML.

Sample Menu Entries:
Pocket Word (\windows\pword.exe)
Pocket Excel (\windows\pxl.exe)
My Website (mywebsite.com)

Template:
<html>
<body>
1. <MCMenu0>

2. <MCMenu1>

3. <MCMenu2>

</body>
</html>

Resultant Menu:
<html>
<body>
1. Pocket Word

2. Pocket Excel

3. My Website

</body>
</html></td></tr>
</table>

Tag Name	Description
<MCLinkN> and <MCDispN> where "N" is the menu item number	These tags let you further separate the menu item to be inserted into the "link" and the "display" text and control where in the HTML template they will be inserted.

Sample Menu Entries

Pocket Word (\windows\ pword.exe)

Pocket Excel (\windows\ pxl.exe)

My Website (mywebsite.com)

Template

```
<html>
 <body>
1. <a
href="<MCLink0>">
<font size=2>
<MCDisp0> </font>
</a> <br/>
2. <a
href="<MCLink1>">
<font size=2>
<MCDisp1> </font>
</a> <br/>
3. <a
href="<MCLink2>">
<font size=2>
<MCDisp2>
</font></a> <br/>
</body>
</html>
```

Resultant Menu

```
<html>
 <body>
1. <a href= "
file://\windows\pword.exe
"> <font size=2>Pocket
Word </font> </a> <br/>
2. <a href=
"
file://\windows\pxl.exe">
<font size=2>Pocket Excel
</font> </a> <br/>
3. <a href=
"http://MyWebsite.com">
<font size=2>My Website
</font> </a> <br/>
 </body>
</html>
```

Tag Name	Description
<MCExeIconN> where "N" is the menu item number	This tag lets you display the built-in icon for an application executable that is in the program menu. Sample Menu Entries: Pocket Word (\windows\pword.exe); Pocket Excel (\windows\pxl.exe); Calculator (\windows\calc.exe) Template: `<html> <body> 1. <a href=" <MCLink0>"> <img src=" <MCExeIcon0>"> </a>   2. <a href=" <MCLink1>"> <img src=" <MCExeIcon1>"> </a>   3. <a href=" <MCLink2>"> <img src=" <MCExeIcon2>"> </a>   </body> </html>` Resultant Menu: `<html> <body> 1. <img src= " %ExeIcon_ 1%%MCSTABLESTOREDIR%\ Lockdownimage\ MCLD_pword.bmp"> 2. <img src= " %ExeIcon_ 2%%MCSTABLESTOREDIR%\ Lockdownimage\ MCLD_excel.bmp"> 3. <img src= " %ExeIcon_ 3%%MCSTABLESTOREDIR%\ Lockdownimage\ MCLD_calc.bmp"> </body> </html>`

<table>
<tr><th>Tag Name</th><th>Description</th></tr>
<tr><td><MCDispImgN>
where "N" is the menu item number</td><td>This tag lets you associate a picture with an entry in the lockdown screen.
<table>
<tr><th>Sample Menu Entries</th><th>Template</th><th>Resultant Menu</th></tr>
<tr><td>Terminal Emulator (\Appl\Term\Term.exe)
Credit Card Sales (\Appl\CCard\CCSales.exe)
My Website (mywebsite.com)</td><td><html>
<body>
1. <a href= "<MCLink0>"> <img src =" <MCDispImg 0>">

2. <a href= "<MCLink1>"> <img src= " <MCDispImg 1>">

3. <a href= "<MCLink2>"> <img src= " <MCDispImg 2>">

</body>
</html></td><td><html>
<body>
1. <img src = "%MCSTABLESTOREDIR%\ Lockdownimage\ Term.png">

2. <img src= "%MCSTABLESTOREDIR%\ Lockdownimage\ CreditCardSales.jpg">

3. <img src= "%MCSTABLESTOREDIR%\ Lockdownimage\ MyWebsite.jpg">

</body>
</html></td></tr>
</table></td></tr>
</table>

Including Pictures in Menu Templates

You can insert images into your template by simply using the Insert Image feature in the built-in HTML Template Editor. MobiControl will deliver the image to the device. Alternatively, if you do not want to use MobiControl to deliver the image, you can simply specify in the HTML template the full path to the graphic for where it will be found on the mobile device (e.g. `<img src="file://\IPSM\images\CompanyLogo.jpg">`).

Using MobiControl Script Variables

If you generate your own custom menu template, you can use MobiControl script variables in your menu template. Using script variables allows you to display device or system information in the lockdown menu. Please see the "Script Variables" topic on page 424 for a full list of the various script variables that are available.

NOTES:

- MobiControl script variables are case-sensitive.
- When you use a script variable, you must enclose the variable name between "%" characters, in the same way that you would use them in an actual script.

EXAMPLE:

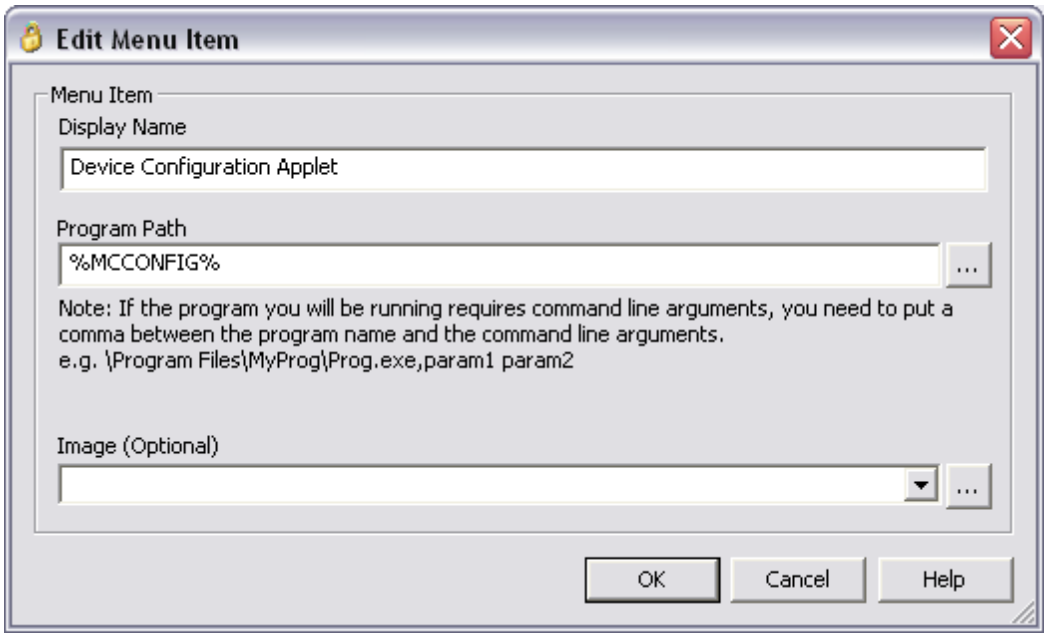
If an HTML template were to contain the line shown below, then when the lockdown menu is displayed on the device, the variable (including the leading and trailing "%" characters) would be replaced by the name of the device.

```
Device Name: %MCDEVICENAME%
```

Linking to the MobiControl Device Configuration Applet

The MobiControl device applet that is normally accessed by tapping on the MobiControl icon on the Today screen or system tray of the device contains a bounty of useful status information. This information can be very useful when trying to troubleshoot a problem in the field, for example resolving connectivity issues between the device and the MobiControl Deployment Server.

To create a link to the applet from the lockdown program menu add a program entry to the following path: `%MCCONFIG%`



Program menu entry for MobiControl Configuration Applet

IMPORTANT:

For WM devices, since you can't specify an exact page you can simply embed the following macro into the template: %MCCONFIG%

If %MCCONFIG% was specified in a earlier version of MobiControl with specific Tab controls to display, this option is no longer valid, but will still open the Configuration Applet.

NOTE:

When the MobiControl Device Configuration Applet link is applied in the lockdown menu, the end user has limited functionality of the settings. This is to prevent unauthorized modifications. The only functions that the user can access are the manual **Connect/Disconnect** button and **Log to File** check box in the **General** Tab, and the **Add** and **Test** buttons in the **Servers** tab. When the lockdown is accessed in Admin mode, the administrator has full control of the MobiControl Device Configuration Applet settings.

Embedding custom data variables

To insert custom data to your lockdown, click on **Edit** and **Insert Custom Data** button or click on the **Insert Custom Data** button on the toolbar. A new dialog window will open which will give you the option to select which custom data profile that has been previously created which you wish to include in your lockdown. As an alternative to pre-defined custom data you can explicitly include the Custom Data URL (REG://...) in the template.

If you wish to have a custom refresh mechanism within your lockdown use the following variable which refreshes the data on your lockdown screen: <a href="mc://home">Refresh<a>

EXAMPLE:

If an HTML template were to contain the line shown below, then the variable (including the leading and trailing "%" characters) would be replaced by the value.

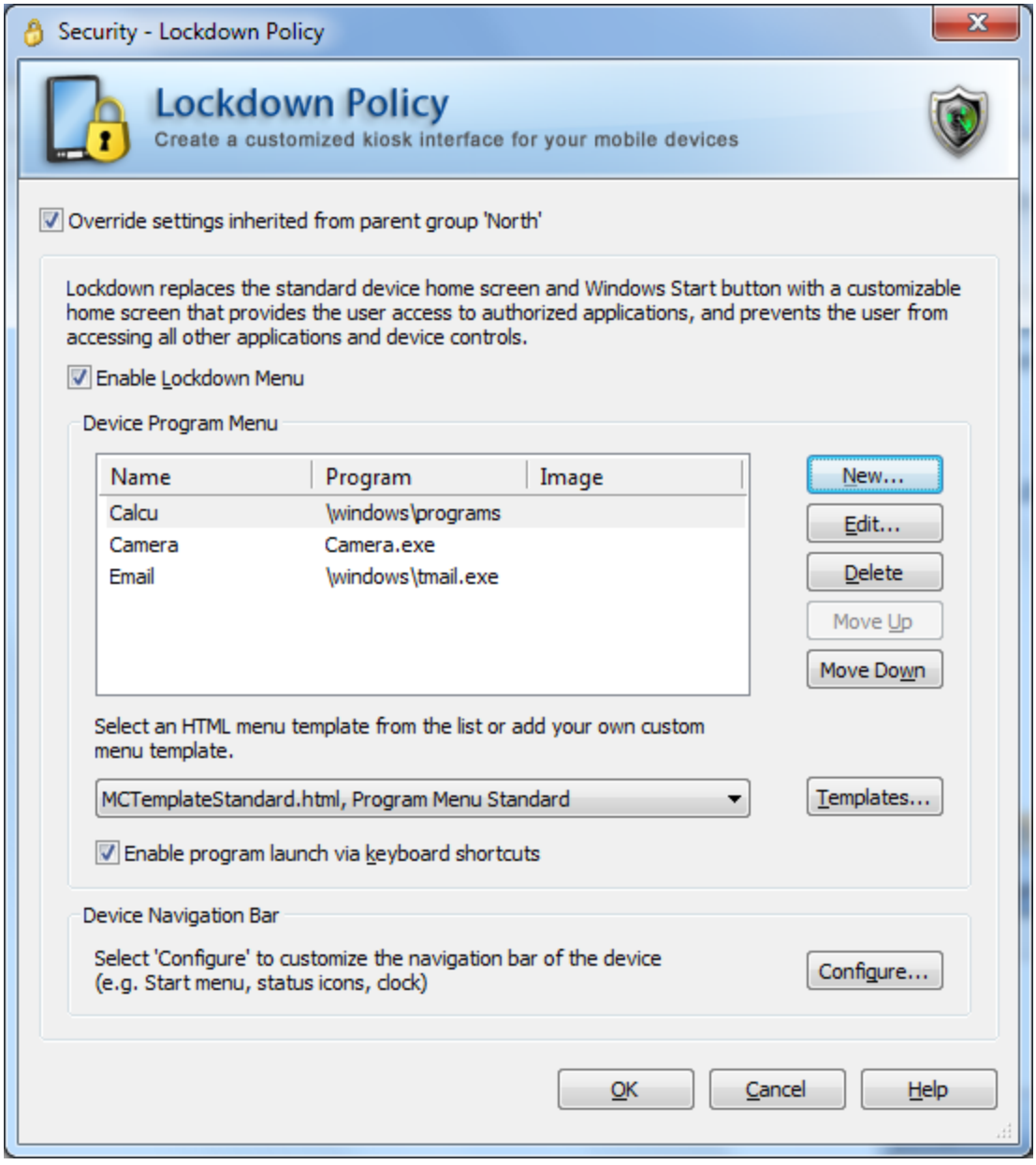
MobiControl Agent: %REG://HKEY_Local_
Machine\Software\APPS\SOTI\MobiControl\DeviceAgent?VN=Connection%
<a href="mc://home">Refresh<a>

Lockdown Menu Template Editor

In MobiControl, you can generate your own custom menu template. To edit the custom template, you can use your favorite HTML editor, or use the built-in editor available in MobiControl. When editing the HTML file be sure to preserve the special MobiControl Menu tags. These special tags are automatically replaced with the appropriate Program Menu entries by MobiControl.

Lockdown Menu

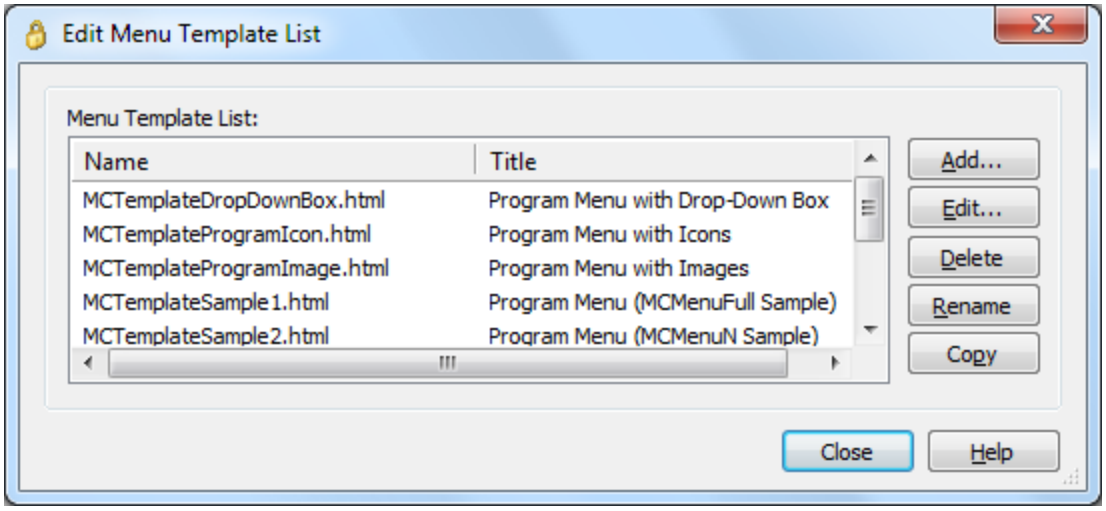
In the lockdown menu, you can select a template available in MobiControl. If you wish to use your own, click the **Templates** button and you will reach the **Template Menu List.**



Lockdown menu main screen

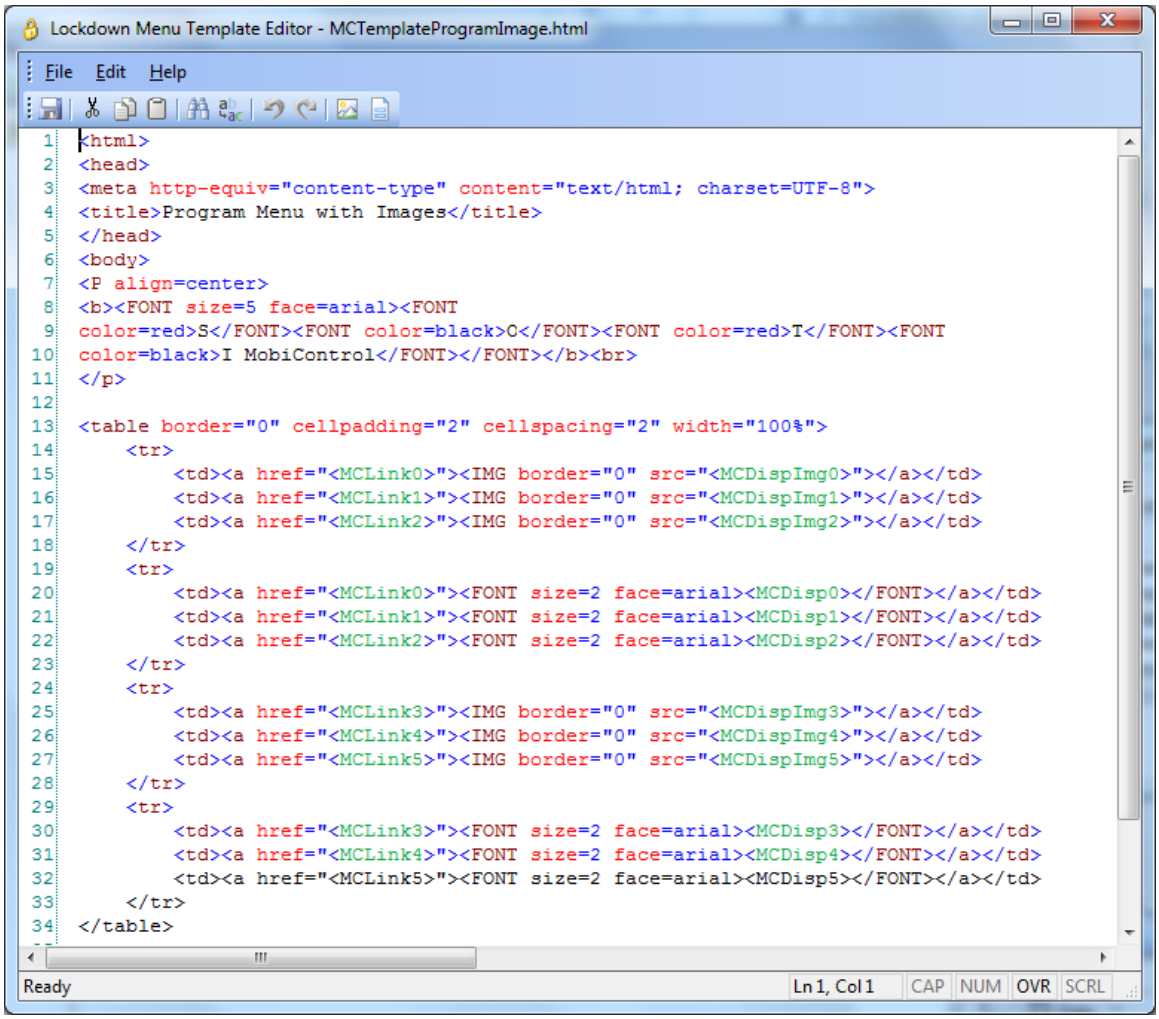
Edit Menu Template List

In the **Edit Template Menu List** dialog box, click **Add** and navigate to the location of your customized lockdown page and select it. You will see the customized menu template in this list now. You can chose to edit this template further by clicking on **Edit** and launching the lockdown menu template editor, or click on **Close** and then select the template from the **Lockdown Menu**.



Edit Menu Template List dialog box

You can edit the lockdown menu templates using the built-in HTML editor. In this editor, all the tags specific to MobiControl's lockdown templates are automatically colored green to highlight the special syntax. After saving a modified template, be sure to select the template file in the combo selection box on the main **Lockdown Configuration** page.



Lockdown menu HTML editor

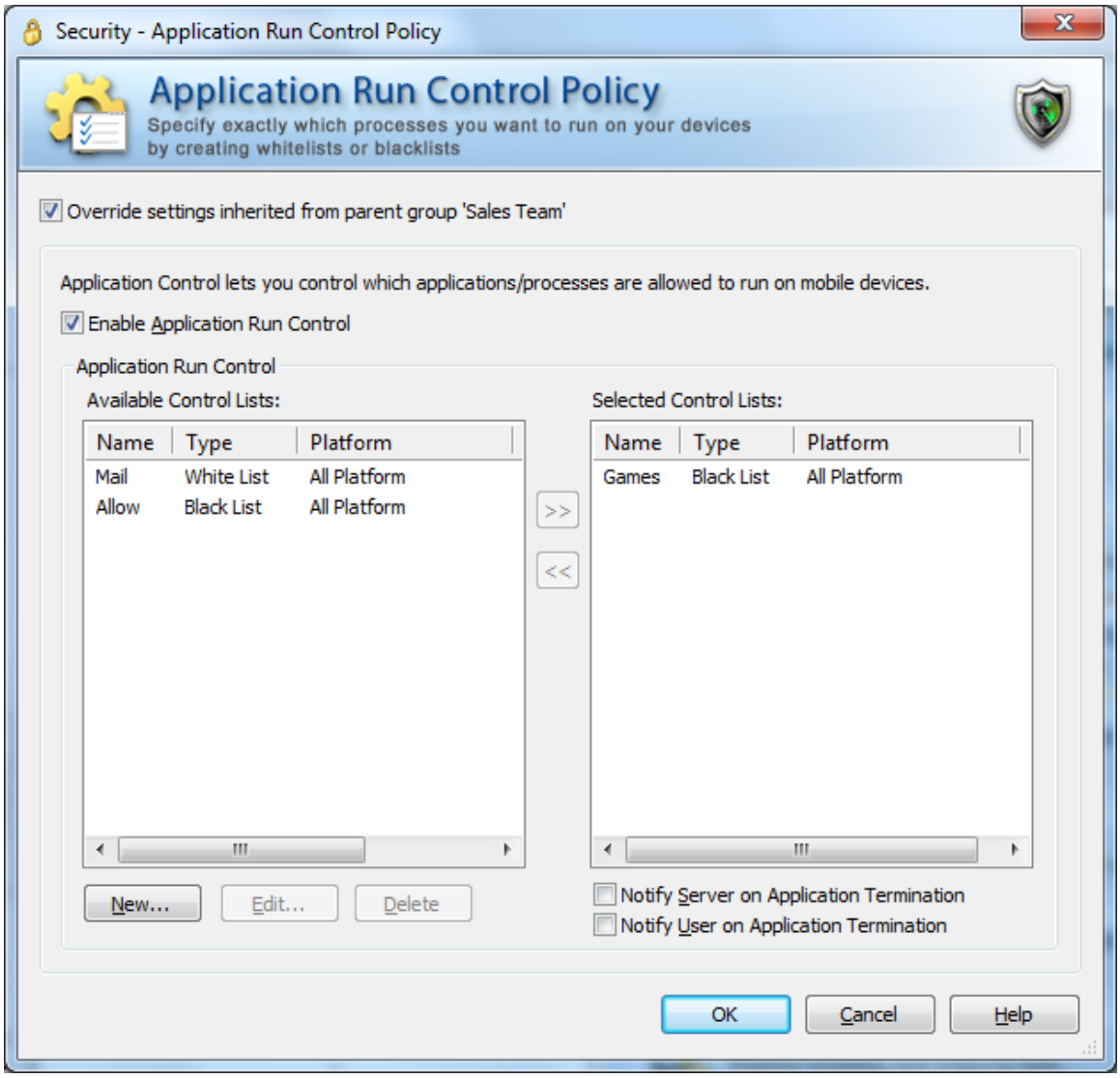
TIP:

You can easily include a graphic in your HTML template by selecting the **Insert Image** menu option in the HTML Editor.

Application Run Control

The easy availability of applications—games, consumer-oriented utilities and third party tools—for mobile devices results in end users installing and running unauthorized personal programs and recreational software on devices meant for business use. In addition to contributing to memory and battery life overhead, this situation also contributes to productivity losses. The installation of unauthorized and unapproved non-business applications contributes to a significantly higher volume of support calls, increasing the IT help desk's support burden. Most critically, it is imperative for security-conscious users to control and restrict the unauthorized installation of personal applications to ensure compliance with strict mobile data protection requirements.

MobiControl's application run control features reduce the risk of leakage of sensitive data and complement the existing network security model by preventing the introduction of malware and viruses into the network through the mobile devices. Additionally, it also allows memory management on the mobile devices to free up resources taken up by unnecessary processes, and allowing for better device performance. MobiControl integrates tightly with the operating system to prevent restricted applications from running entirely on the mobile device, making it much more efficient than competing white list and black list solutions which use CPU and battery-consuming processes to monitor for and destroy restricted applications.



Application Run Control dialog box

For assistance with Override Settings Click Here.

Application Run Control Modes

MobiControl provides two modes of operation for Application Run Control with two control list types:

1. The **black list**, or list of restricted applications, allows IT administrators to ensure that an application will not be allowed to execute on the device. The MobiControl Device Agent prevents any black-listed processes from executing on the device.
2. The **white list**, or list of approved/allowed applications, limits what programs can be executed on the devices. Only the applications and processes included in the white list are allowed to execute on the device. This provides an added layer of security for organizations concerned about unknown processes and applications that may be introduced to the device—maybe without the end user being aware of it, as is frequently the case with viruses, spy ware and other malicious applications.

NOTE:

If an application is being run from the lockdown, and it is blacklisted on the device, the application will still run as the lockdown takes precedence over the blacklist.

IMPORTANT:

If the white list is not set up correctly, you may end up blocking a potential system critical applications and cause the device to crash.

To enable application run control for a device or group of devices, select **Application Run Control Policy** from the MobiControl Security Center. (Please see the "Device Security and Control" topic on page 183.)

Control List Creation Methods

IMPORTANT:

Whether you are creating a white list or a black list, the use of learning mode is strongly encouraged.

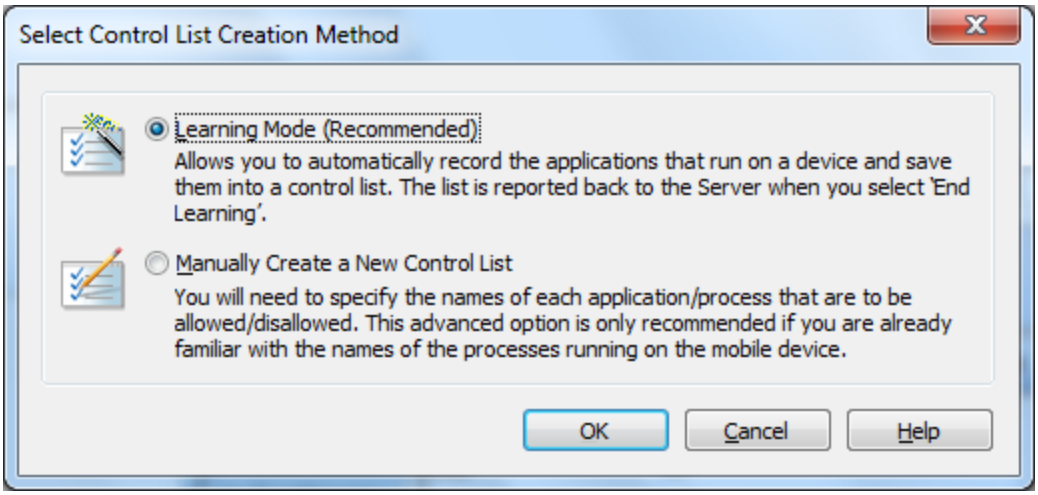
Configuration of application run control begins with the creation of an application control list. An application control list is simply a listing of the names of the executables files that correlate to the application you may wish to allow or disallow on the mobile device. For example, `pword.exe` corresponds to Microsoft Word for Windows Mobile, and `tmail.exe` corresponds to Microsoft messaging client for Windows Mobile. The categorization of the application control list, either as a white list or a black list, determines whether the specified programs will be allowed or disallowed.

Application control lists may be specified manually or they can be auto-generated using learning mode.

Learning Mode

Learning mode can only be enabled or disabled on a device that is **online**. If you right-click on a device group or an offline device, you will receive an error message if you try to enable learning mode.

Learning mode allows you to quickly and easily capture the names of all the executable processes that might be relevant to the everyday use of the device by the end user. Once generated, you may edit the list that was created. One device can be used to capture the applications that are commonly used. A control list can then be applied to a larger set of devices, for instance by applying the control list at a group level.

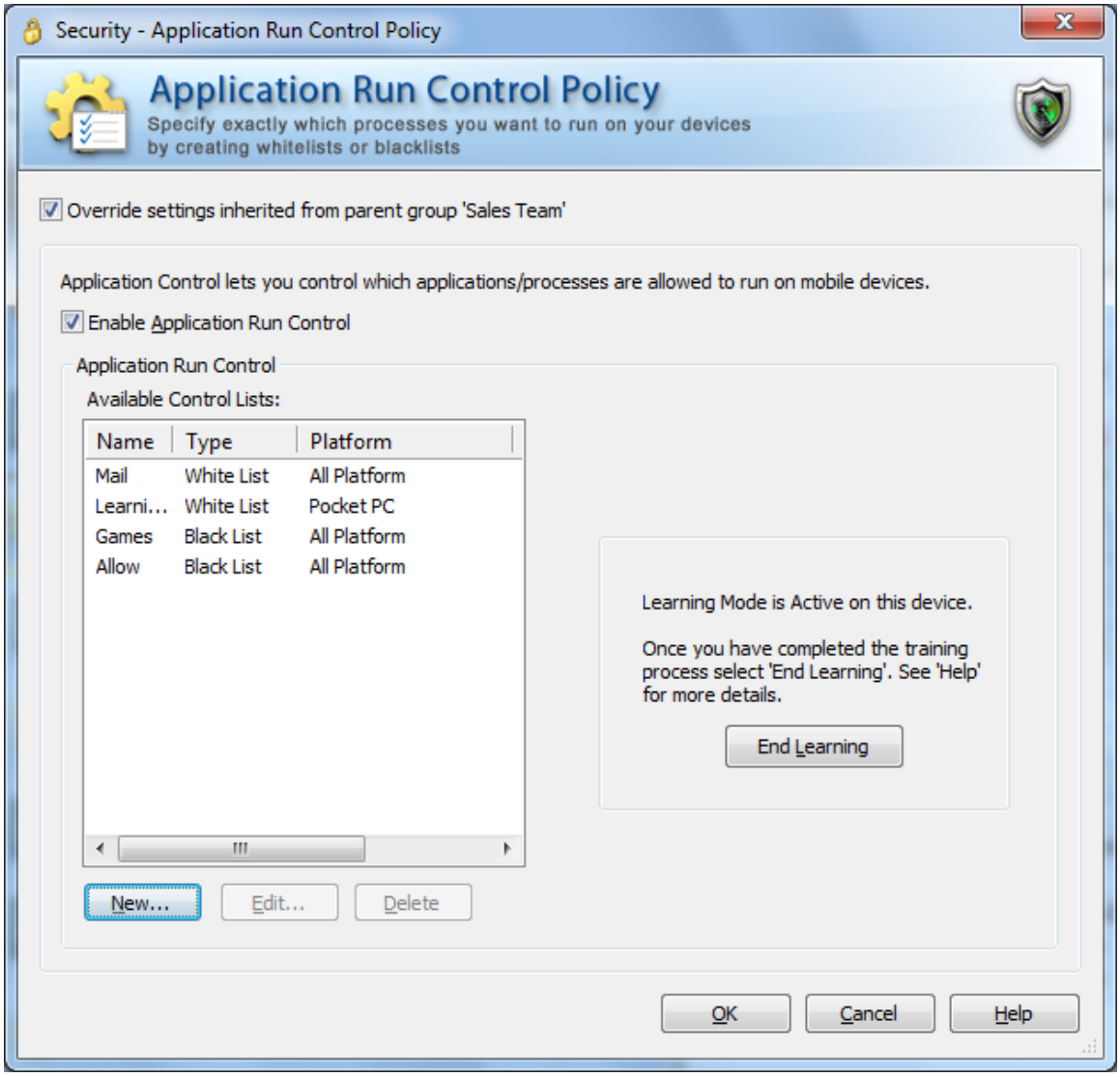


Select Control List Creation Method dialog box

Enable learning mode by selecting the **New** button in the **Application Run Control** dialog box, and then choosing **Learning Mode** in the **Select List Creation Method** dialog box.

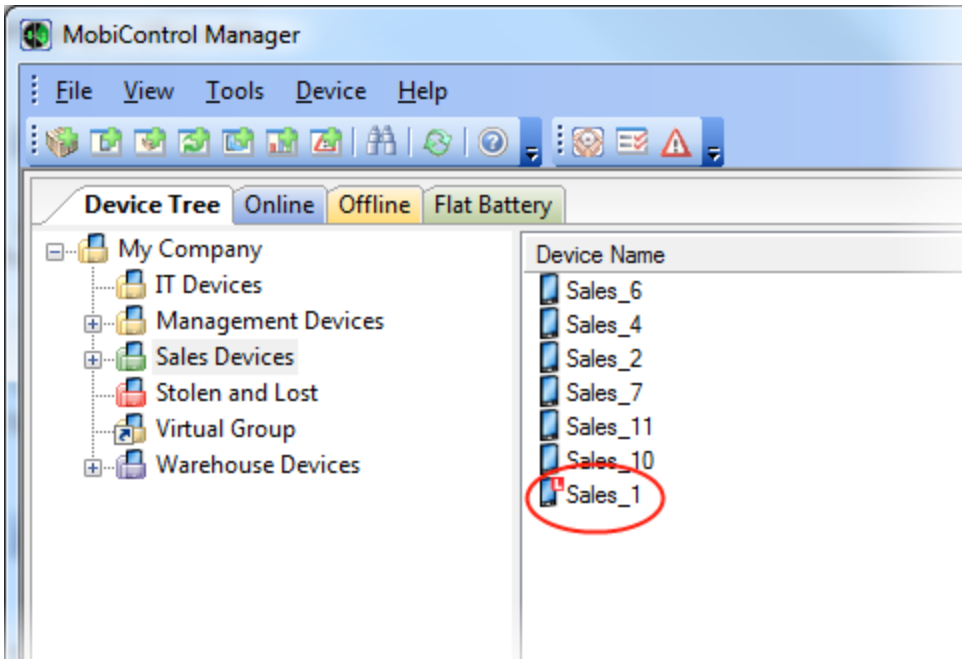
Once you have enabled learning mode, begin using the device. If you wish to develop a white list, run all the applications that the typical end user will need (i.e. Microsoft Messaging, Microsoft Word, Calendar, Contacts). Go through normal, everyday situations like making and receiving a phone call, soft-resetting the device, etc. Use the device with learning mode enabled for as long as it takes you to ensure that all the applications that your user will need to execute have been launched at some point. (You can run it for an hour, a day, a week,…)

Once you are satisfied that you have fully trained the device's application run control, click the **End Learning** button.

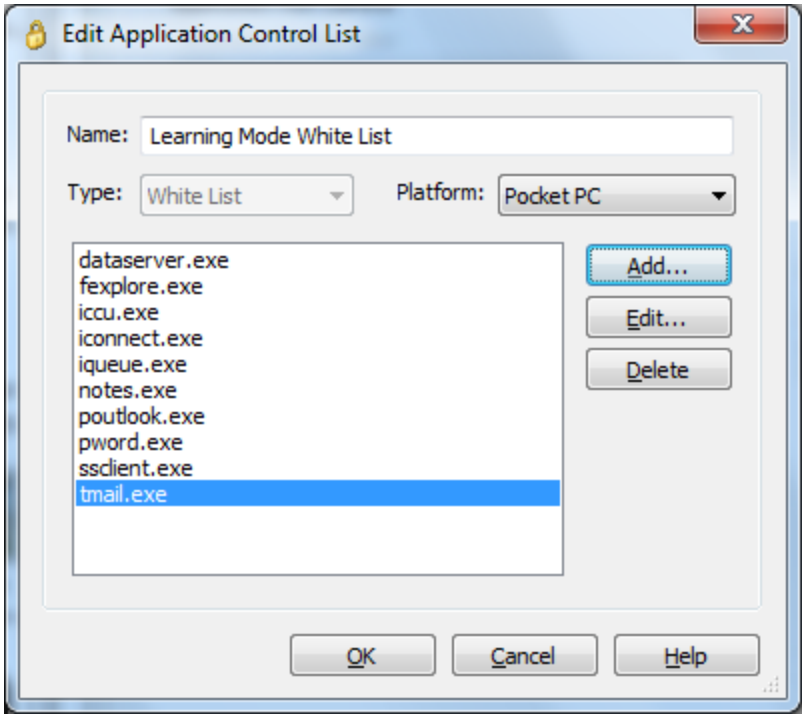


Application Run Control Learning Mode dialog box

While the device is in learning mode, a red **L** icon will appear on the device until learning mode has ended.



The list of "learned" applications will be presented to in a dialog box that allows you to edit the list. For example, you may wish to delete an application that was mistakenly executed during the learning. Before saving the control list, you must name it.

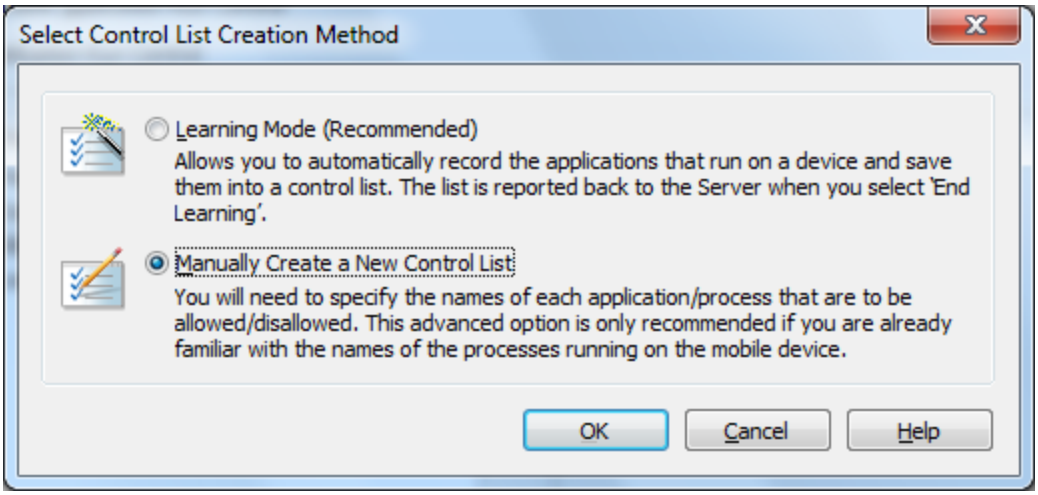


Application Run Control Learning Mode list

Now the application run control list has been created, you may assign it to various devices and groups.

If you wish to develop a black list using the Learning Mode, run all the applications that you do not want your user to be able to access (i.e. Solitaire, Bubble Breaker, Internet Explorer, etc.) Once you are satisfied that you have executed all the applications that are to be banned, click **End Learning.** Since learning mode lists all the processes that were found to be running, it is important that you go through and remove from the blacklist those application that are not to be disallowed.

Manual Mode

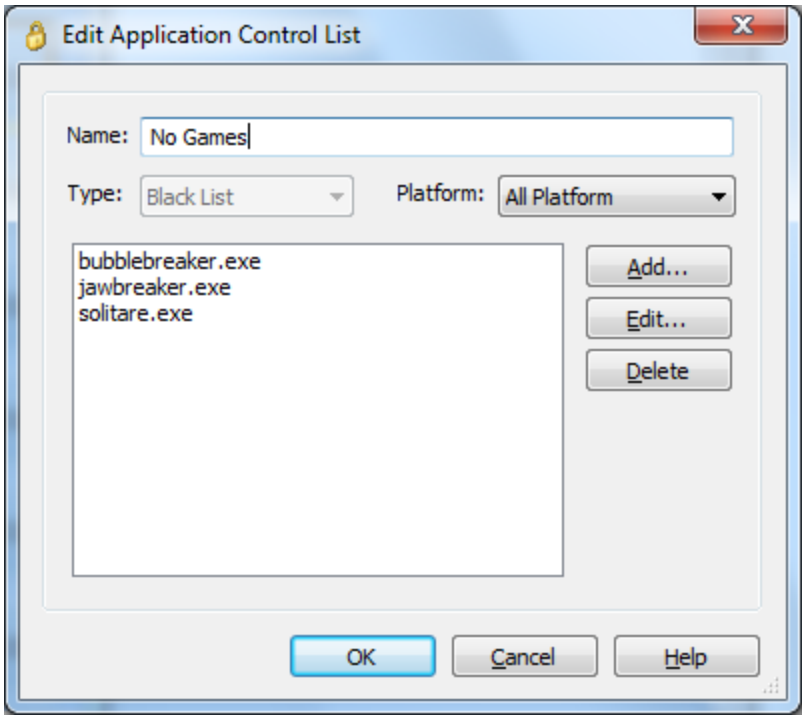


Select Control List Creation Method dialog box

Manual list creation is provided for the expert device administrator who already knows exactly which executables are to be put on the white list or black list. This advanced feature is only recommended if you have already used learning mode and are aware of the names of the executables that need to be allowed for correct device operation, and those that you wish to restrict.

You can manually create a new application control list by clicking the **New** button in the **Application Run Control** dialog box, and then choosing the **Manually Create a New Control List** option in the **Select Control List Creation Method** dialog box. The **New Application Control List** dialog pops up, allowing you to specify the application that you want to add to the list, and the platform for which this entry would be valid. This allows you to restrict applications on a device running a specific operating system (e.g. Windows Mobile 5), if you have a mix of devices with different operating systems in the same group.

Once created, the list may be applied to one or more devices or groups.



Creating a black list in manual mode

IMPORTANT:

Application run control can adversely impact the operation of the mobile device if configured incorrectly. After you have developed a control list, apply it to one or two select devices for extended field testing before expanding it to the general deployment. As a general rule, if you don't know what the executable does (e.g. `somestrangename.exe`), allow it to run instead of blocking it as it might be critical for the device's proper operation.

Modifying or Deleting a Control List

An application control list can be edited whether it is currently in use or not, but its type (white list or black list) cannot be changed once created.

An application control list can only be deleted if it is currently not selected for any devices or device groups. A control list that is listed in the **Selected** field is considered in-use, even if the application run control is disabled for the given group or device.

NOTE:

If you edit an application control list that is shared among device groups that are not subgroups of the group you are configuring, the changes will not be propagated to the other devices. The modified control list will only affect devices belonging to the group being configured or its subgroups.

Application Run Control Event Notification

Every time MobiControl's application run control feature blocks or terminates an application that is not allowed to run by the security policy in effect, it can notify the server or the user if the appropriate options are selected.

The following two options are available:

- The **Notify Server on Application Termination** option will generate a log event on the server and display it in the Event Logs for that particular device when an attempt is made to run a blocked operation. Device logs can be viewed in the MobiControl Manager by highlighting the device or the group of devices and enabling the **Logs** tab. This allows the administrators using MobiControl Manager to track any attempts by the end users to run or install unauthorized applications and ensures a higher level of monitoring.
- The **Notify User on Application Termination** option causes a message box to be displayed on the user's device when an application is blocked.

NOTES:

- When logged in as Admin on the mobile device, application control enforcement is suspended.
- Certain processes and applications are critical and necessary for stable device operation and normal execution of the MobiControlDevice Agent. These processes are automatically protected through a built-in "permanent white list" and cannot be put on a black list. Applications that are included in a lockdown program menu are automatically on a white list, and cannot be put on a black list.

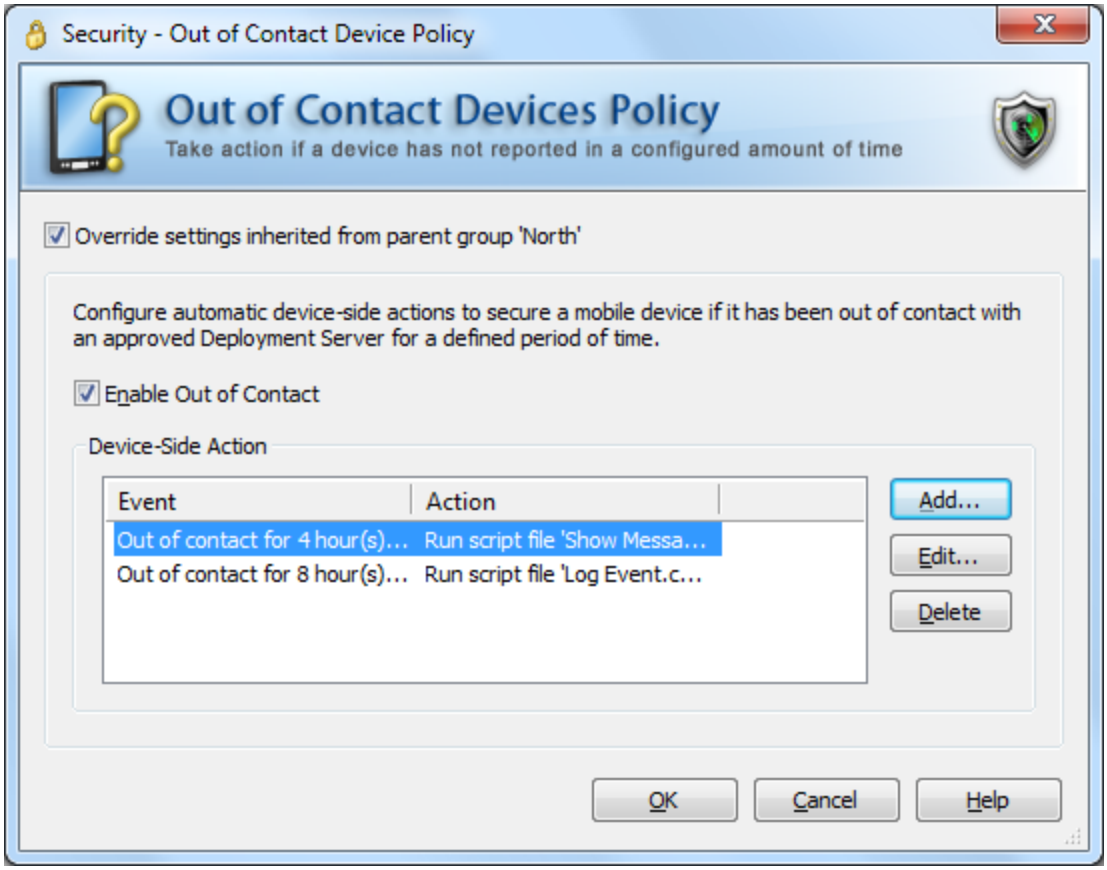
Out-of-Contact Devices

The out-of-contact devices policy dialog box allows you to manage security on "out-of-contact" devices which are not able to connect to the MobiControl Deployment Server. This feature can be used to define security actions that can be triggered if a device has not contacted the MobiControl server for a specified time interval, or has been lost or stolen and appears as offline in the device tree.

To enable the out-of-contact devices policy for a device or group of devices, select **Out of Contact Devices Policy** from the MobiControl Security Center. (Please see the "Device Security and Control" topic on page 183.)

EXAMPLE:

If a device does not contact the server for two days, you can configure it to be wiped to avoid losing any sensitive data on the device. Other actions and standard script commands can also be executed.



Out of Contact Device Security Policy dialog box

For assistance with Override Settings Click Here.

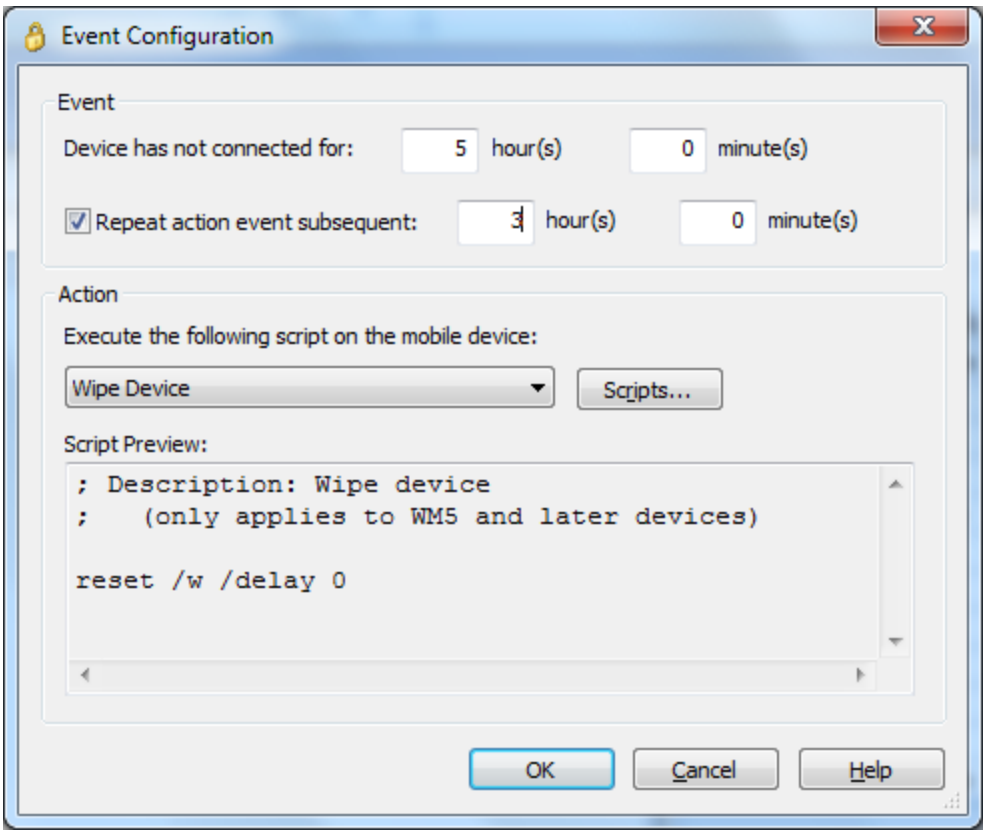
To add an event for which security actions can be specified, click the **Add** button. Click on the **Edit** button to modify an existing event or an action. Click on **Delete** to remove an event and its corresponding action from the list.

Action	Description
Add	To add an event for which security actions can be specified.
Edit	To modify an existing event or an action. Clicking this button presents the option to edit an action or the corresponding action.
Delete	To remove an event and its corresponding action from the list.

Add Event

To add an event, click the **Add** button to bring up the **Out of Contact Event Configuration** dialog box. Specify the time interval after which an action (or a script) should be triggered if the mobile device has not connected to the MobiControl Deployment Server (which is indicated by the device appearing as online in the device tree).

After you have specified the time interval, select a script to execute, or click **Scripts** to bring up the **Manage Scripts** dialog box. Please see the "Script Manager" topic on page 141 for further details.



Out of Contact Event Configuration dialog box

File Encryption

Due to the portable nature of data stored on mobile devices, there always exists the possibility of this data being found by someone other than the intended user. For instance, if a device is lost or stolen, sensitive business information (contacts, emails, spreadsheets, documents or other confidential data) may be found. Data can be easily retrieved from the device using a variety of file transfer methods (i.e. USB cradle, Bluetooth or Wi-Fi file transfer, or infrared beam).

MobiControl helps secure data stored on the mobile device and SD memory cards or storage media to help businesses achieve compliance with strict data storage and processing regulations. The file encryption feature allows encrypting data stored on a device or memory card so that it can not be accessed by an unauthorized person. This protects sensitive data if an attempt is made to extract it from the mobile device and access it on another mobile device, computer or data reader by an unauthorized person.

File Encryption Policy dialog box

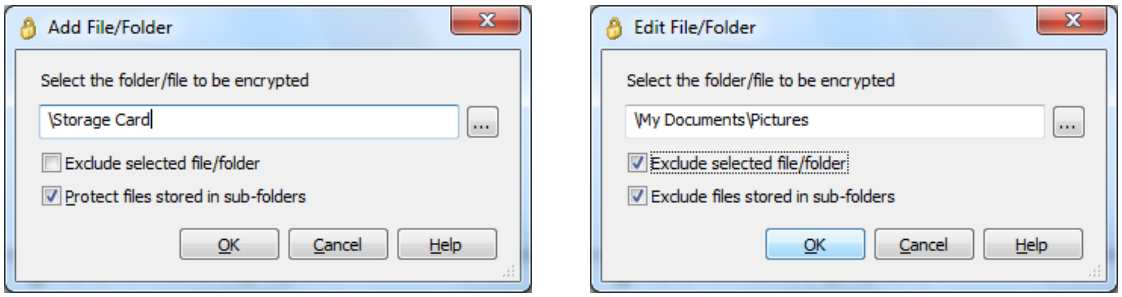
For assistance with Override Settings Click Here.

MobiControl's policy-based file encryption uses FIPS 140-2 validated AES-256 encryption algorithms to secure mobile data. On-the-fly file encryption is implemented easily and transparently without affecting

the end users experience and allows data to be encrypted and decrypted in memory when needed by mobile applications on the device. MobiControl provides granular control allowing encryption of specified files and folders, including the ability to select an entire volume such as a storage card.

To enable file encryption for a device or group of devices, select **File Encryption Policy** from the MobiControl Security Center. User authentication must be enabled prior to enabling file encryption. (Please see the "Device Security and Control" topic on page 183 and "Authentication Security" topic on page 186 for more information.)

Use the **Add** and **Edit** buttons to bring up the **Add File/Folder** dialog box to create a new entry or modify an existing entry. Individual files or entire folders can be encrypted. If a folder is selected and the option to **Protect files stored in sub-folders** is enabled, all sub-folders within it will also be encrypted. The **Exclude selected file/folder** option makes it possible to exclude a file or folder from encryption. For instance, this option can be used to exclude a folder from encryption if its parent folder is encrypted, and the option to protect files stored in the parent folder's sub-folders is enabled. When the **Exclude selected file/folder** option is selected, the option below it changes to **Exclude files stored in sub-folders.** When this second option is selected, sub-folders of the selected folder will also be excluded from encryption.



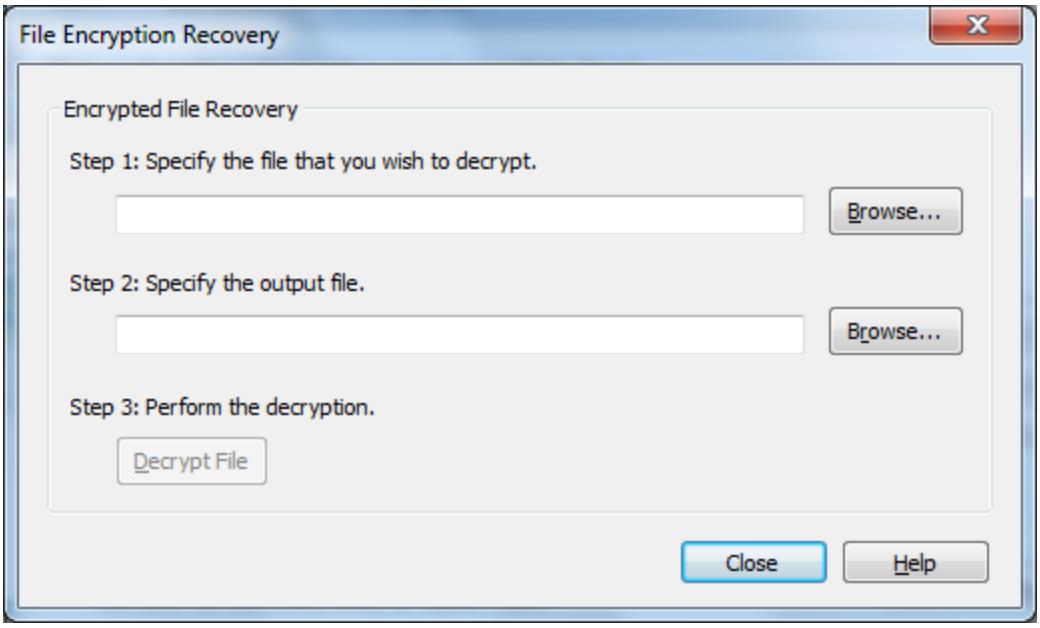
Add File/Folder dialog box for encrypting a folder (left) and excluding a folder from encryption

TIP:

MobiControl supports the use of wildcards when entering folder/file names. The asterisk ("*") substitutes for any zero or more characters, and the question mark ("?") substitutes for any one character. For example, entering "*.doc" with Protect files stored in sub-folders enabled will encrypt any document with the .doc extension on the device.

Automatic Key Archiving for Recovery of Encrypted Data

During the encryption process, the encryption key is stored on the mobile device so that any encrypted data on the mobile device or the storage / SD memory card can be accessed on the mobile device by an authenticated user. It may become necessary in certain situations to decrypt that data for use on another device (i.e. a hardware failure on the mobile device requiring the data on the storage card to be recovered on another device). If the encryption key is saved on the mobile device only and the device is stolen or damaged, the data on the accompanying storage cards would be rendered unusable as well.



File Encryption Recovery dialog box

MobiControl automatically, and transparently to the end user, archives a backup copy of the encryption key in the MobiControl database to allow the recovery of encrypted data in exceptional scenarios. This archiving of the encryption key takes place at the same time as it is generated to allow easy recovery of encrypted data, to deal with extraordinary situations and device failures.

Files can be decrypted using the MobiControl Manager. Click on the **Recover Data** button in the **File Encryption Policy** dialog box to recover encrypted files. The **File Encryption Recovery** dialog box allows you to specify the encrypted file (on a storage card or any other medium) and decrypt the file, recovering it to the destination file specified as the output file.

Device Feature Control

For security-conscious organizations and environments where privacy and information security concerns require controlling the unauthorized transfer of mobile data out of the mobile devices, MobiControl provides various on-device feature controls including the capability to block various device communications, similar to firewall functionality. MobiControl's device features control policy allows IT administrators to selectively disable device features. Applying the policy at the individual or group level allows custom profiles for different users and locations in an organization. The ability to disable or enable Bluetooth and infrared ports allows controlling whether end users can beam business cards, applications or documents to one another.

To enable device feature control for a device or group of devices, select **Device Feature Control Policy** from the MobiControl Security Center. (Please see the "Device Security and Control" topic on page 183.)

Device Feature Control Policy dialog box

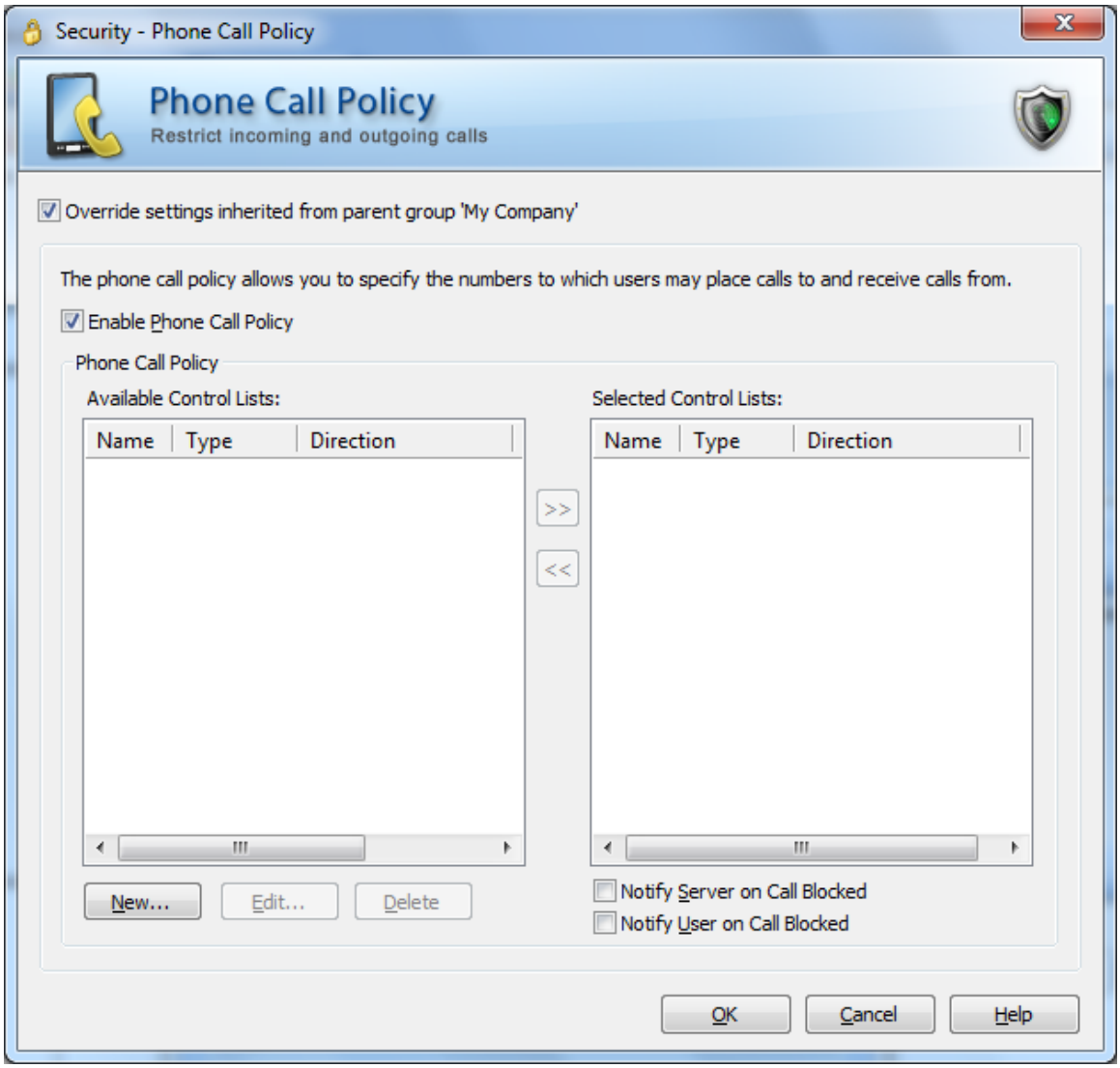
For assistance with Override Settings Click Here.

The following features can be enabled or disabled using the device feature control policy:

Field Name	Description
Disable application/hardware buttons	Disables the function buttons on PDAs that allow access to various applications on the device (i.e. Internet browser, calendar, email, phone) **NOTE:** This feature applies only to Pocket PC devices and results may vary depending on the device's manufacturer and model.
Disable Desktop ActiveSync connection	Disables the ActiveSync connection on the device so that data cannot be transferred from the device to a computer using the ActiveSync or WMDC (Windows Mobile Device Center) connection
Disable SD Card Auto-Execute	Prevents programs and applications from automatically executing from an SD or flash memory card when it is inserted in the device This feature can be used to prevent installation of unauthorized applications on the device.
Disable Phone	Restricts unauthorized voice calls and phone usage on PDAs and Mobile Devices with phone capability
Disable Bluetooth	Disables the Bluetooth wireless connection on the device preventing data transfer to and from the device **NOTE:** In certain environments, the Bluetooth radio may need to be disabled due to regulatory requirements.
Disable Beam	Disables the infra-red port on the device preventing beaming of important business data and information from the mobile device to other devices
Disable Camera	If the PDA is equipped with a camera function, this feature can be disabled to prevent unauthorized or unnecessary usage of the camera.

Phone Call Policy

MobiControl provides various on-device feature controls including the capability to block various device communications, including what numbers a device is able to call or receive calls from.



Phone Call Policy dialog box

For assistance with Override Settings Click Here.

Phone Call Policy Control Lists

MobiControl allows you to specify the numbers to which users may place calls to and receive calls from:

1. The **Available Control Lists** displays all control lists that have been defined, but currently are not in use. IT administrators are able to create several different phone call policies without having them be activated on the devices.
2. The **Selected Control Lists** displays all currently activated control lists. Only the control lists included in the selected control lists are allowed to execute on the device. This provides an added layer of security for organizations concerned about unknown phone calls that may be placed from or received by the device. This can potentially happen without the end user being aware of it, as is frequently the case with viruses, spyware and other malicious applications.

NOTE:

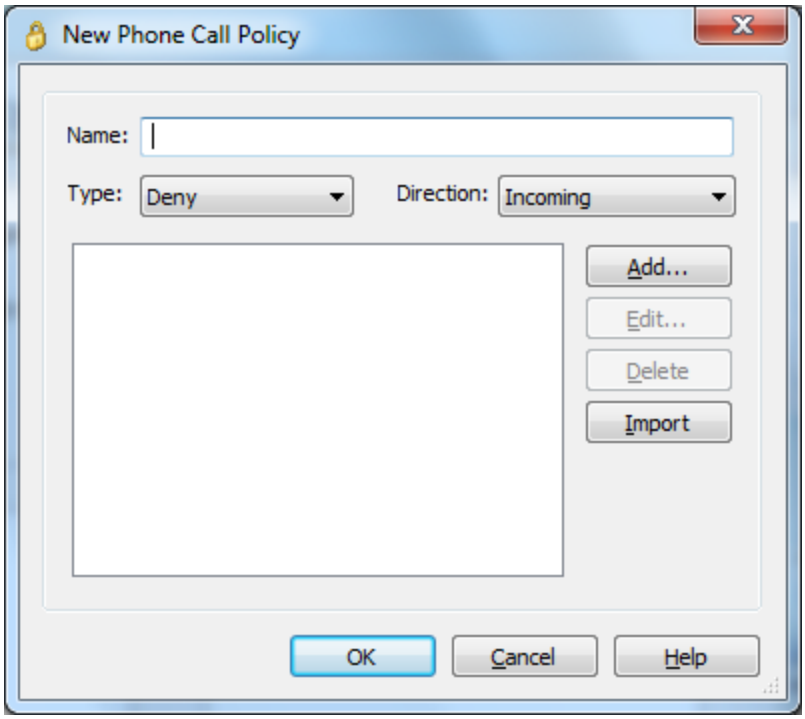
You can't have both deny and allow control lists activated at the same time. All control lists for a particular direction must be the same type.

IMPORTANT:

If the allowed list is not set up correctly, you may end up blocking or not allowing a potential system critical phone call.

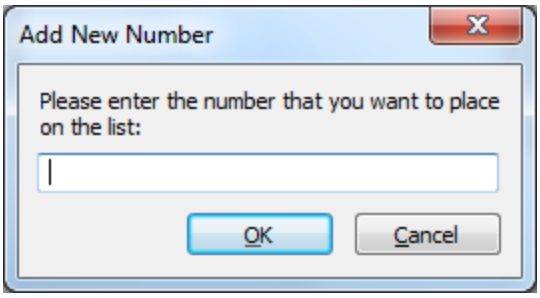
3. When the **Notify Server on Call Blocked** check box is checked, the server's log file will output all calls that were blocked, along with the phone number that was trying to call in or out for the particular device.
4. When the **Notify User on Call Blocked** check box is checked, and the user receives an incoming call from a phone number that was blocked, a message box will be displayed

To enable phone call policy control for a device or group of devices, select **Phone Call Policy** from the MobiControl Security Center. (Please see the "Device Security and Control" topic on page 183.)



New Phone Call Policy entry dialog box

Field Name	Description
New	Clicking on this button allows you to create a new phone call policy with the dialog box as shown above. Assign a meaningful name to help distinguish between the various phone call policies you may setup.
Type	The available options allowed are either Allow or Deny. The type Allow indicates the phone calls that can either be placed from the phone or received by the phone or both based on Direction set for this policy. The type Deny indicates the phone calls that can not either be placed from the phone or received by the phone or both based on Direction set for this policy. If attempting to block restricted or unknown callers simply add **<Unknown>** and/or **<Restricted>** to the deny list.
Direction	The available options are Incoming, Outgoing, or Both. Incoming indicates that this policy is for calls received by the device. Outgoing indicates that this policy is for calls placed by the device. Both indicates that the policy is for both incoming and outgoing calls. For example, you may want to allow all communication to and from your device to your IT Support team and hence you would select both in this case with the appropriate phone numbers that can be dialled to work with your support team.



Add Phone Call Policy entry dialog box

Once you have configured the Name, Type and Direction, click on **Add...** in order to enter in the phone number(s) that the policy applies to and the dialog box is displayed above.

MobiControl will compare the number either received or placed with the list of numbers mentioned in the policy and compare the exact phone number displayed with the list of numbers you provide. If you have a series of numbers that you would like to enter in, there are a few options available, which can be used in combination with each other:

1. Leverage the wild card character, which is the asterisk, or '*'. The asterisk indicates any number of digits. For example, you may want to only allow calls coming from a particular area code. In this case, you can enter in '<area code>*' as the number.

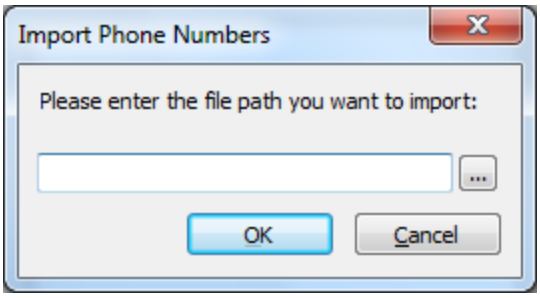
EXAMPLE:

416* would match all calls that start with 416.

2. Leverage the single wild card character, which is the question mark, or '?'. The question mark indicates any single digit.

EXAMPLE:

You may want to allow communication to a list of phone numbers that only vary by a single digit. In this case, you can enter in as an example, 444-555-123?. This indicates the policy applies to the following list of numbers:
444-555-1230
444-555-1231
444-555-1232
444-555-1233
444-555-1234
444-555-1235
444-555-1236
444-555-1237
444-555-1238
444-555-1239
Combinations of the two wild card characters can also be used if required. For example, 4??-555-12* would succeed if the phone number is 432-555-1234, but not if the phone number is 432-432-1234



Import Phone Call Policy entry dialog box

When the **Import** button is selected, the dialog box above is displayed. From here you can select any file type. MobiControl assumes that the input file format is **one phone number per line**.

EXAMPLE:

905-888-8888
519-222*
416*
Upon reading in the file, the individual numbers will be added to the list control, just as though they were individually typed in using the Add button.

IMPORTANT:

The file being imported must not contain more than 2000 lines.

Connection Security

To ensure the integrity of the corporate firewall and to provide an additional layer of security for data flowing between the mobile device and the MobiControl Manager(s) and Deployment Server(s) over public networks, SSL Communication Mode is available to provide encrypted communication. When SSL is not enabled MobiControl encrypts all communications using proprietary algorithms. SSL provides the additional benefit of standards-based authentication and encryption security.

To enable SSL communication for a device or group of devices, select **Connection Security Policy** from the MobiControl Security Center. Please see the "Device Security and Control" topic on page 183.)

This dialog box allows you to enable SSL communication for specific devices. For example, one group of devices which are in your warehouse do not need to use SSL, whereas you do want another group of devices that are in the field and communicating over public networks to use SSL.

Configure SSL device settings dialog box

For assistance with Override Settings Click Here.

The dialog box above allows you to specify the means by which you wish to have the MobiControl system deliver the Device Agent's certificate and private key to the device.

NOTE:

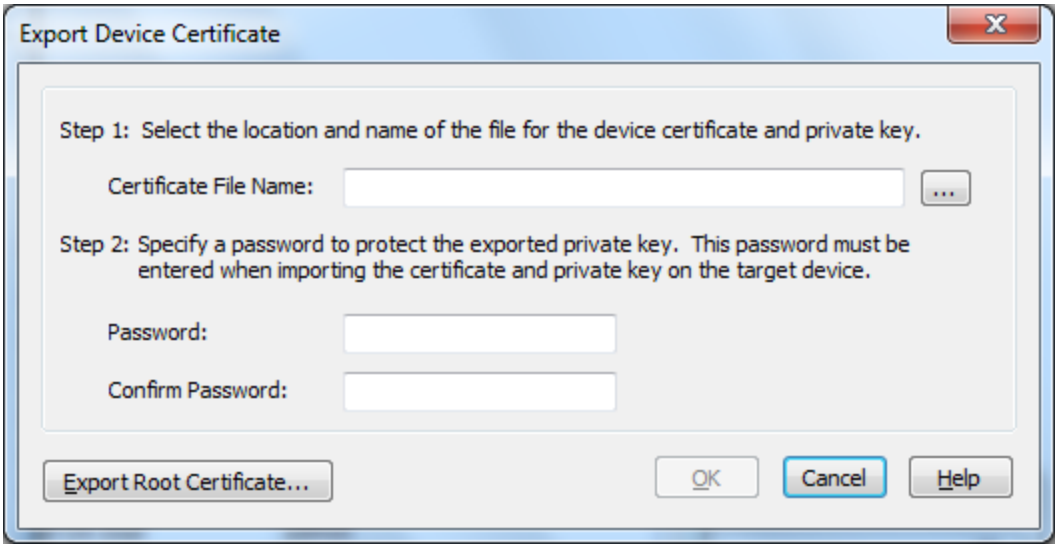
When SSL is enabled, MobiControl acts as its own certificate authority. It generates certificates for the MobiControl entities (Manager, Deployment Server, and Device Agents).

The table below summarizes the three available options for delivering and installing the device's MobiControl certificate:

Option	Description
Automatic delivery and silent installation of certificates	When this option is selected the Deployment Server will automatically deliver the certificate and private key for the device when the device connects. No user interaction is required.
Automatic delivery and prompt for password before installation on device	This option provides additional assurance that only authorized devices receive an SSL certificate and private key. When this option is selected, the Deployment Server will prompt the device user to enter the password specified in this dialog box before it delivers the certificate and private key. The device will be able to connect and stay online even if a password is not entered, however in this state the device will not receive any packages, or execute file synchronization. The administrative user can remote control the device to assist the device user with entering the password to retrieve the device certificate. The user will be given several chances to enter the correct password. If the user enters an incorrect password five times, and the **Keep Device Connected** check box is not selected, the device will be disconnected and disabled. To re-enable the device right-click on it in the device tree and select **Enable.** If the **Keep Device Connected** check box is selected, the device will remain online, and as described above, will not be eligible for package delivery or file synchronization but can be remote controlled.
Manual Installation (No automatic delivery or installation)	When this option is selected certificates and private keys will not be automatically delivered to the devices. The certificate and private key must be exported (`*.pfx` file), and delivered to the device by some means. This could be via email, file transfer, etc. **NOTE:** Importing certificates is only supported on Windows Mobile 5 devices and Windows desktop clients (Windows 2000/XP).

In all the cases above, the Device Agent stores the certificate and private key into the Windows operating system's personal certificate store. The MobiControl Root CA certificate, on the other hand, is stored in the operating system's trusted root certificate store.

Manual Installation



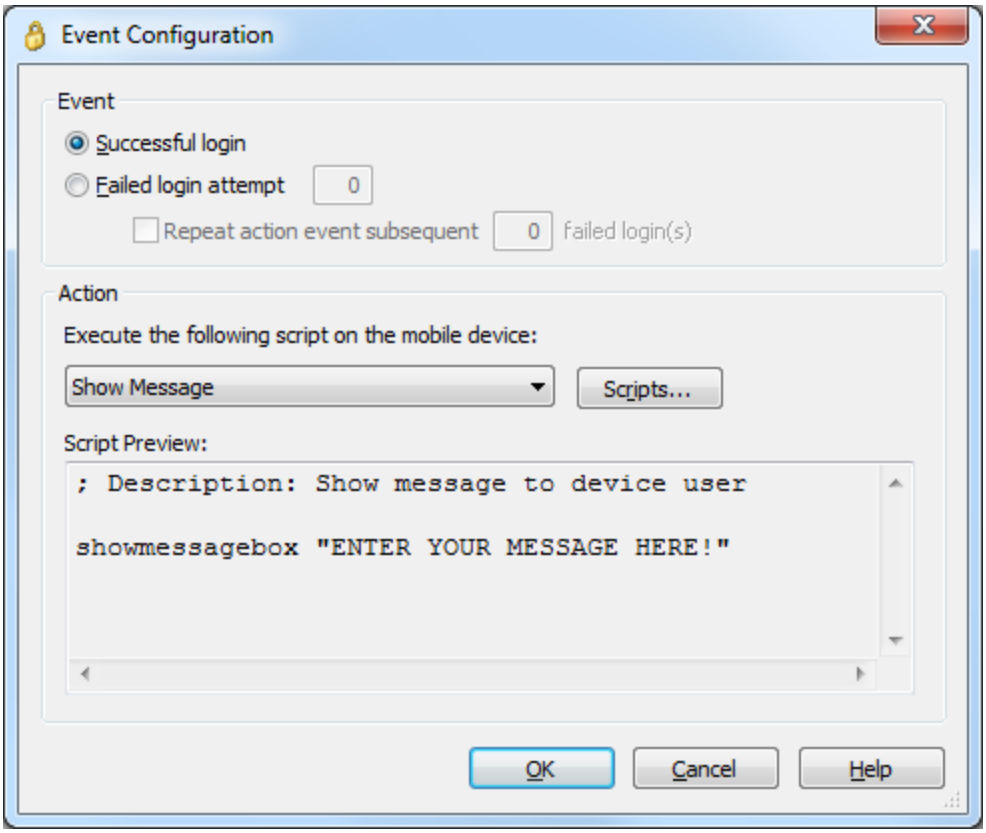
Export Device Certificate dialog box

When this option is selected, the certificate and private key must be exported (`*.pfx` file), and delivered to the device via email, file transfer, storage card, etc.

Once the `*.pfx` file has been delivered to the target device, the user must use the MobiControl applet running on the device to import it. For further information, refer to the SSL Cert tab in the mobile device configuration applet on importing the certificate. (Please see the "Mobile Device Configuration Applet" topic on page 397.

Configuring Event Scripts

Use the Event Configuration dialog box to create or edit actions for **user authentication** and device **out-of-contact** events. Events are scripts that run on the device when the specified event occurs. You can also click the drop-down box if you wish to use an existing script stored in the MobiControl database. Enter your script commands in the space provided. The **Scripts** button on the right provides shortcuts for command sets that are commonly used in action scripts. A description of these common actions appears below. Please see the "Script Command Set" topic on page 72 for more information on MobiControl's script commands.



Event Configuration dialog box

The following table describes fields in the **Event Configuration** dialog box:

Action	Description
Successful login	Will execute a selected script upon a successful login
Failed login attempt <number>	Will execute a selected script upon after a specified number of unsuccessful login attempts
Repeat action event subsequent <number> failed login(s)	Will re-execute a selected script upon a specified number unsuccessful login attempts
Scripts	Will open the **Manage Scripts** dialog box

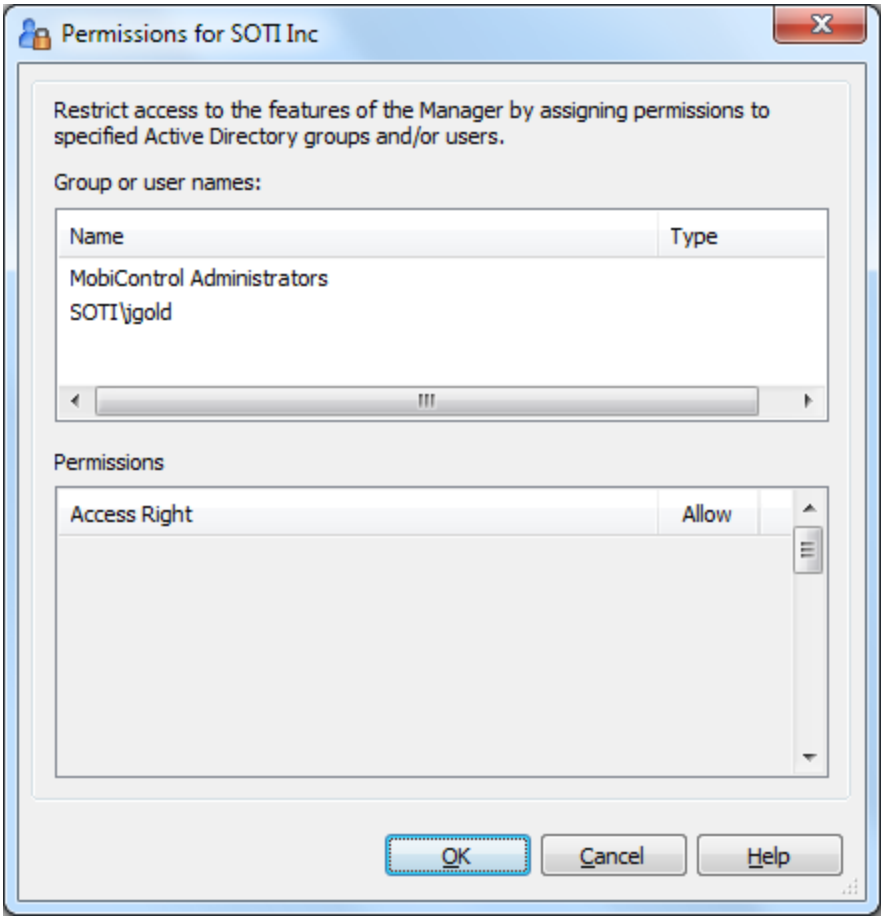
Select Script

Clicking the **Scripts** button brings up the **Manage Scripts** dialog box. You can use this dialog box to select an existing script stored in the MobiControl database for the action, to import a script from a file, or to delete a script from the database. Please see the "Script Manager" topic on page 141 for more information on MobiControl's **Manage Scripts** dialog box.

Device Group Permissions

Device group permissions allow for the segregation of MobiControl management privileges based on the device tree structure. For example, a support team operating out of California may be responsible for supporting all the devices in the western states, while another team out of New York is responsible for controlling all the devices in the eastern states. Using device group permissions, the members of the two respective teams can be granted varying levels of access to the devices in their own region (i.e. full access), and those in other regions (e.g. no access).

To enable group permissions, you must first enable the MobiControl Manager Console user security. (Please see the "Manager Console User Security" topic on page 409.) Once the Manager Console user security is enabled and configured, right-click on a group for which you would like to implement permissions and select **Group Permissions.**



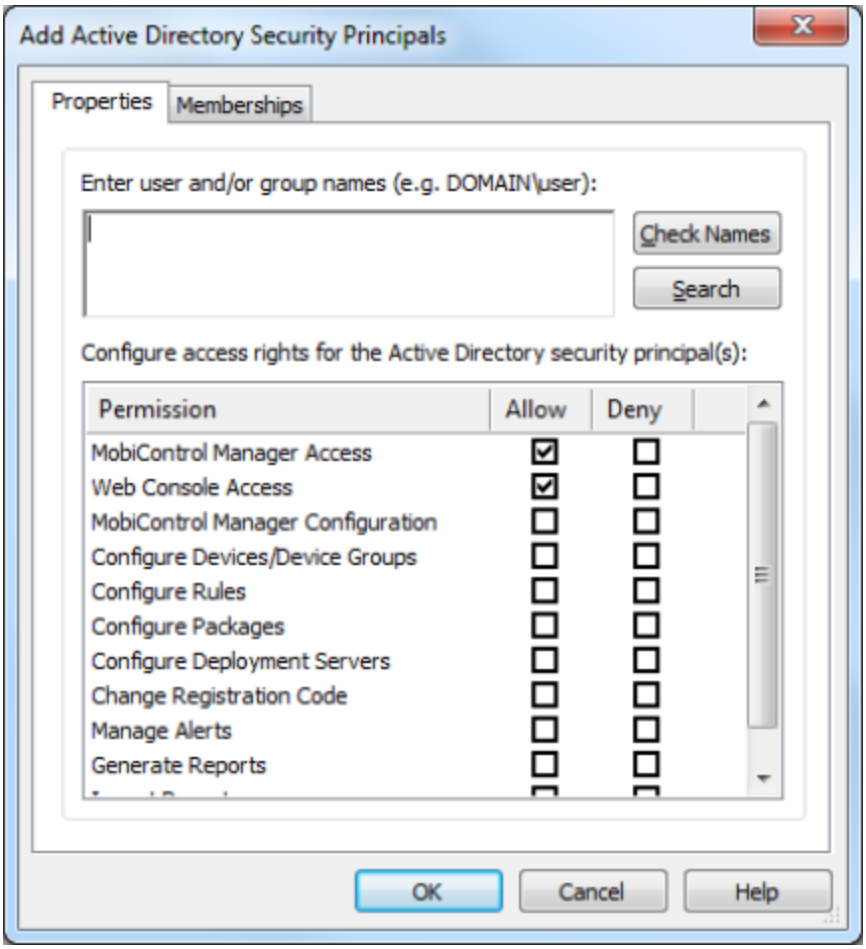
Selecting "Device Group Permissions" in MobiControl Manager

From the **Device Group Permissions** dialog box, you can customize user access and permissions. For instance, if you would like a user to be able to do everything, then you would select **Full Control.** Alternatively, if you would like the user only to be able to remote control the device, then select only that option. These security settings are applied to the devices groups in MobiControl Manager and define what users can do at the device level.

The permissions in the group permissions page can be set at the group level, as well as the individual user level. The permissions will take the most restrictive settings.

NOTE:

If the user or group belongs to the local domain, then the domain is not needed (i.e. you can type in just "`TestUser`"). However, if the user or group is from a different domain, then you do need to include the domain (i.e. `Domain\TestUser2`).



Device Group Permissions dialog box

IMPORTANT:

If **Allow** is **NOT** selected, then the permission is not present and therefore not assigned to the user/group (as there is no deny option). However, if the permission is granted based on group membership, then the appropriate permissions are applied to all users within that group. Once the permission has been given on the group level, the permissions **CAN NO LONGER BE DENIED**.

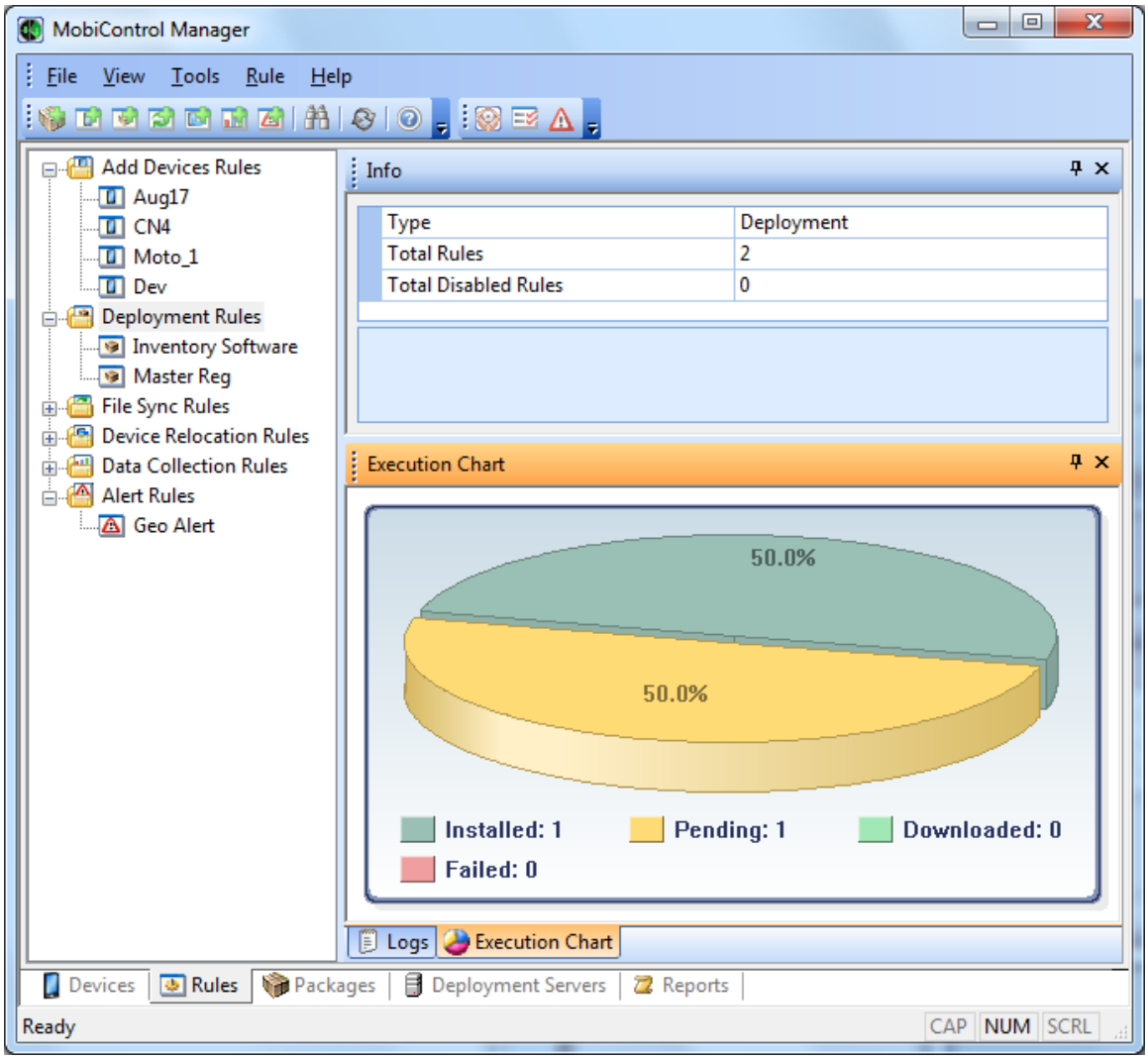
Take caution in assigning permissions to groups.

Access Right	Description
Full Control	Allows all features listed below
View Device Groups	View the device groups
Modify Device Groups	Modify the device groups
Configure Group Permissions	Configure device group permissions
Configure Devices	Modify device advanced settings such as connection mode, retry delay and log settings
Configure Device Security	Modify device security configurations such as lockdown and out-of-contact actions.
Send Messages to Devices	Send a text message to a set of devices
Send Scripts to Devices	Send a script to a set of devices
Move Devices	Move devices between device groups
Remote Control Devices	Start a remote control session
View Device Files	View device files through remote control
Update Device Files	Update the device files through remote control
View Device Registry	View the device registry through remote control
Update Device Registry	Update the device registry through remote control
View Device Task Info	View the Task Manager and Service Manager tool through remote control
Manage Device Tasks	Execute/kill device processes through remote control
View Device System Info	View device system information through remote control
Open DOS Command Window	Open the DOS Command Box and execute MobiControl commands through remote control
Remote Control Scripting	Execute script files on the device through remote control
Send Keyboard/Mouse Input	Send keyboard/mouse input to the device through remote control
Remote Control Device Without Notification	Start a remote control session without requiring the device user to accept the session
Manage Device Notes	Add, edit and delete device notes

Access Right	Description
Location Services	View the device's GPS location
Device Agent Upgrade	Enable, disable, or force agent upgrade for device(s) in the group
Network Agent Upgrade	Enable, disable, or force agent upgrade for the entire network

Rules View

MobiControl uses rules to simplify the tasks of device management and configuration. There are five rule types: add devices rules, deployment rules, file sync rules, device relocation rules, and data collection rules. Each is described below.



MobiControl Manager Rules view (tab)

Add Devices Rules

1. Create an add devices rule.

   An add devices rule allows you to configure the settings that MobiControl uses to set up and communicate with your devices. These settings include: the device group to which devices are added, how often the device is to check for updates, and the parameters to be used for remote control sessions. Please see the "Add Devices Rule" topic on page 261 for detailed information about creating an add devices rule.

2. Create a Device Agent.

   The Device Agent is the MobiControl software that resides on mobile devices and communicates with MobiControl Deployment Servers. Device Agents execute instructions received from MobiControl Deployment Servers, report status information, and send real-time information to Deployment Servers. Device Agents also restore the device state after a hard reset, service remote control sessions, install or uninstall packages, and synchronize the device clock. Please see the "Device Agent Manager" topic on page 277 for detailed information about creating a Device Agent.

3. Install the Device Agent onto the devices.

   Once created, there are several options for installing the agent on to your devices. For example, installation can be accomplished via cradled ActiveSync, via a website download, via an SD card, or using an existing software distribution mechanism. Please see the "Device Agent Manager" topic on page 277 for detailed information about installing the Device Agent.

Deployment Rules

1. Create a package.

   A package is a set of software and data files that have been packed into a single compressed file. MobiControl provides a tool called MobiControl Package Studio that allows you to quickly and easily create packages. For complex packages, Package Studio allows users to add scripts that get automatically executed at various points in the installation or un-installation of the package. Please see the "Creating Packages" topic on page 414 for detailed information about creating packages using MobiControl.

2. Create a deployment rule.

   To deploy a package using MobiControl, you need to create a deployment rule. When you create a deployment rule, you need to specify the package(s) to be deployed, the devices to which the package(s) will be deployed, and the installation time. Please see the "Deployment Rule" topic on page 327 for detailed information about creating a deployment rule.

3. Check the rule execution status.

   Once you have created a deployment rule, you may want to confirm that all devices have been provisioned with the specified packages. The execution status of the deployment rule is graphically represented in the execution chart in the Rules view (tab). MobiControl also provides a report called the 'Deployment Rule Execution Summary Report'. Please see the "Generate Reports" topic on page 390 for detailed information about MobiControl Reports.

File Sync Rules

1. Create a file sync rule.

   A file sync rule allows you to schedule file(s) to be synchronized between a set of devices and the Deployment Server. When creating a file sync rule, you will need to specify the file(s) you want synced (both their original location and their destination), the interval in between the syncs and which direction the sync should go in (either device to server, or server to device) and which devices should be involved in the sync. Please see the "File Sync Rule" topic on page 344 for detailed information about creating a file sync rule.

2. Check the rule execution status.

   Once the file sync rule has been created, you may want to confirm that the scheduled syncs occurred. You can do this by looking at the rule execution status or by checking the rule execution report in the Reports view (tab). Please see the "Generate Reports" topic on page 390 for more detail about reports.

Device Relocation Rules

1. Create a device relocation rule.

   A device relocation rule allows you to automatically move your mobile devices among different device groups in the MobiControl device tree, based on the IP address or other custom criteria. This is useful for managing mobile devices in a deployment where the device tree represents different physical locations (e.g. retail stores, warehouses, regional offices, etc). Please see the "Device Relocation Rule" topic on page 335 for detailed information about creating a device relocation rule.

2. Check the device relocation rule execution status.

   Once the device relocation rule has been created, you may want to confirm its execution. You can do this by looking at the rule execution status or by checking the rule execution report in the Reports view (tab). Please see the "Generate Reports" topic on page 390 for more detail about reports.

Data Collection Rules

1. Create a data collection rule.

   A data collection rule allows you to set up rules to collect data from your mobile devices automatically. Please see the "Creating Data Collection Rules" topic on page 318 for detailed information about creating a data collection rule.

2. Check the data collection rule execution status.

   Once the data collection rule has been created, you may want to confirm its execution. You can do this by looking at the rule execution status or by checking the rule execution report in the Reports view (tab). Please see the "Generate Reports" topic on page 390 for more detail about reports.

Alert Rules

1. ## Create an Alert Rule

   An Alert Rule allows Administrators and Users to be notified when events of interest arise on the system. Please see the "Alert Rule" topic on page 296 for detailed information about creating an Alert Rule.

2. ## Check the Alert Rule execution status.

   Once the Alert Rule has been created, you may want to run a report to see what alerts have been generated. You can do this by looking at the Alert Rule Summary report in the Reports view (tab). Please see the "Generate Reports" topic on page 390 for more detail about reports.

Creating Add Devices Rules

Add devices rules allow MobiControl to name devices, place devices in the appropriate device group, and to generate a customized MobiControl Device Agent that, when installed onto devices, allows them to be managed by MobiControl.

When you generate a Device Agent for an add devices rule, MobiControl places an identifier for the rule (i.e. rule tag) into the `.cab` file for the generated agent. When the Device Agent is installed onto a device, it will connect to a MobiControl Deployment Server and supply the rule tag to the server. The server will then look up the add devices rule and configure the device accordingly.

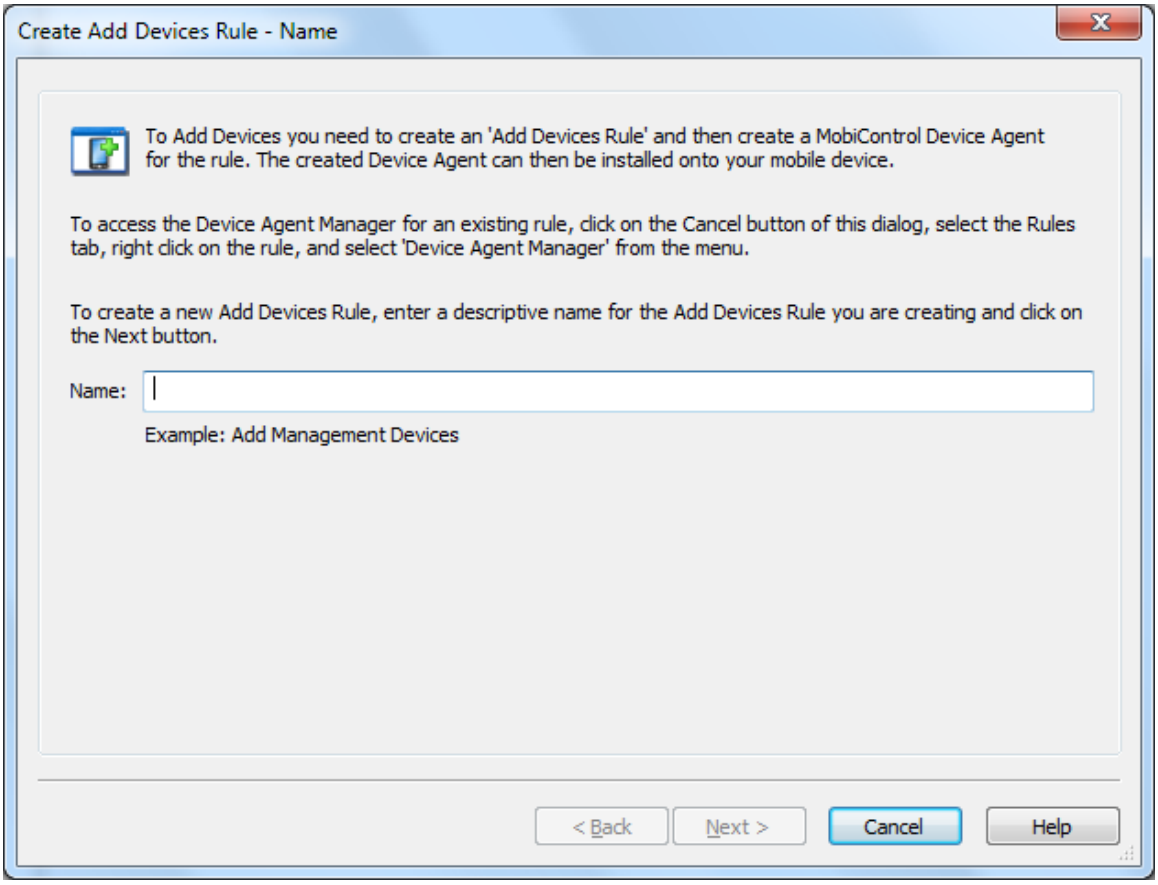
To create an add devices rule, select the Rules view (tab) within MobiControl Manager, then click the **Rule** menu, select **Create Rule**, and click **Add Devices Rule**. The Create Add Devices Rule Wizard will be displayed.

The six steps below describe how the Create Add Devices Rule Wizard can be used to create an add devices rule:

1. Start the wizard.

   Select the Rules view (tab), then click the **Rule** menu, select **Create Rule**, and click **Add Devices Rule**. The first page of the Create Add Devices Rule Wizard will be displayed.

   Enter a descriptive name for the add devices rule you are creating and click **Next.**



First page of the Create Add Devices Rule Wizard

2. Configure the device group.

Device Group Selection page

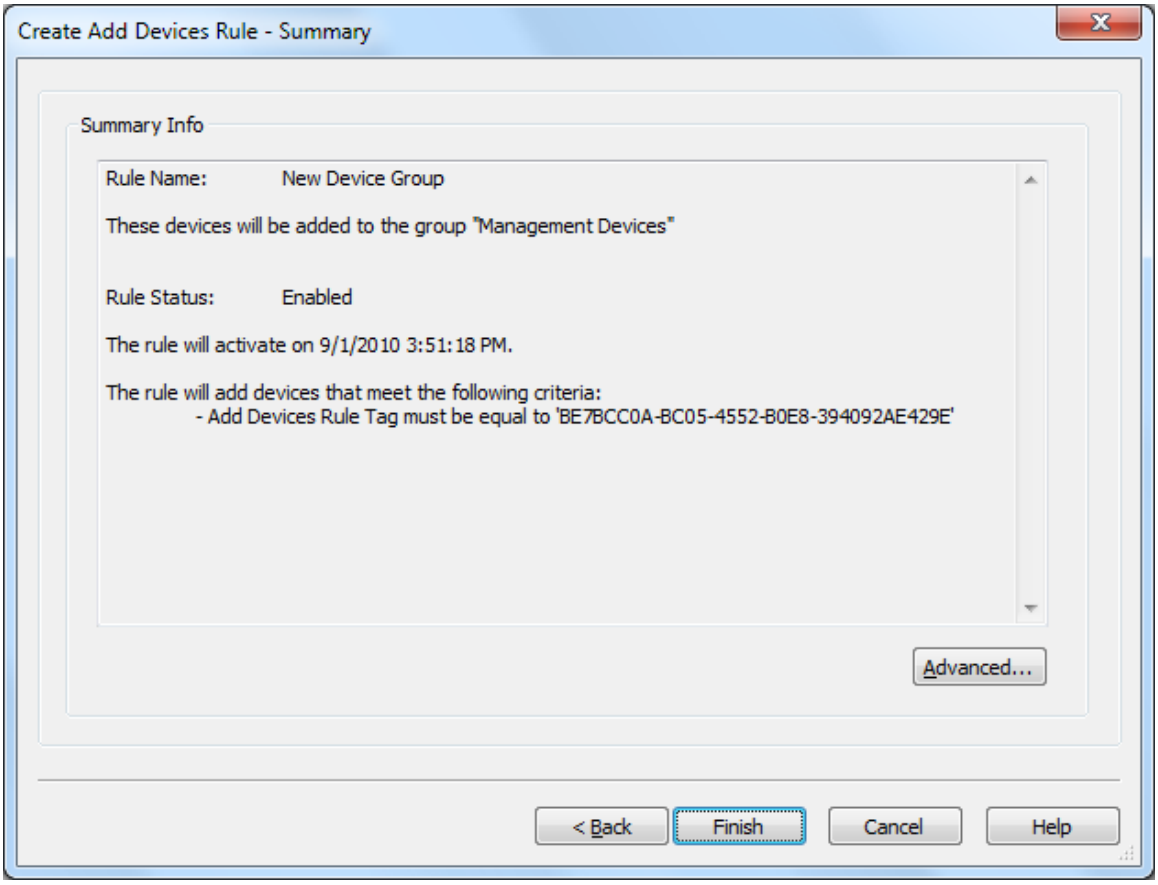
First, select to which device group the devices configured by this rule will be added. The dialog box below displays the current device tree. Select the group where devices need to be inserted and then click **Next.** If you need to add a new group or change the structure of the device tree, exit the wizard, go to the Devices view (tab), edit the tree, and then begin the wizard again.

After selecting a device group click on the **Next** button.

3. Review summarized information.

The **Rule Summary Information** page summarizes the settings configured on the previous pages of the wizard.

If you are satisfied with the configured settings, click on the **Finish** button to create the device rule, otherwise use the **Back** button to go to previous screens and make adjustments.

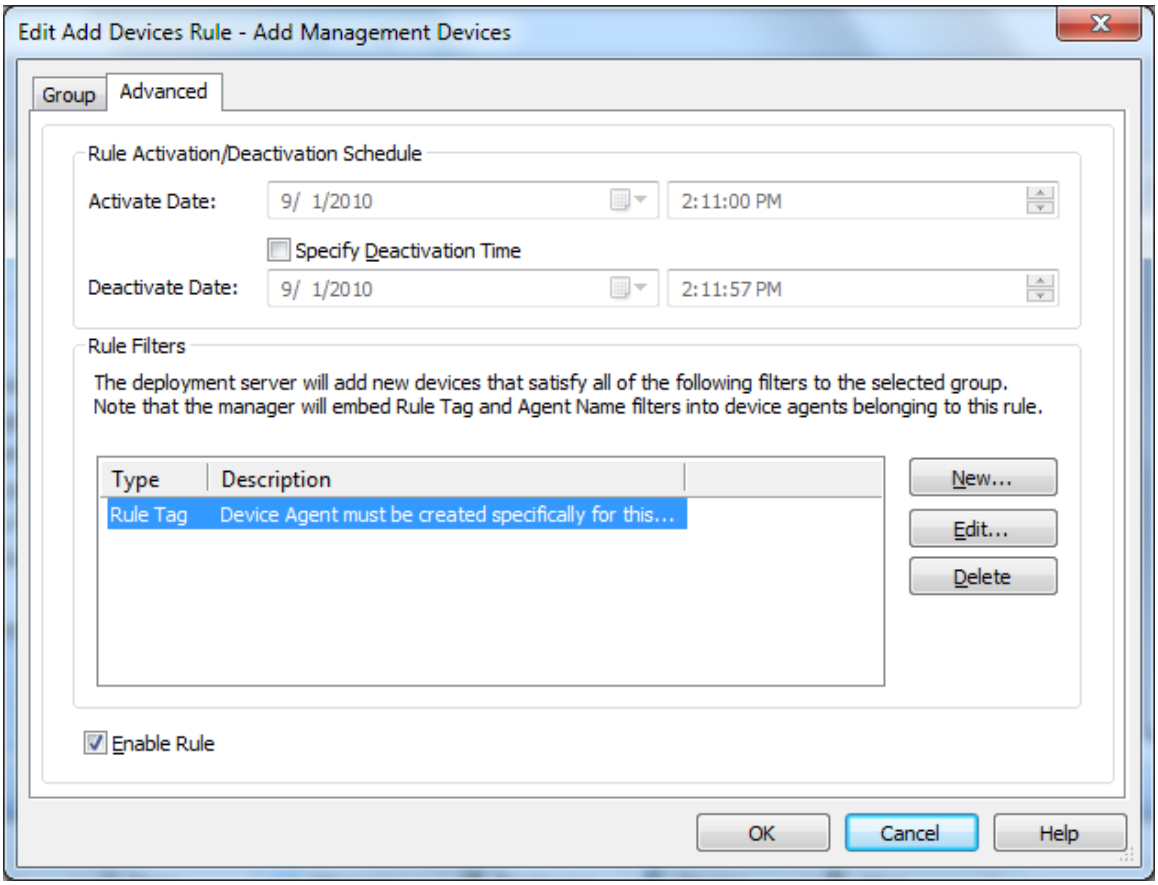


Rule Summary Page

4. Advanced Settings.

The **Advanced Settings** button allows you to specify which devices are to be configured by this rule. By default, MobiControl will use this rule to configure only those devices that are running a Device Agent created specifically for this device rule. By using advanced settings filters, you can broaden or further restrict which devices get configured by this rule when they connect to MobiControl. Please see the "Rule Filters" topic on page 294 for detailed information about Advanced Settings.

Once you have made the changes, click **Next.**

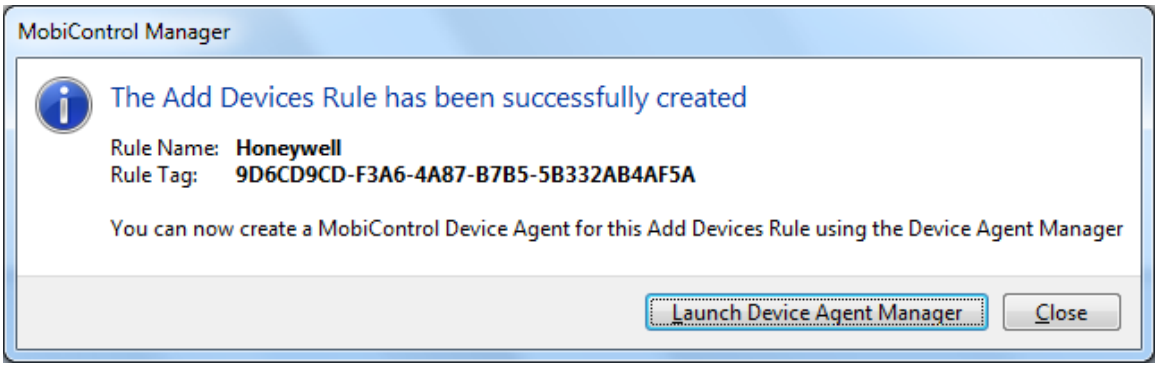


Advanced Settings Page

5. Receive confirmation that the rule has been created.

   A notification of rule creation will be displayed once the device rule has been created. The message box confirms that the rule has been successfully created and allows you to immediately generate a MobiControl Device Agent for the rule.

   If you click the **Yes** button on the message box, the wizard to create a Device Agent will be launched. If you click on the **No** button, you can generate a Device Agent later.



Rule Creation Notification message box

Once you have created an add devices rule, the next step is to generate a MobiControl Device Agent. You can generate a Device Agent for an add devices rule immediately after creating the rule or at any time after creating the rule using the Device Agent Manager. The generated agent is customized for the specific add devices rule that you select. Please see the "Device Agent Manager" topic on page 277 for instructions on how to create a Device Agent using the Device Agent Manager.

NOTE:

You can access the Device Agent Manager from the Rules view (tab) in MobiControl Manager. Right-click on a specific add devices rule in the left pane, and then select **Device Agent Manager** from the pop-up menu.

Generating a Barcode

Barcode Generator is a method that can be used to provision the MobiControl Device Agent on devices by scanning barcodes.

The generated barcode will encode all the necessary information to allow the device to connect to the MobiControl Deployment Server.

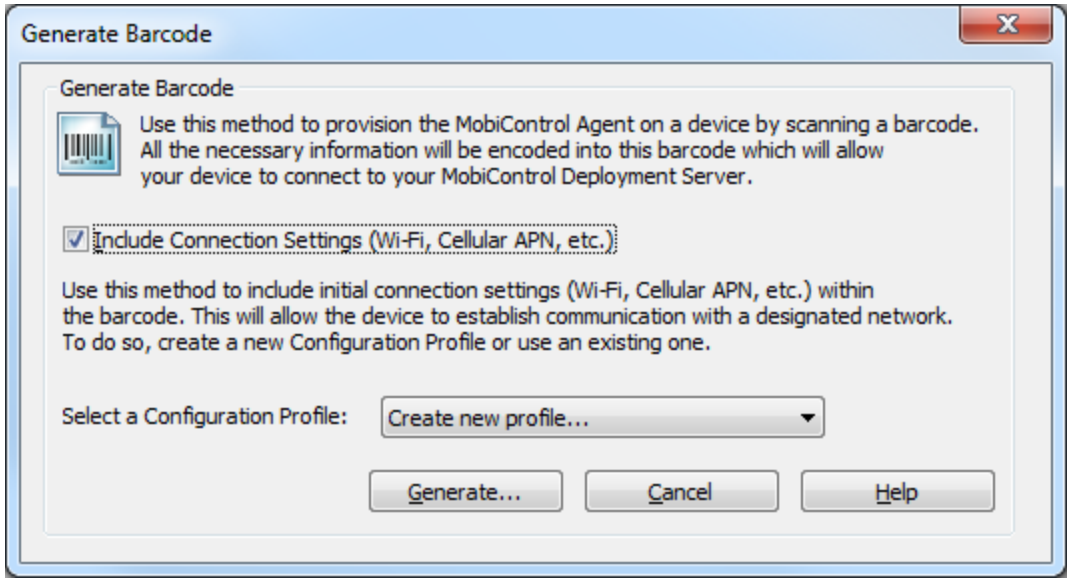
IMPORTANT

MobiScan requires .NET 3.5 to be installed to work properly. Click here to download .NET 3.5.

The following series of steps describes how to Generate a Barcode:

1. Start the wizard

In **Device Agent Manager**, select the appropriate Device Agent, then click **Provision Device,** click **Generate Barcode:**



Option	Description
Include Connection Settings	This option enables you to include the initial connection settings (Wi-Fi, Cellular APN, etc..) within the barcode. The device can use these Settings to establish a connection with the designated network. Please review Configuration Profile Manager section for further details regarding these settings.

2. Select a Configuration Profile.

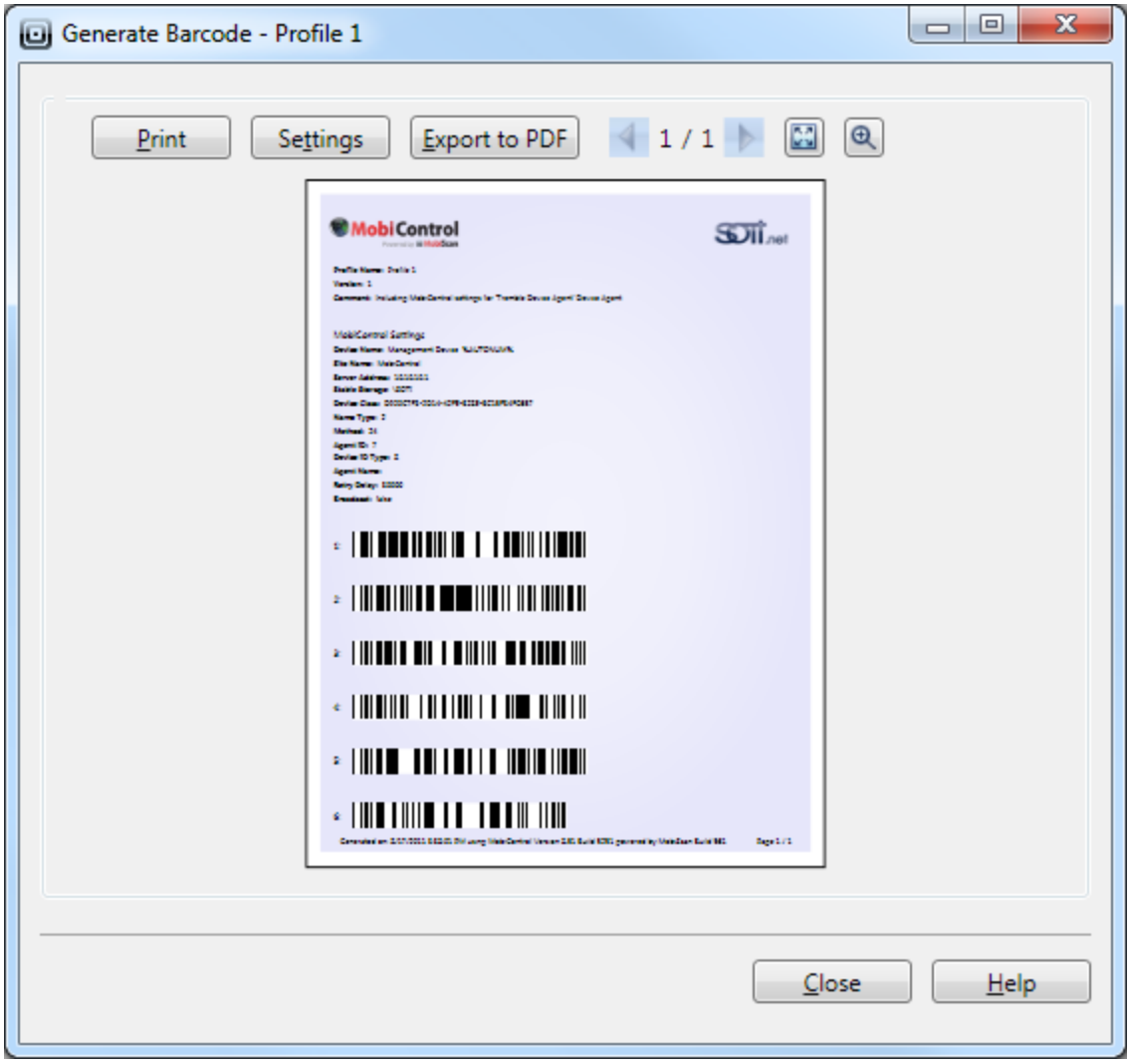
You can select a Profile available from the list or create a new Profile using Configuration Profile Manager.

3. Generate Barcode

Click on **Generate**

If a Configuration Profile is selected from the list, it will generate the Barcode with encoded settings according to that Profile.

If "Create new profile" is selected from the list, it will open the Configuration Profile Manager wizard to create a new Profile. The barcode will be generated at the end of this wizard.



NOTE:

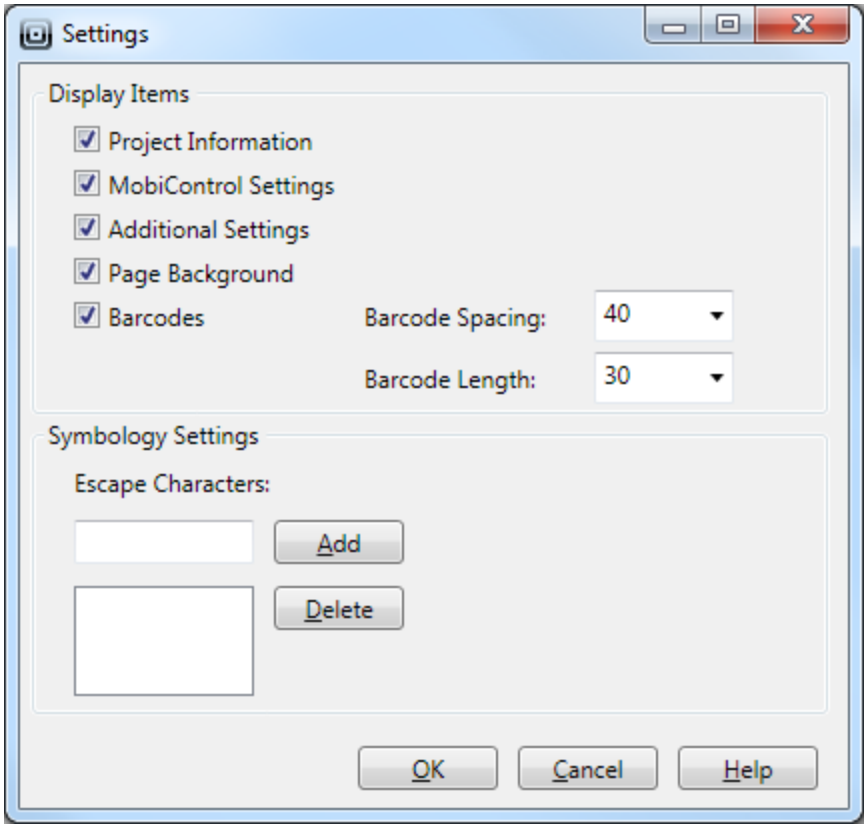
If you have not checked the Include Connection Settings option, the Barcode will be generated only with the MobiControl Device settings information.

Click on "**Print**" to print the current Barcode.

Click on "**Export to PDF**" to export Barcode to a PDF file, which can be forwarded or printed at a later date.

Click on "**Settings**" to modify the Barcode settings.

4. Barcode Settings



Field Name	Description
Project Information	Check this option to display the Project information (name, version, comment, etc..) in the page.
MobiControl Settings	Check this option to display the MobiControl Device Agent settings information in the page.
Additional Settings	Check this option to display the configured Settings included via Configuration Profile in the page.
Page Background	Check this option to display a background with the page.
Barcodes	Check this option to display the generated barcodes in the page. **Barcode Spacing:** Can be adjusted according to preference. **Barcode Length:** Can be adjusted according to preference.
Escape Characters	You can add **Escape Characters**, if required in your barcode.

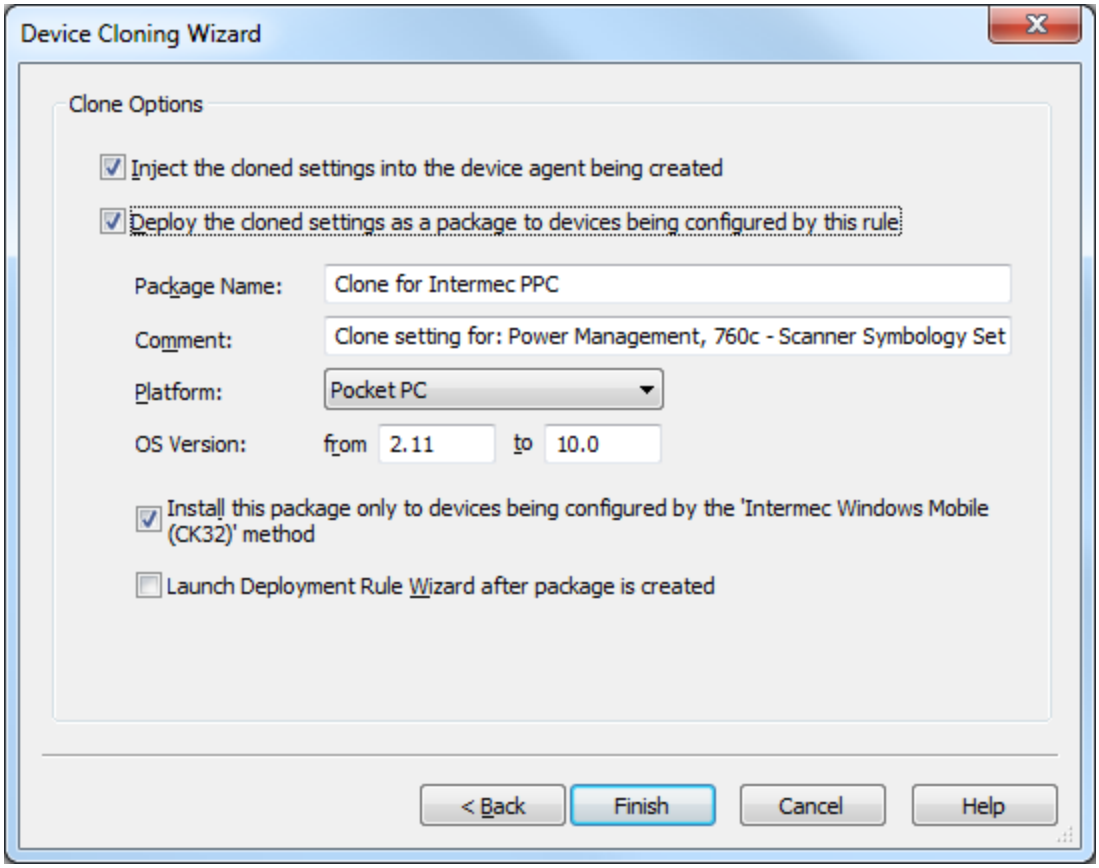
Device Agent Clone Settings

As part of the process of creating a Device Agent, you can also clone the settings of a "master" device, include those settings in the agent you create, and generate a distributable package that contains the settings.

In the Device Agent Wizard, click the **Clone Settings** button on the **Device Platform Configuration** page.

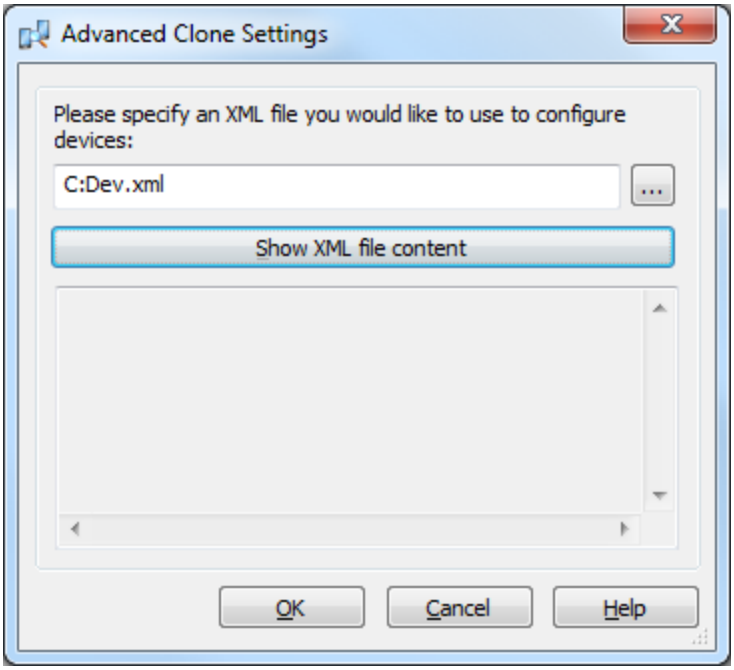
1. Select the settings to be cloned.

   Select the desired items from the list. The settings that can be cloned depend on the profile that has been set up for a type of device. If there are settings for your mobile device that you would like to clone but are not listed as being clonable, please contact us.



Device Clone Options

Click the **Advanced** button to open the **Advanced Clone Settings** dialog box.



XML Device Cloning

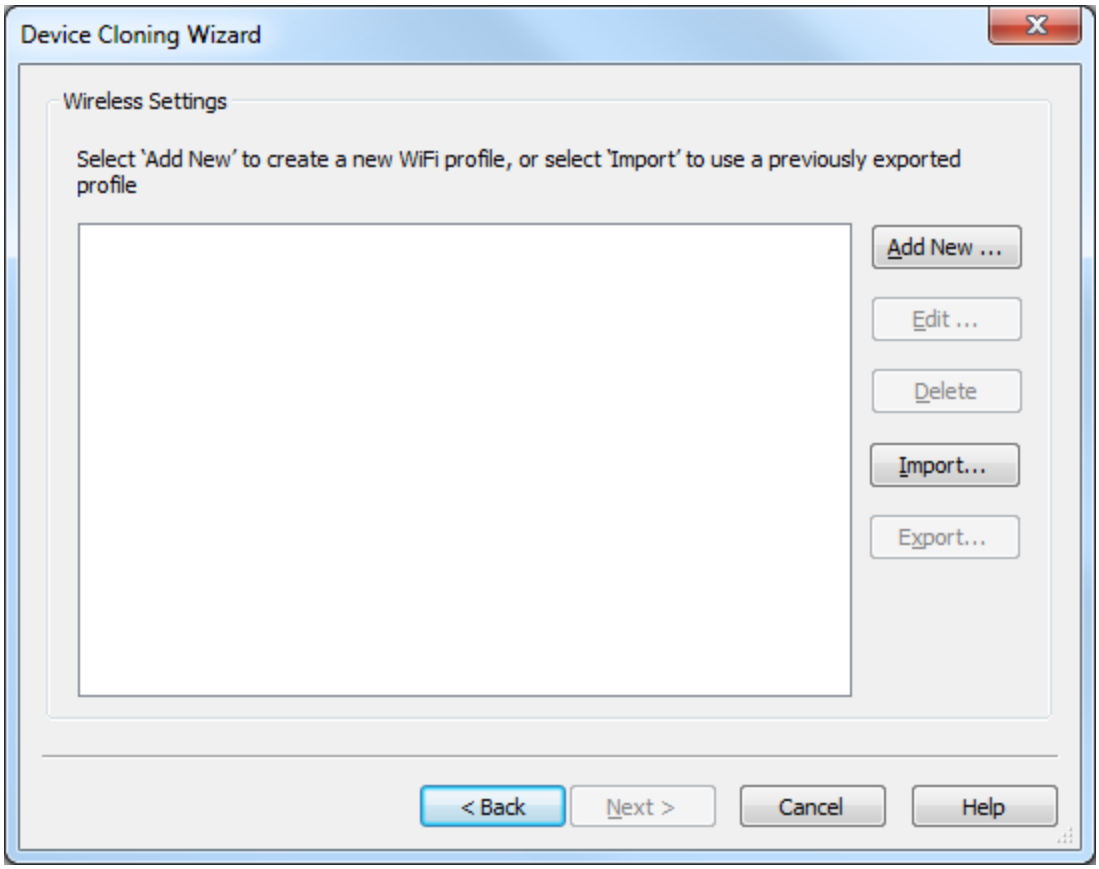
XML device cloning can be used to load advanced configuration options to the device via an `.xml` file. The provided `.xml` file is not parsed by MobiControl, but is passed over to the operating system. Beginning in Pocket PC 2003, there is a configuration management system which allows for easy configuration through a standardized `.xml` file. Almost every aspect of the device can be configured by this method, from encryption certificates to Wi-Fi settings. Please see the "Advanced XML Setup Script" topic on page 370 for a sample script.

NOTES:

- Please see the "Intermec SmartSystems Settings" topic on page 368 for more information on cloning Intermec SmartSystems settings.
- Hand Held Products Power Tools must be installed in order to facilitate cloning of EZConfig settings.

2. Select, create, export or import a Wi-Fi profile.

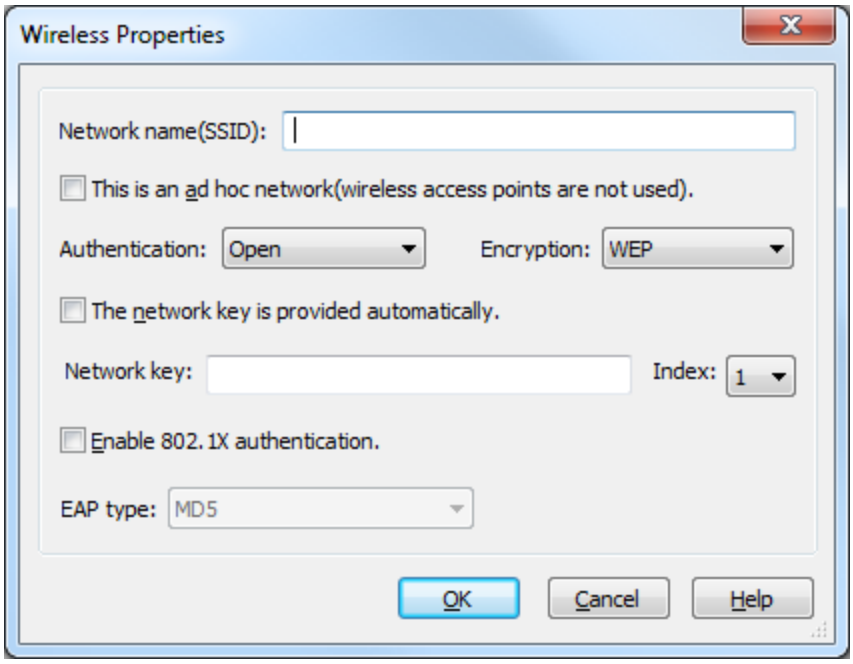
This step is only visible if the **Wireless Network 802.11** option is selected. The cloning of Wi-Fi settings is only available on select devices that support the standard Microsoft Wireless Configuration API. Once a Wi-Fi profile has been created, it can be cloned to multiple devices. In addition to creating a profile, you can also export or import a previously-exported profile.



Wireless Settings page

The following values must be known to set up a Wi-Fi profile:

- Your wireless network name, the SSID (Service Set Identifier), which identifies your network
- The encryption type: WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access)
- A network key for secure networks

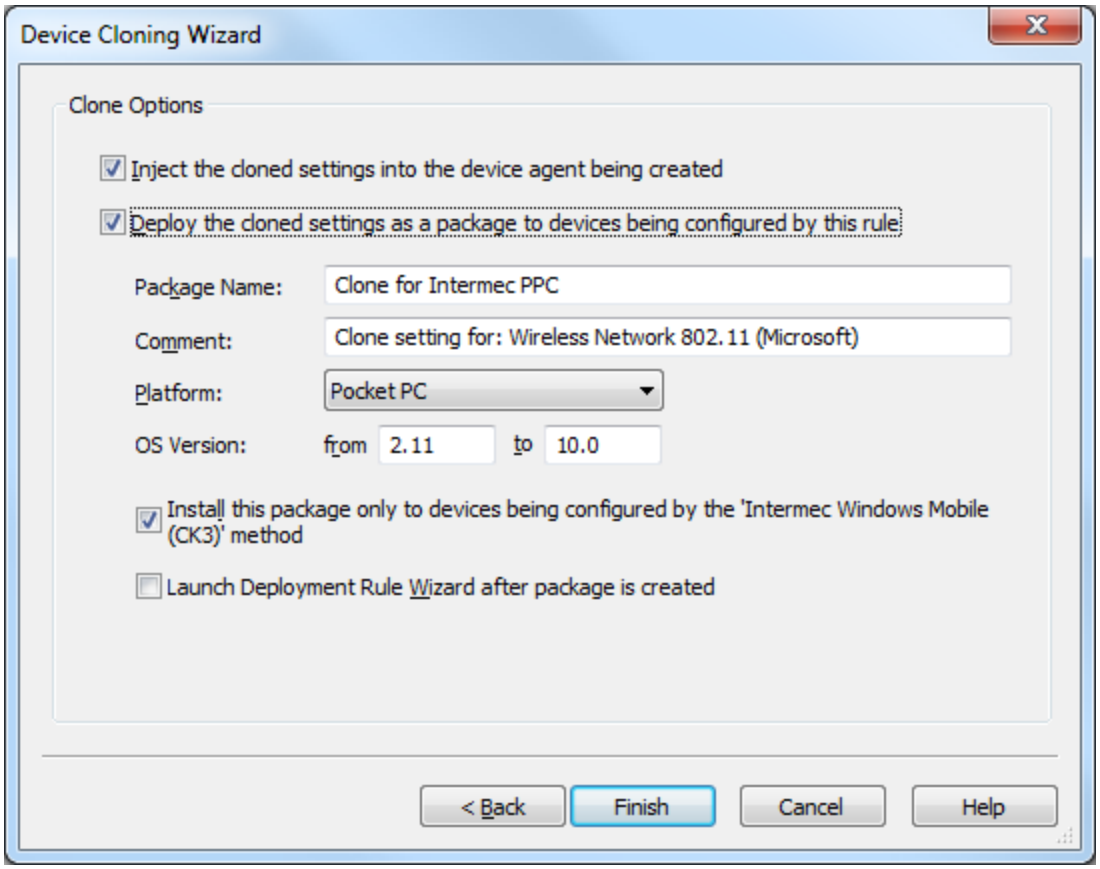


Wireless Properties dialog box

3. Specify the delivery mechanism.

There are two available ways to deliver the cloned settings to your devices. The first is to inject them into the Device Agent that you are creating. The second is to place the settings in a package, and then deploy the package. Injecting the settings into the agent allows you to establish the cloned settings on the device as part of the MobiControl Device Agent installation process. The package creation option allows you to easily distribute new settings to devices that are already deployed and are running MobiControl.

If you select the second option, provide a name for the package, and a comment that describes what it contains. In addition, you can specify the platform and OS version constraints.



Device Clone Options

Click the **Finish** button when you have completed the settings in this dialog box and you will be returned to the Device Agent Wizard.

If you choose the option to create a package, the new package will be added to the MobiControl database, and will be listed on the Packages view (tab) of the Manager after clicking **Finish**. If you selected the **Launch Create Deployment Rule Wizard after package is created** check box, then you will be immediately guided to the wizard for deploying the new package to your devices. If you did not select this check box, you can switch to the Rules view (tab) and select **Create Deployment Rule** from the **Rules** menu.

Device Agents

The MobiControl Device Agent is the MobiControl software that is installed onto mobile devices. The Device Agent communicates with MobiControl Deployment Server(s) and carries out the instructions it receives from the servers. Device Agents also provide reporting and real-time information to Deployment Servers.

Device Agent Installation

The MobiControl Device Agent is typically distributed in the form of a `.cab` file to mobile devices. Before the Device Agent is installed onto a mobile device, it must be created and customized using the Device Agent Manager. You can access the Device Agent Manager from the Rules view (tab) in the MobiControl Manager, right-clicking on a rule in the **Rules** menu and selecting **Device Agent Manager**. Please see the "Add Devices Rule" topic on page 261 for more information.

The Device Agent Manager allows users to create a customized `.cab` file for a particular installation. Parameters required for the agent to connect to and be managed by MobiControl Deployment Servers are inserted. Once an agent `.cab` file is installed onto a device, the agent automatically connects to a Deployment Server, configures the device, and provides the device with the appropriate packages.

By creating custom MobiControl Device Agents in this way, much of the manual data input and configuration typically required for configuring mobile devices is eliminated. To facilitate easy installation of the Device Agent software on a small number of devices, the Device Agent creation tool can automatically install the agent on devices through an ActiveSync connection. By docking each device into the cradle and clicking **Install**, MobiControl Device Agents can be quickly installed onto devices. Alternatively, the **Copy** button can be used to export the agent installation files and deliver them to the device via some other means, for instance as an email attachment or posted on a website. When there are many devices to be configured, it might be convenient to have the device provider pre-install the agent onto the devices before delivery.

Device Agent Configuration Applet

MobiControl includes a configuration applet on the device from which the MobiControl Device Agent settings can be viewed and modified. Please see the "Mobile Device Configuration Applet" topic on page 394 for more information.

The Device Agent configuration applet can be accessed from the desktop of the device by clicking on the **MobiControl** system tray icon.

NOTE:

On a Smartphone device, the MobiControl Device Agent configuration applet is accessed via the Start menu.

Device Agent Manager

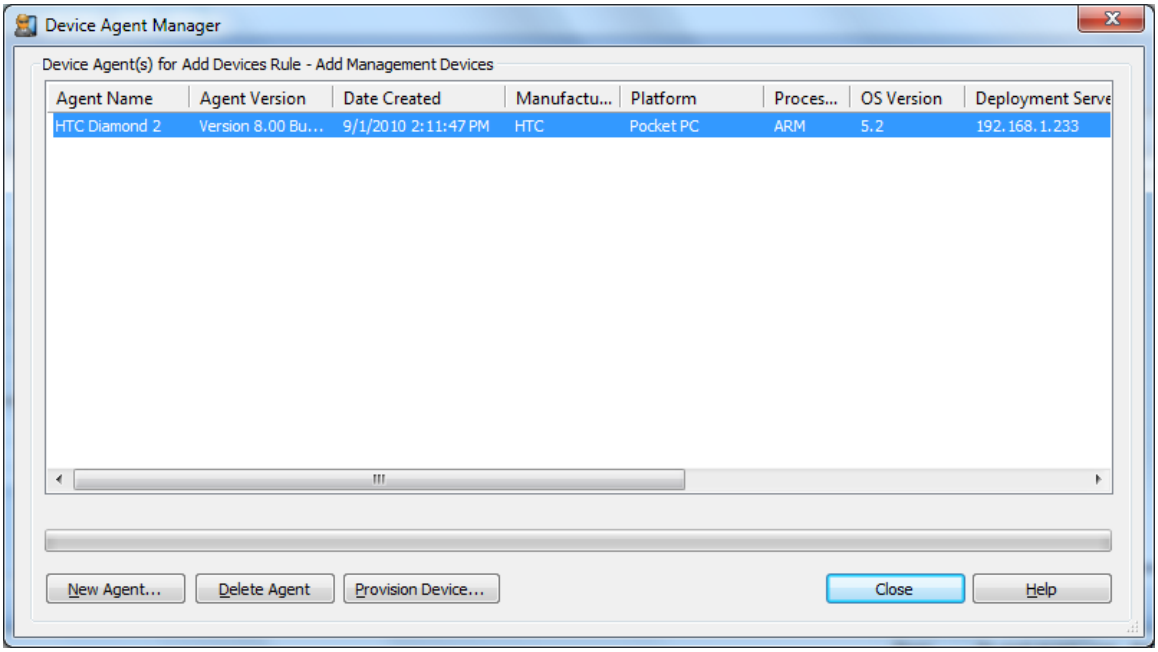
The Device Agent Manager is an interface that allows the user to manage the Device Agents that are installed to the devices. A Device Agent is a program that is installed on to the various devices that are to be managed by MobiControl. The software facilitates the server-client communications. The Device Agent Manager allows creation of custom Device Agents that have been specially configured to the settings of your MobiControl installation and the type of devices you have.

You can access the Device Agent Manager from the Rules view (tab) in MobiControl Manager by right-clicking on a specific add devices rule in the left pane, and then selecting **Device Agent Manager** from the pop-up menu.

Once you have created an add devices rule, the next step is to create a MobiControl Device Agent. You can create a Device Agent for an add devices rule immediately after creating the rule or at any time after creating the rule using the Device Agent Manager. The created agent is customized for the specific add devices rule that you select.

The following steps outline how to create a Device Agent using the Device Agent Manager.

1. Create a Device Agent.



Device Agent Managerdialog box

The MobiControl Device Agent Manager allows you to create a Device Agent for a specific add devices rule. The Device Agent Manager also allows you to view and copy files for Device Agents previously created. After creating a device rule, you can access the Device Agent Manager by clicking on the **Yes** button on the message box displayed immediately after the rule is created, or by going to the Rules view (tab) in MobiControl Manager, and then right-clicking on a specific add devices rule in the left pane, and then selecting **Device Agent Manager** from the pop-up menu.

The Device Agent Manager displays a list of the Device Agents that have previously been created for the selected device rule, and allows users to create new Device Agents, provision Device Agents onto devices (by directly installing, exporting or generating barcodes) and to delete obsolete Device Agents. For newly-created add devices rules, the list will be empty until an agent is created.

If an agent has been already created, select the Device Agent and click on **Provision Device**

The following methods can be used to provision the Device Agent on the devices.

You can install the agent onto a device via desktop ActiveSync, by clicking on **Install Agent by ActiveSync** button if the device is connected to this computer

You can generate a barcode, by clicking on **Generate Barcode** to provision the Device Agent on a device by scanning a barcode

You can export the Device Agent files to a destination folder by clicking on the **Export Agent** button. This allows you to deliver the installation files to the target devices via a web site, email, SD cards, etc.

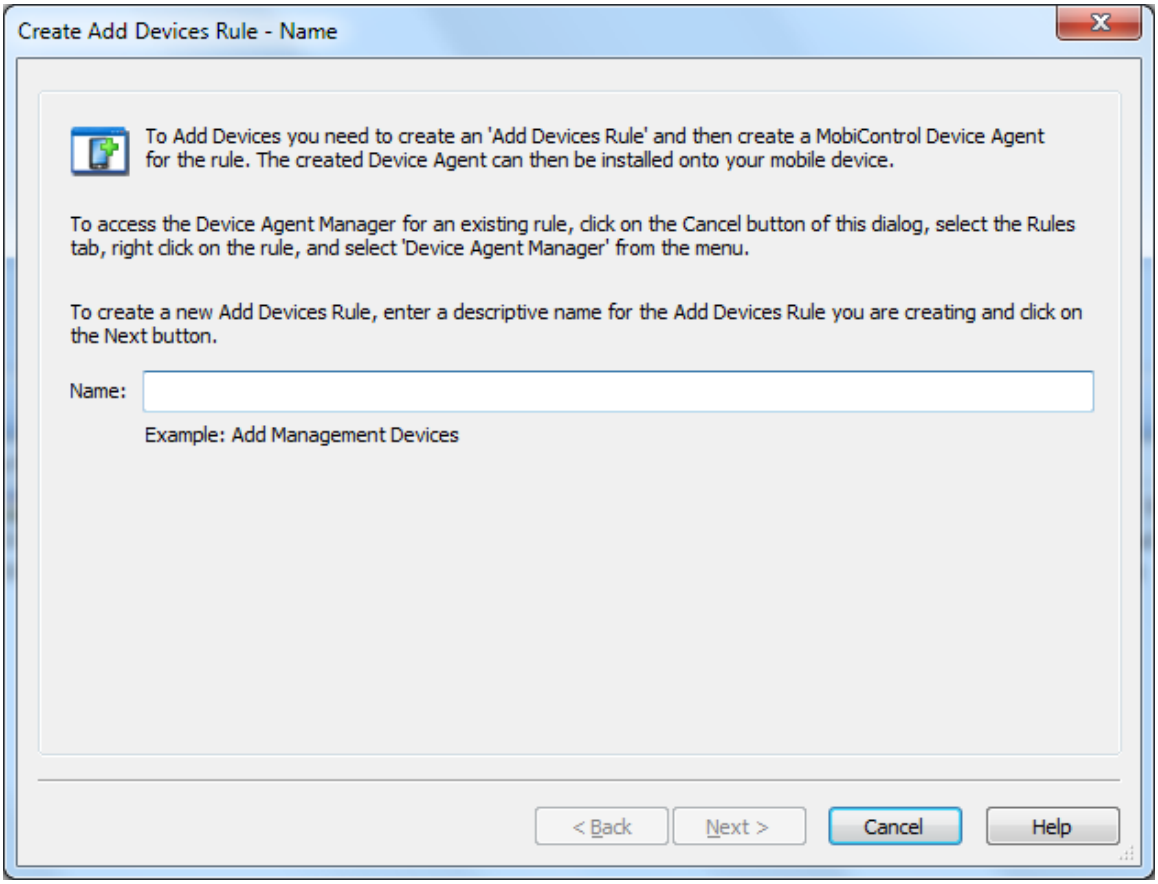
To delete an agent, select the agent from the list and click the **Delete Agent** button.

To create a new agent, click the **New Agent** button, the Device Agent Wizard will be displayed.

2. Name the Device Agent.

If your Device Agent was created prior to MobiControl version 6 then the Device Agent name will be blank.

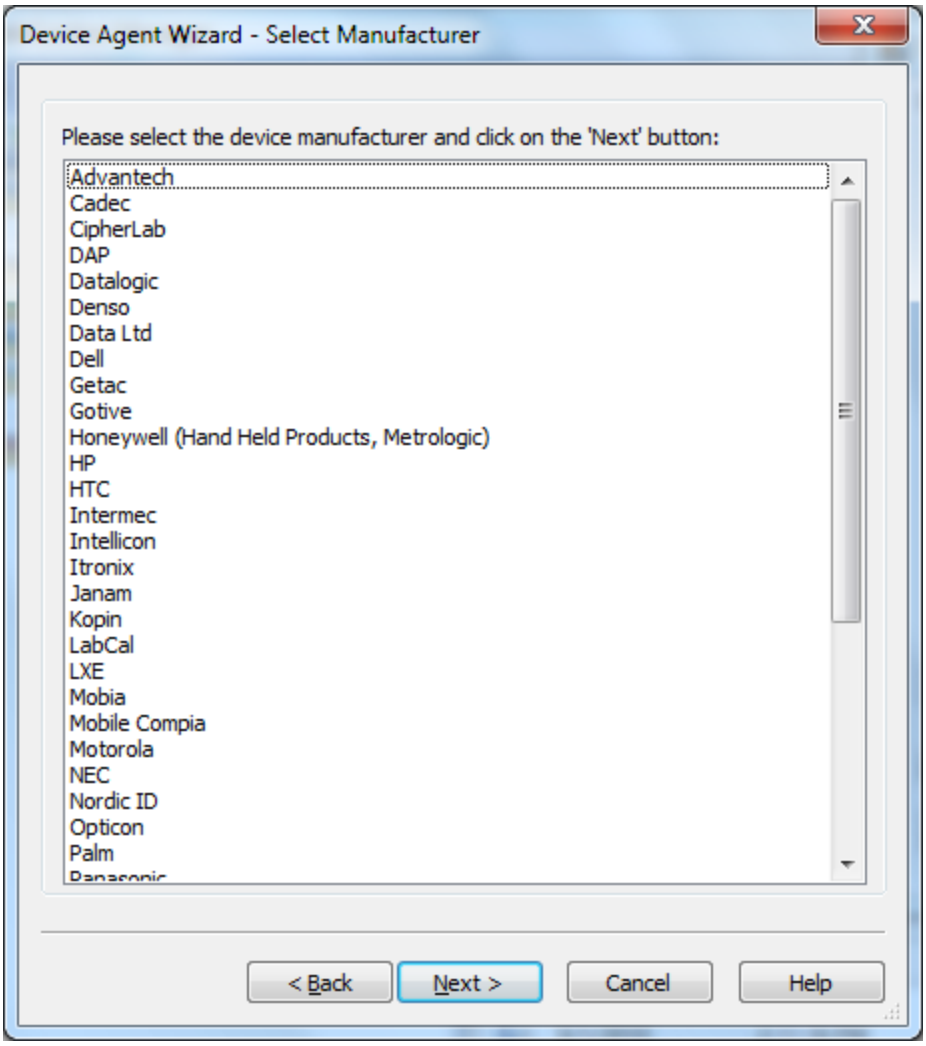
This will allow you to add a custom name to the Device Agent, which will help to identify it. Once you have entered a unique name, click **Next** to move to the next step. This page will only appear in version 5.06 and above.



3. Select the device manufacturer.

   On the second page of the Device Agent Wizard, select the manufacturer of your device and click the **Next** button. If the manufacturer of your device is not listed you can try selecting the **Other Manufacturers** option and click the **Next** button or you can contact us to make sure that your device is properly supported.

   After selecting the manufacturer, click the **Next** button.



Manufacturer Selection page

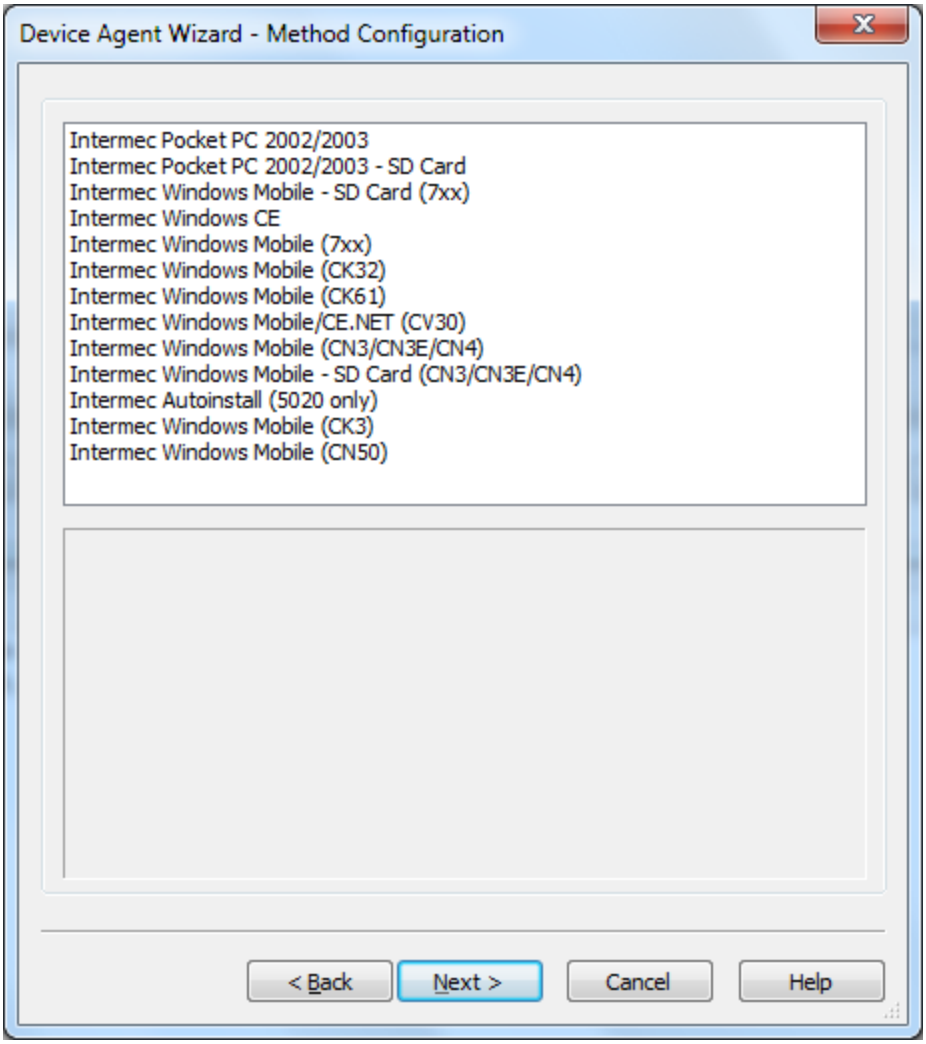
NOTE:

You can create a Device Agent for computer workstations, laptops, tablet PCs, etc. In order to create agents for these devices, select **Microsoft Windows 2000/XP/XP Embedded** for the device manufacturer. Please see the "Frequently Asked Questions" topic on page 1500 for more information.

4. Select a method.

   This page allows you to select a method that is appropriate for your device. For details about a specific method, select the method by clicking on it. The **Help** text box at the bottom of the page will display information about the method.

   Select the method that is suitable for your device and then click the **Next** button.



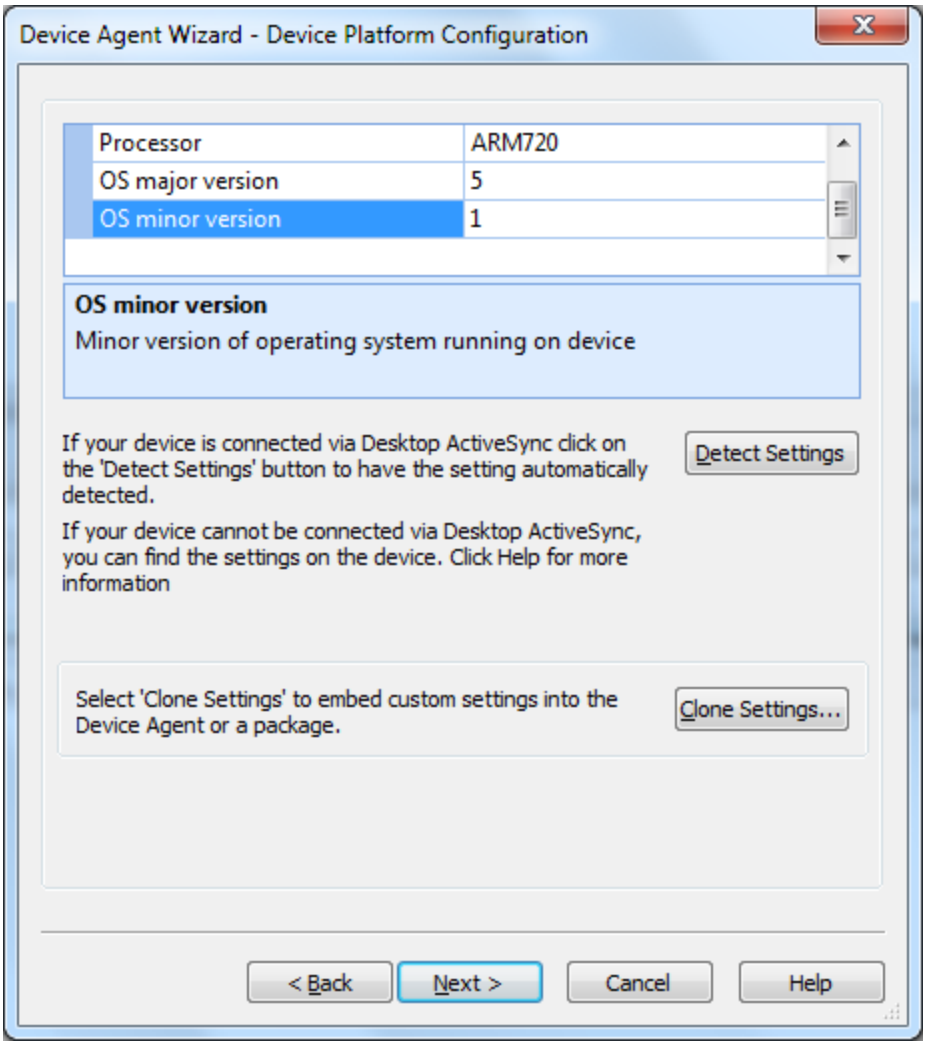
Method Selection page

5. Configure the device type.

The **Device Type** dialog box allows you to configure platform, processor and operating system information about your devices. If you dock one of your devices via ActiveSync, and click on the **Detect Settings** button, the wizard can automatically detect most of the device settings. If your device is not docked you can enter the settings manually.

Click **Clone Settings** to embed cloned settings into the agent you are creating or optionally create a package which can be deployed to a set of devices via the deployment rule engine. Please see the "Clone Settings Package Wizard" topic on page 361 and the "Device Agent Clone Settings" topic on page 270 for more information.

Click the **Next** button when you have completed the settings in this dialog box.



Device Type Configuration page

NOTE:

The OS version refers to the version of Windows CE or Windows Mobile. For example, if the version of the OS is 4.20, set the **OS Major Version** field to 4, and set the **OS Minor Version** field to 2. You can get information about the OS and the processor from the device. Typically, this information is available at the following locations for these mobile devices, however this may vary for some devices. If the device says Windows Mobile, and is a touch screen enabled device, select Pocket PC even though it says CE below on the CE OS Build. If the device is not a touch screen, select Smartphone.

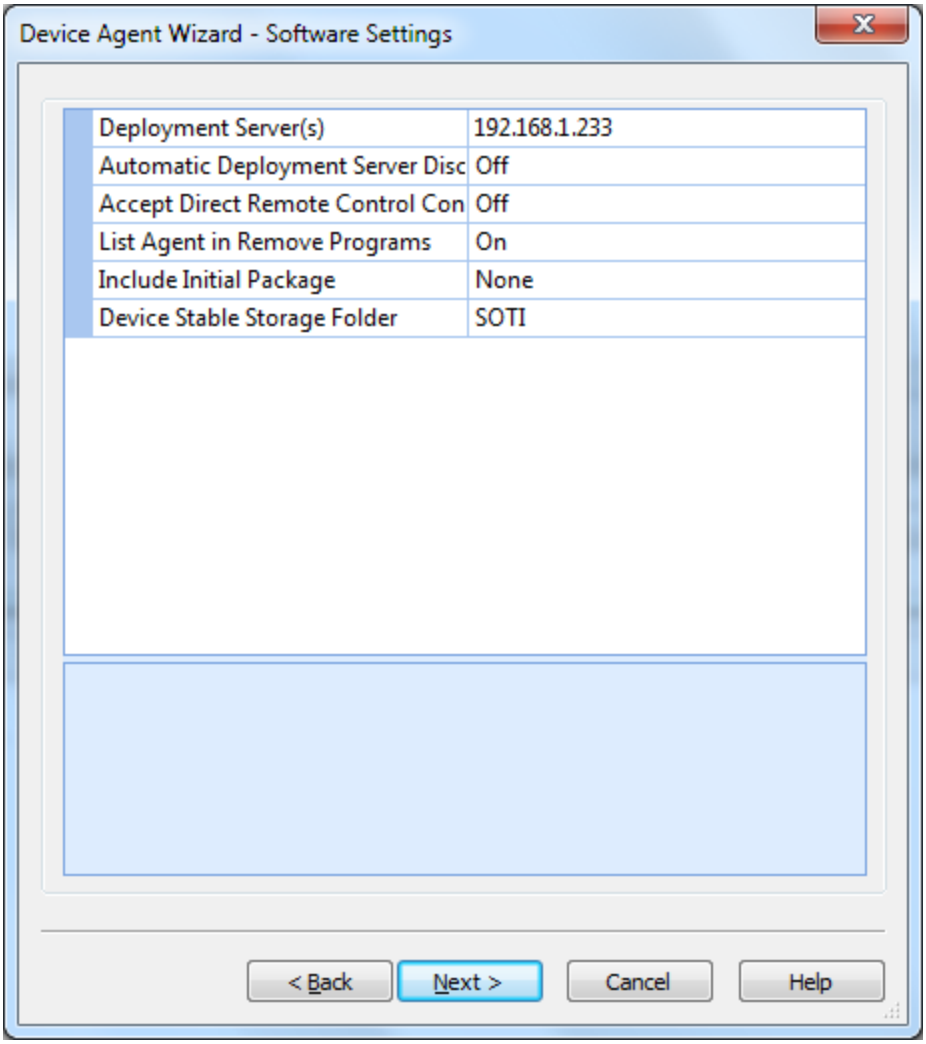
Device type	OS or Processor Information
Pocket PC	Select **Start**, then click **Settings**, click **System**, and click **About** to view the information.
Smartphone	Select **Start**, then click **Settings**, and click **About** to view the information.
Windows CE	Select **Start**, then click **Settings**, click **Control panel**, and click **System** to view the information.

TIP:

Intermec and SmartSystems Settings: We have added the functionality to clone SmartSystems Settings in Intermec devices. Please see the "Intermec SmartSystems Settings" topic on page 368 for more information about this feature.

6. Configure software settings.

The **Software Settings** page allows you to configure various parameters built into the agent. Click the **Next** button when you have completed the settings in this dialog box.



Device Agent Wizard - Software Settings page

Field Name	Description
Deployment Server(s)	Devices that have the MobiControl Device Agent software installed onto them connect to MobiControl Deployment Servers to receive configuration information as well as to get provisioned with software and data. It is crucial that the device is able to reach the IP address

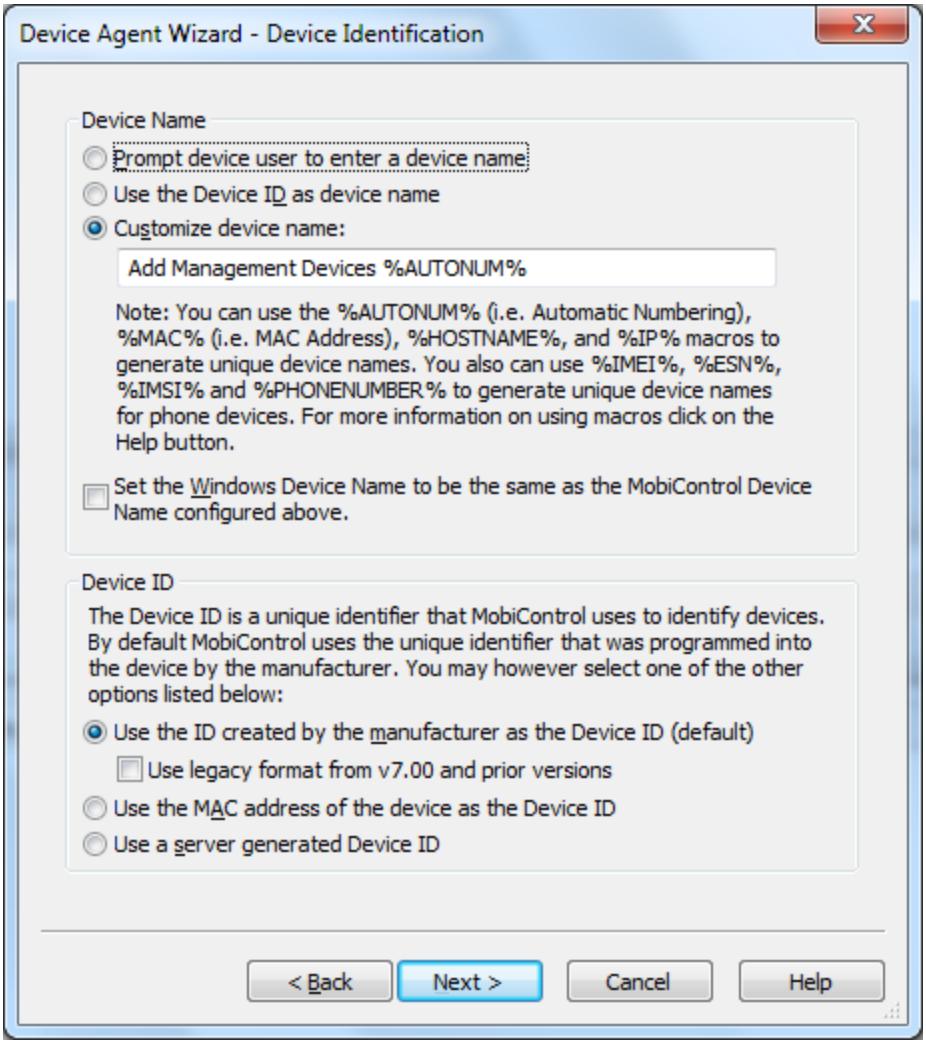
NOTE:

Configuration of the Deployment Server address should be performed before agents are created, as the address information will be embedded into the agent installer.

Field Name	Description
	of the Deployment Server via the IP network to which the device is connected. If your device will be on a public network such as the Internet, you will need to setup an externally routable address for your Deployment Server. Please see the "Set Deployment Server Properties" topic on page 383 for instructions on setting up an external IP address for the Deployment Server.
Automatic Deployment Server Discovery	When this option is enabled, MobiControl Device Agent(s) will attempt to discover Deployment Server(s) using UDP broadcasts when they cannot connect to configured servers. If you have multiple MobiControl installations on the same network, you need to set a unique site name for each installation so that the discovery process will not detect servers in a different installation.
Accept Direct Remote Control Connections	When this option is enabled, the Device Agent will accept direct remote control connections (TCP/IP remote control connection profile). A direct connection improves performance by reducing latency, however it requires the device to accept the connection without authentication unless SSL Security is enabled. (Please see the "Communication and Connection Security" topic on page 411 for more information about this.) Remote control is permitted via the TCP/IP(Server) remote control connection profile regardless of this setting.
List Agent in Remove Programs	When this option is disabled, no entry will appear for the agent in the Remove Programs settings applet on the device, thus preventing the agent from being uninstalled by the device user.
Include Initial Package	Allows you to specify a package that will be embedded into the Device Agent installer and automatically execute when the agent is installed on the device.
Device Stable Storage Folder	A stable storage folder is a special folder in the devices file system that is not erased when a device is hard reset. MobiControl uses the stable storage folder on the device to store data and packages so that MobiControl and packages and settings deployed via MobiControl can persist through hard reset. **NOTE:** Stable storage folders do not exist on all devices. For devices that do not feature a stable storage folder, MobiControl will default to a standard folder in the file system. Optionally, you may use an external SD card as the stable storage folder. This option is not recommended in most scenarios, as removal of the SD card will severely impact the operation of the MobiControl Agent.

7. Configure the device identifier.

   The **Device Identifier Configuration** page allows you to select how devices are named and uniquely identified.



Device Agent Name Configuration page

The following table provides descriptions for the three device naming options:

Field Name	Description
Prompt Device User	When this option is selected, the Device Agent will prompt the user for a device name when it is first started.
Use the Device ID	When this option is selected, the device ID will be used as the device name. Since the device ID is a cryptic string that is not very readable (e.g. `0003000F-3EAC-0F94-0F00-0300AA3EE877`), we generally do not recommend this option.
Customize the Device Name	This option allows you to enter text as well as use macros to create device names. MobiControl does provide macros. Please see the text following this table.
Set Windows Device Name Checkbox	When this option is checked, MobiControl will set the Windows Device Name to be the same as the MobiControl Device Name configured above.

Macros

- **%AUTONUM%** allows you to automatically use a numbered sequence as part of the device name. For example, if the value of this field is set to `WH%AUTONUM%`, then the first device configured will be assigned a name of `WH00001`, the second device will have a name of `WH00002`, and so on. `%MAC%` expands to the MAC address of the device. This macro is suitable for use with devices that have a wireless or wired networking capability. The MAC address is a unique number that is built into the network hardware used on the device. In most cases MobiControl can retrieve the MAC address from the hardware. For example, if the value of this field is set to `DEV%MAC%`, then the device names configured would look similar to `DEV00A0F85324D4` and `DEV00A0F8533422`. When the MAC macro is used as the Device ID, the Wi-Fi radio must be enabled when the agent is installed in order for the macro to work.
- **%HOSTNAME%** expands to the local host name of the device. We recommend using this macro only in cases where unique hostnames have previously been assigned to devices before the MobiControl Device Agent software is installed.
- **%IP%** expands to the IP address of the device. We recommend using this macro only in cases where the mobile devices have wireless or wired networking capabilities and are using fixed IP addresses. The use of this macro is not suitable for situations in which the mobile devices are using dynamic IP addresses (i.e. DHCP) since when the IP address changes the device name will be incorrect.
- **%PHONENUMBER%** expands to the phone number of the device. We recommend using this macro only in cases where the mobile device is a Smartphone or Pocket PC Phone Edition. For some devices, the phone number may not be available.
- **%IMEI%** expands to the IMEI (International Mobile Equipment Identity) number of the device. We recommend using this macro only in case where the mobile device is a Smartphone or Pocket PC Phone Edition. For some devices the IMEI number may not available.

- **%ESN%** expands to the ESN (Electronic Serial Number) number of the device. We recommend using this macro only in case where the mobile device is a Smartphone or Pocket PC Phone Edition. For some devices the ESN number may not available.
- **%IMSI%** expands to the IMSI (International Mobile Subscriber Identity) number of the device. We recommend using this macro only in case where the mobile device is a Smartphone or Pocket PC Phone Edition. For some devices the IMSI number may not available.
- **%REG://%** expands to the registry in the device. This will allow custom names like serial number (read from registry key) to be used out of the box for device naming, e.g. `%REG://HKEY_LOCAL_MACHINE\Software\Apps\SOTI\MobiControl?VN=ESN%`
- **%TXT://%** will get the content of specified line of the text file (if LN is not specified, it assumes the first line), e.g. %TXT://\Device.log?LN=1%
- **%INI://%** will pull a value from a Section in an `.ini` file and make it the device name, e.g. `%INI://\pdb.ini?SC=Device&NM=DeviceName%`
- **%EXE://%** will get the exit code of the executable and make it the device name, e.g. `%EXE://\windows\system32\calc.exe%`
- **%STDOUT%** will pull the first line of STDOUT output of the Executable and make it the device name, e.g. `%STDOUT://cmd.exe /c dir%`

The table below provides descriptions for device ID configuration:

Field Name	Description
Use the ID created by the manufacturer	Select this option to use the device ID created by the manufacturer to uniquely identify the device. This is the default and Windows recommended option.
Use legacy format from v7.00 and prior versions (Checkbox)	Check this option if you wish to use MobiControl's legacy format for manufacturer device ID.
Use the MAC address of the device	Select this option to use the device's MAC address to uniquely identify the device.
Use a server-generated Device ID	Select this option to allow the Deployment Server to automatically generate a unique ID for the device.

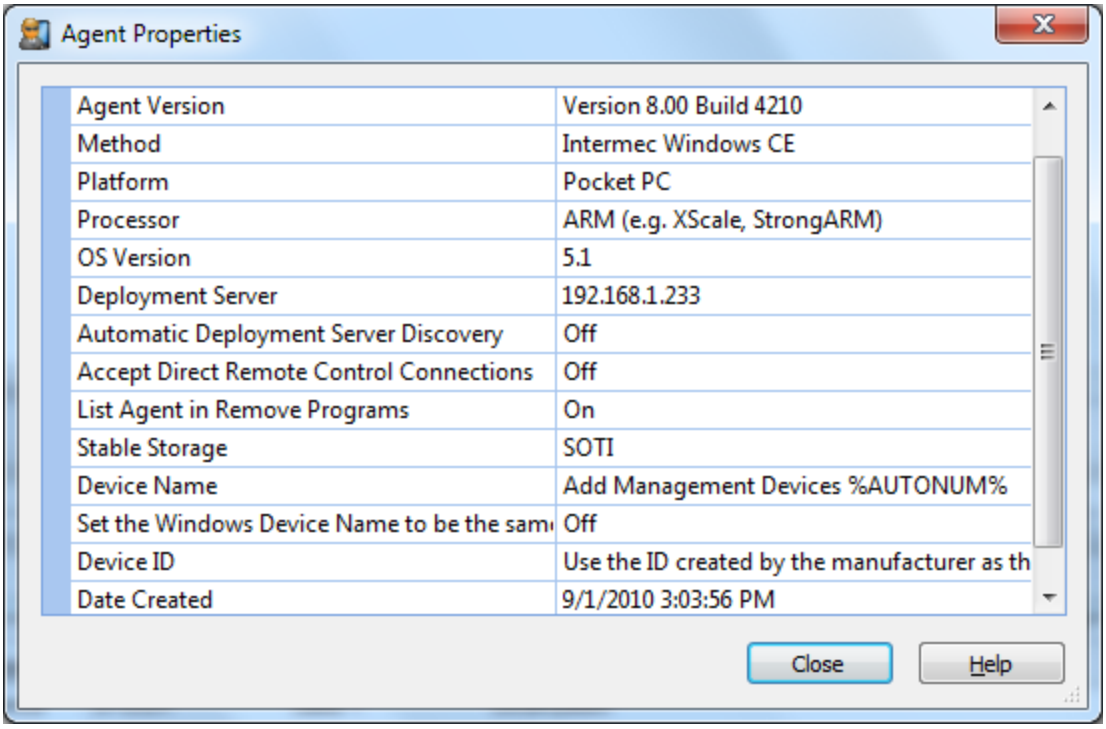
Click **Next** when you have completed the settings in this dialog box.

8. Review agent summary information.

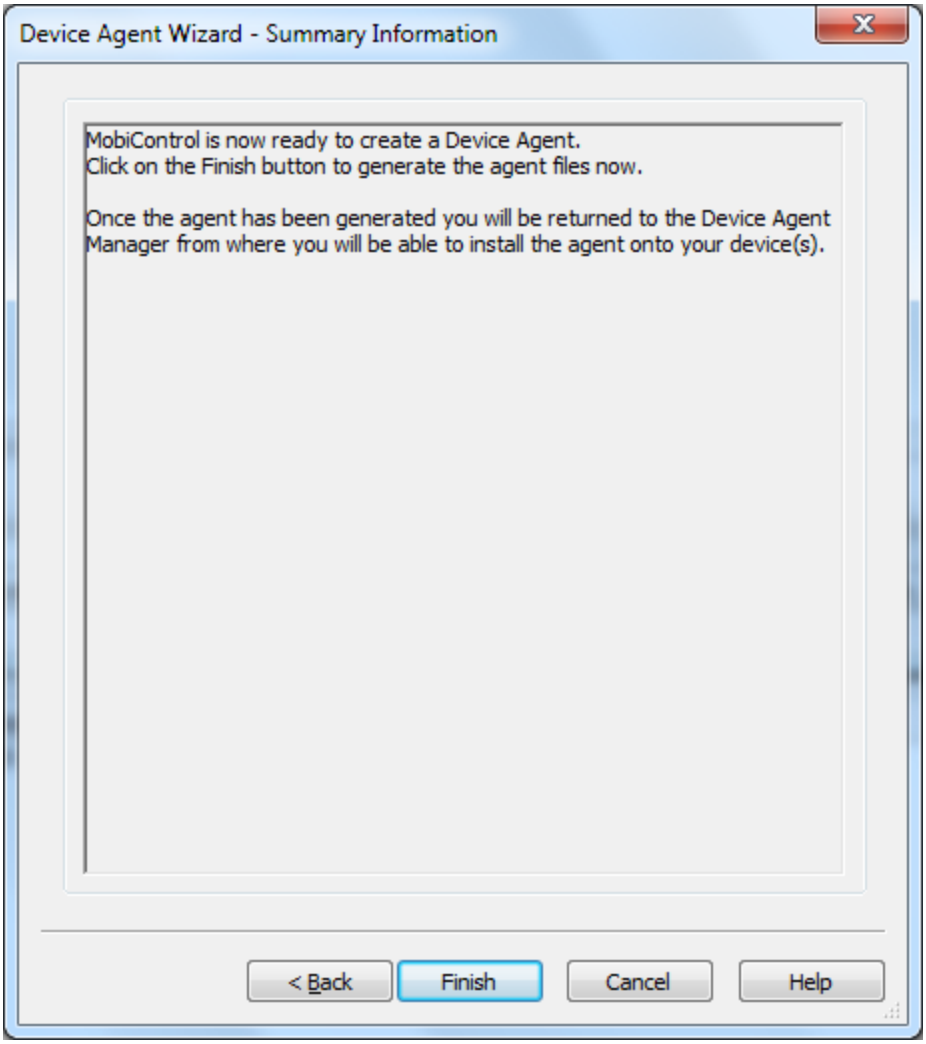
The **Agent Summary** page summarizes the information about the Device Agent and provides instructions for installing the Device Agent.

Click the **Finish** button to create the Device Agent files.

To see the details of an agent, right-click the agent and then select **Properties** from the pop-up menu.

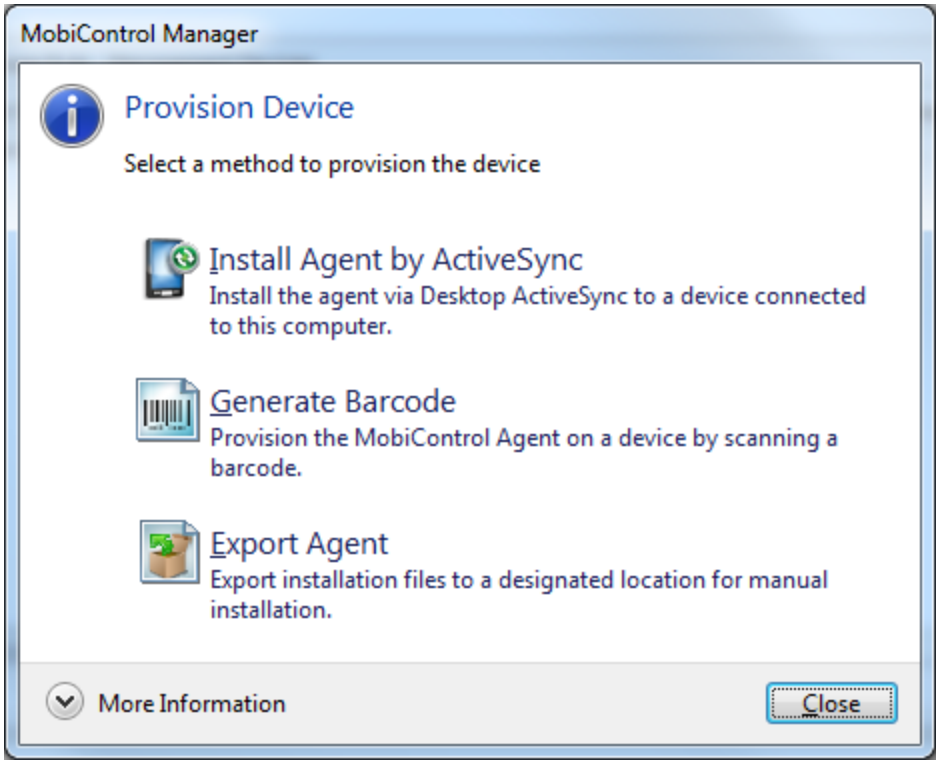


Agent Properties dialog box



Device Agent Wizard summary information page

9. Provisioning agent on a device.

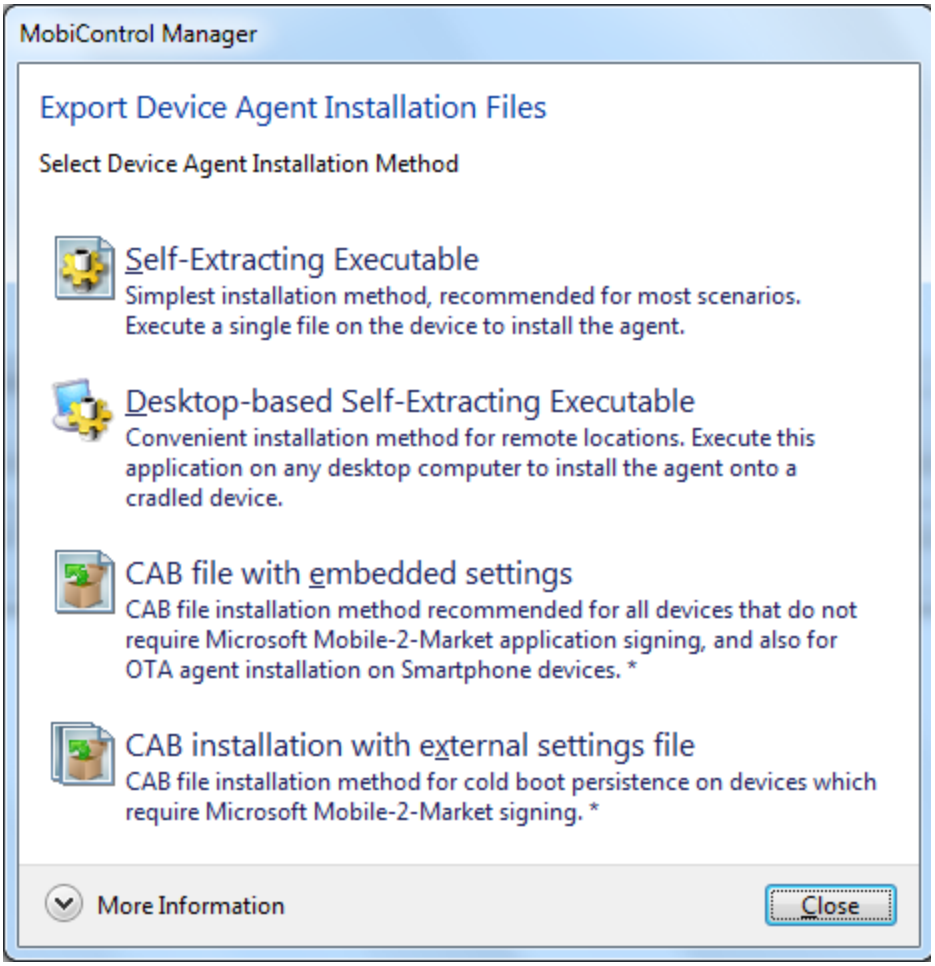


Provision Device Page

After the agent is created, you have several options to install it on the devices.

- If your device is connected to the computer running the Manager console via **ActiveSync**, click the **Install Agent by ActiveSync** button and the agent will be installed onto the connected mobile device.
- If you wish to provision the agent by scanning a **Barcode**, click on **Generate Barcode** button.

  Please refer to the Generating a Barcode section for further information regarding this.
- If you wish to **manually deliver the installation file(s)** to the devices, select the **Export Agent** button.



Export Device Agent Installation Files dialog box

You are given four options for export:

Option	Description
Self-Extracting Executable	This is the simplest installation method and is recommended for most scenarios. A single executable file (`*.exe`) will be exported. To install the agent, simply deliver this file to the device and execute it. The self-extracting executable contains the agent's installation `.cab` file, as well as any other supporting files that may be required for targeted device platform. **NOTE:** This method is not supported on Windows Mobile 5 Smartphone or Windows Mobile 6 Standard devices.
Desktop-based Self-Extracting Executable	Convenient installation method for remote locations. Execute this application on any desktop computer to install the agent onto a cradle synced device. This will open a light application that will install the agent on to the device via ActiveSync.

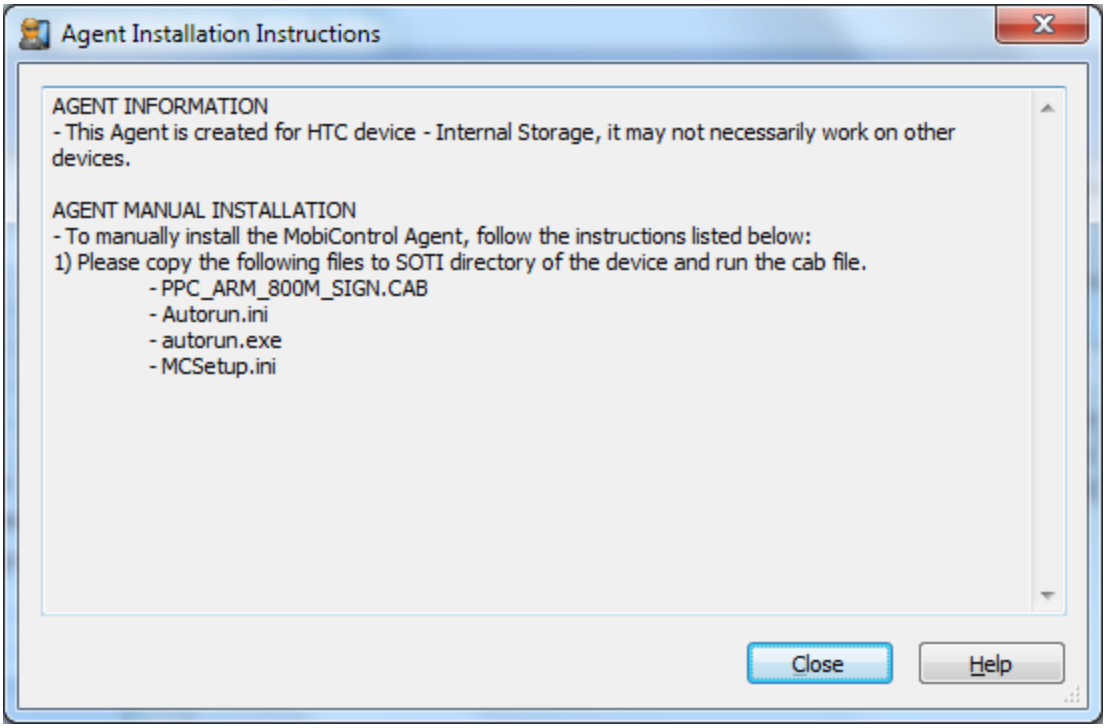
Option	Description
CAB file with embedded settings	.Cab file installation method recommended for all devices that: • do not require Microsoft Mobile-2-Market application signing. This includes devices that run Windows Pocket PC 2003 and earlier operating systems, Windows CE .NET devices, and rugged hand held devices (e.g. Intermec, Hand Held Products, Psion Teklogix, Symbol). • run Windows Mobile 5 Smartphone or Windows Mobile 6 Standard operating system (non-touch screen devices). Starting with Windows Mobile 5, Microsoft introduced the Mobile-2-Market application signing program. The MobiControl Device Agent .cab file for Windows Mobile 5 or later operating system devices is signed under this program. However, by embedding the settings selected during the Device Agent Wizard into the .cab file, the signature is invalidated. If you are installing the agent on a device that does NOT require Microsoft Mobile-2-Market signing, the invalidity of the signature is of no consequence. This method is recommended for Smartphone devices in the scenario where the agent will be made available as a web-download since the Internet browser on a Smartphone does allows .cab files, but not .exe files to be downloaded. Since all Smartphones require Mobile-2-Market signing, the device user will be prompted to confirm the installation of the "unsigned" .cab file. An exception to this recommendation is for Smartphone devices that have been confirmed with 2-tier security. These devices do not permit the installation of unsigned .cab files. In this situation, the first or third export option is recommended. **NOTE:** If the device has persistence and it also checks for applications to be Mobile-2-Market digitally signed (like a Pidion device), then you will encounter a problem if you deploy an agent with embedded settings (e.g. initial package or embedded cloned settings). The reason this happens is that the signature of the CAB has been broken, and so it will FAIL to re-install after a cold boot (because the device requires a signed CAB for a silent and automatic re-install).
CAB file with external settings file	.Cab file installation method for devices which require Microsoft Mobile-2-Market signing. In this method, the signature of the .cab file remains intact since the settings are specified in a separate file called MCSetup.ini. Both the .cab file and MCSetup.ini file must be delivered to the device, along with any other files that may be exported. See the manual installation instructions for details.

Manual Installation Examples

NOTE:

Smart phones are capable of downloading only `.cab` files.

- Post the `.cab` or `.exe` on a **website** and direct your users to select the link.
- Deliver the `.cab` or `.exe` file as an **email attachment** with instructions for your users to execute the attachment.
- Deliver the `.cab` or `.exe` on an **SD card**, and execute the file on the device.
- Transfer installation files via existing **network** applications.



Agent Properties dialog box

To see the instructions on how to install an agent manually, right-click the agent, and then select **Instructions for Manual Installation** from the pop-up menu. Due to the variations between different devices on the market, each set of install instructions is unique. Review the installation instructions provided in the `readme.txt` file exported along with the installation file(s).

Rule Filters

The **Add Devices Rule Advanced Settings** are accessible from the Create Add Devices Rule Wizard by clicking the **Advanced Button** (Advanced Tab when editing a Rule.) This page allows you to specify which devices are to be configured by a specific Add Devices Ruleadd devices rule. By default when you create an Add Devices Rule, MobiControl will use the rule to configure only those devices that are running a Device Agent Device Agent created specifically for that Add Devices Rule. By using Advanced Settings filters, you can broaden or further restrict which devices get configured by a specific rule when they connect to MobiControl.

Types of Filters

- Rule Tag Filter

  The **Rule Tag filter** will cause the rule to configure only devices with a certain device rule tag. When a MobiControl Device Agent is generated, a unique identifier (rule tag) is inserted into the agent. When the Device Agent connects to a MobiControl Deployment Server, it presents the server with the rule tag. When this filter is used, the Deployment Server will only configure a device if there is a match between the rule tag presented by the agent and an add devices rule in the database. In this way, an add devices rule will be used to configure only those devices that are using an agent specifically created for that rule.

  This is the default filter; it is automatically added when an add devices rule is created. If this filter is removed, then this rule can be used to configure devices that are using Device Agents created by third parties (i.e. When a MobiControl Device Agent is already installed on the device when it comes from the manufacturer) or Device Agents created for other device configuration rules.

- IP Address Filter

  The **IP address** filter causes the add devices rule to configure only those devices whose IP addresses are in the range specified. This rule is useful as an extra security blanket for limiting connections to only devices that have an IP within the authorized range of IP addresses. The rule may also serve as a means of segregating different sets of devices.

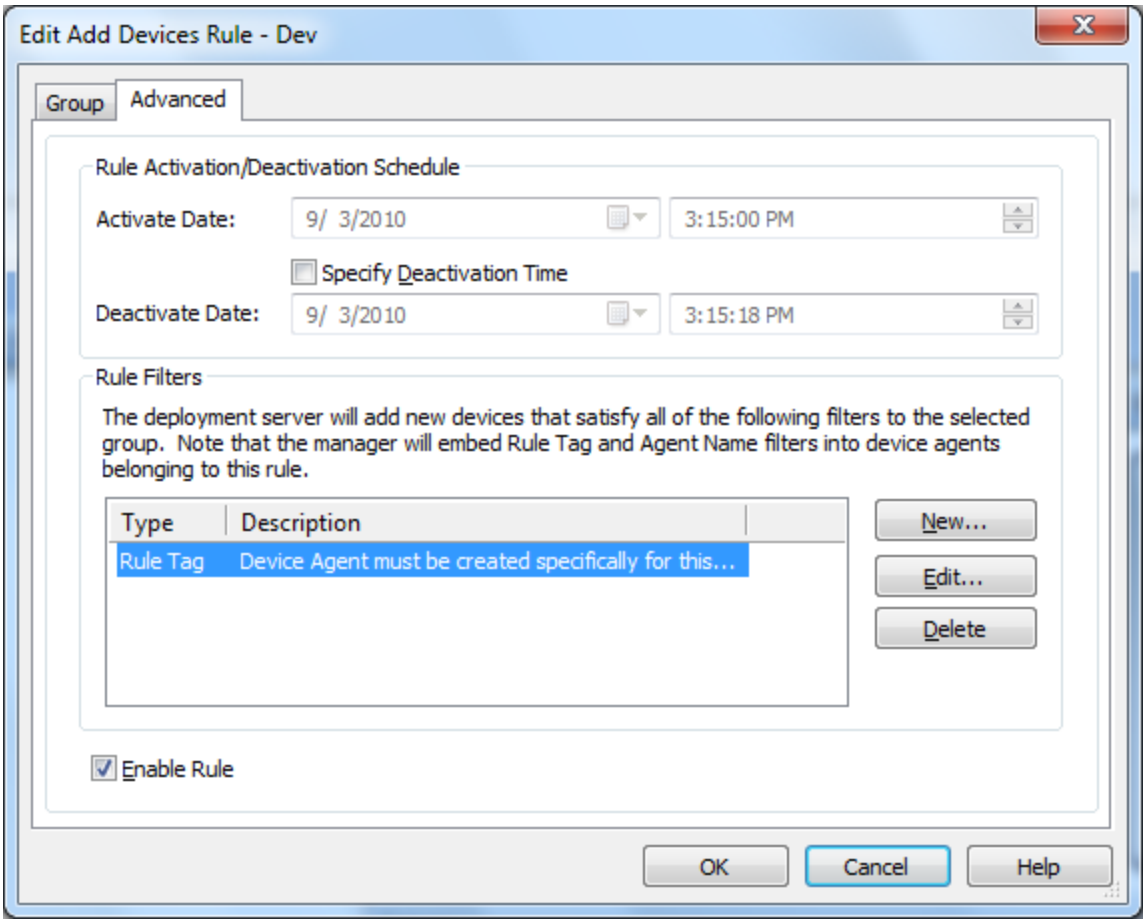
  EXAMPLE:

  If an IP address filter from 192.168.1.10 to 192.168.1.99 has been set, then only devices with an IP address in this range would be configured by this add devices rule. If a device with an IP address of 192.168.1.100 connects to MobiControl, it would not satisfy the IP address filter test for this rule and so, it would not be configured by this rule.

  The IP address filter is used for limiting connections to approved IP ranges. Please see the "Device Relocation Rule" topic on page 335 for dynamic relocation of devices from one device group to another and reconfiguring devices based on the IP address of the mobile devices (or other criteria).

- Agent Name Filter

  The **agent name filter** causes the add devices rule to affect only devices with the same agent name. When this filter is set, all agents generated for this rule will automatically be named appropriately. This rule is useful in the event you have a set of devices already equipped with Device Agents. Simply creating this rule will allow the Device Agents on those devices to connect to the Deployment Server.

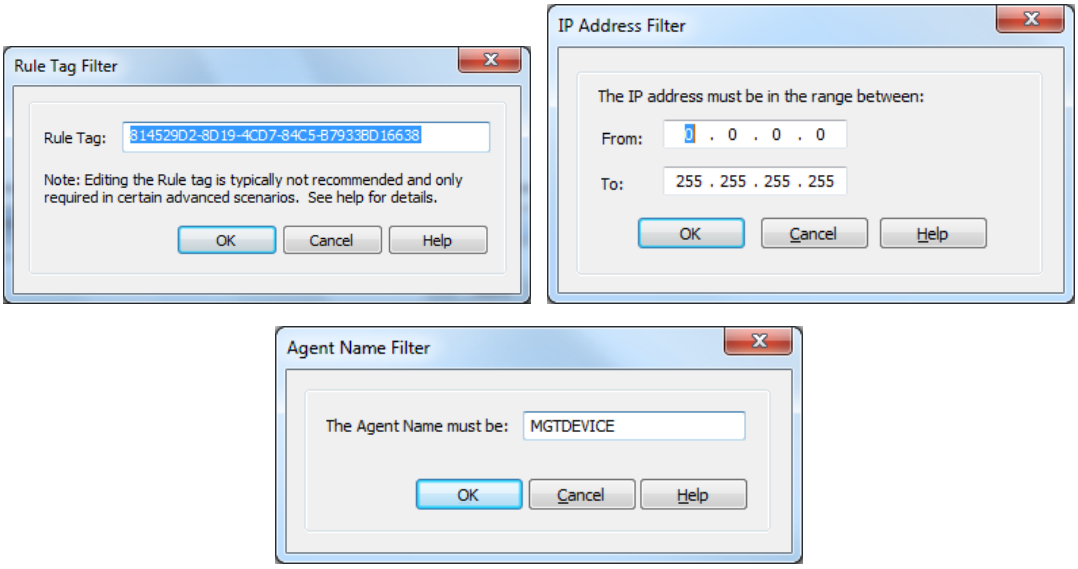


Add Devices Rule Advanced Settings dialog box

Adding a Filter

To add a filter, click the **New** button and select the appropriate filter type from the pop-up menu.

The dialog box displayed depends on the type of filter selected. If the **Add IP Address Filter** was selected from the menu, the **IP Address Filter** dialog box will be displayed. If the **Add Agent Name Filter** was selected, the **Agent Name Filter** dialog box will be displayed. If an **Add Devices Rule** is created, the filter is automatically added. This option will not be available if this filter has already been added.



Rule Tag Filter, IP Address Filter dialog box and Agent Name Filter dialog box

To complete the operation, fill in the information asked for in the dialog box and click the **OK** button.

Editing or Deleting a Filter

To edit or delete a filter, select the filter from the filter list and click the **Edit** or **Delete** button.

Creating Alert Rules

Alert Rules allow Administrators to be notified when events of interest arise on the system. This notification system allows Administrators to quickly and effortlessly communicate an event message to large groups of people via email, and notifies users via the MobiControl Manager Alert popup window. For every type of scenario, whether it is a Rule Change or a Device Error, the system will rapidly deliver your message to a designated audience.

To create an Alert Rule, select the Rules view (tab) within MobiControl Manager, then click the **Rule** menu, select **Create Rule**, and click **Alert Rule**. The Create Alert Rule Wizard will be displayed.

NOTE:

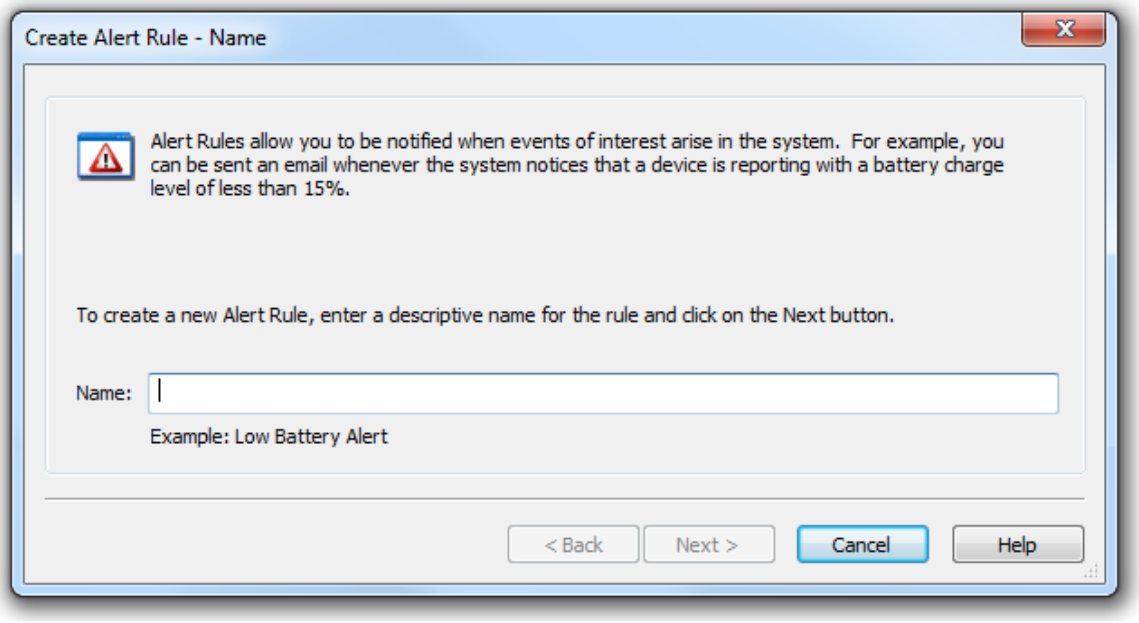
The Deployment Server must be online in order for Alerts to be generated and sent out.

The steps below describe how the Create Alert Rule Wizard can be used to create an add devices rule:

1. ### Start the wizard.

   Select the Rules view (tab), then click the **Rule** menu, select **Create Rule**, and click **Alert Rule**. The first page of the Create Alert Rule Wizard will be displayed.

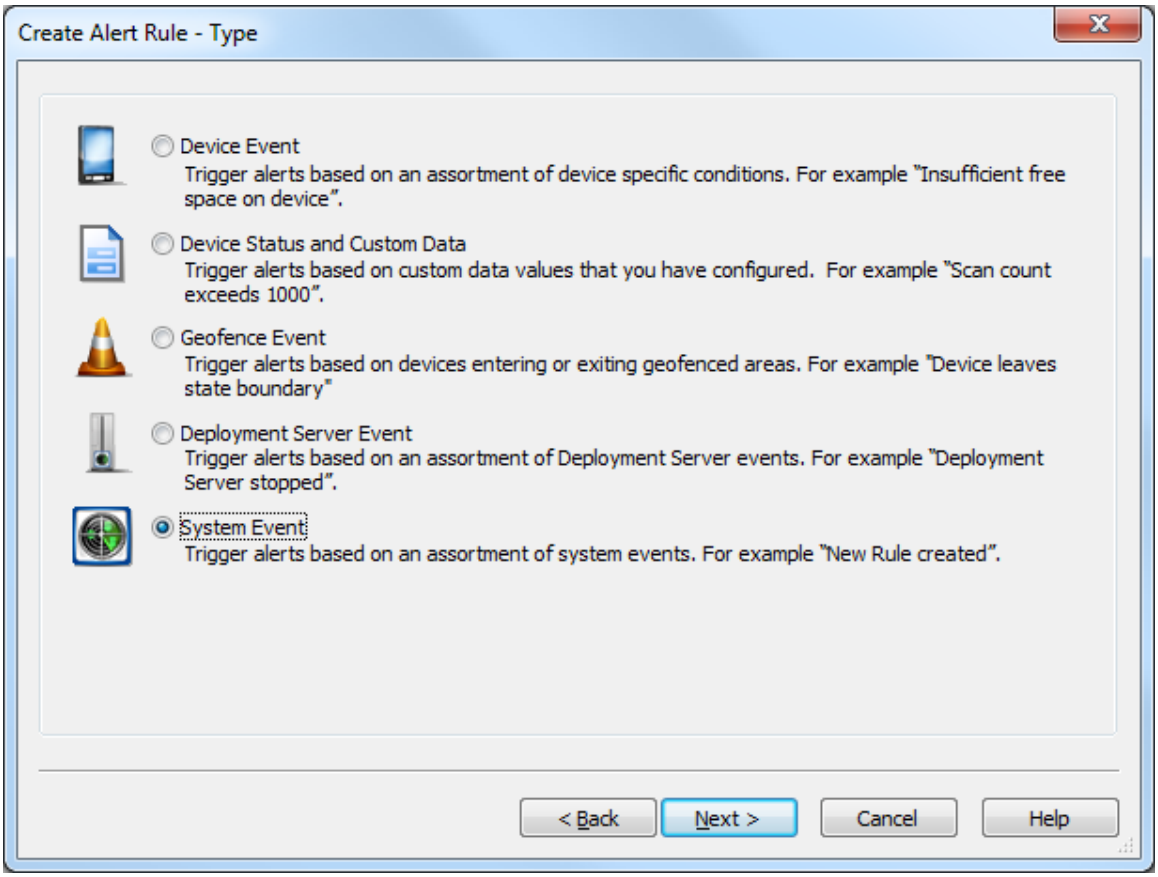
   Enter a descriptive name for the Alert Rule you are creating and click **Next.**



First page of the Alert Rule Wizard

Select the Alert Rule Type.

2.

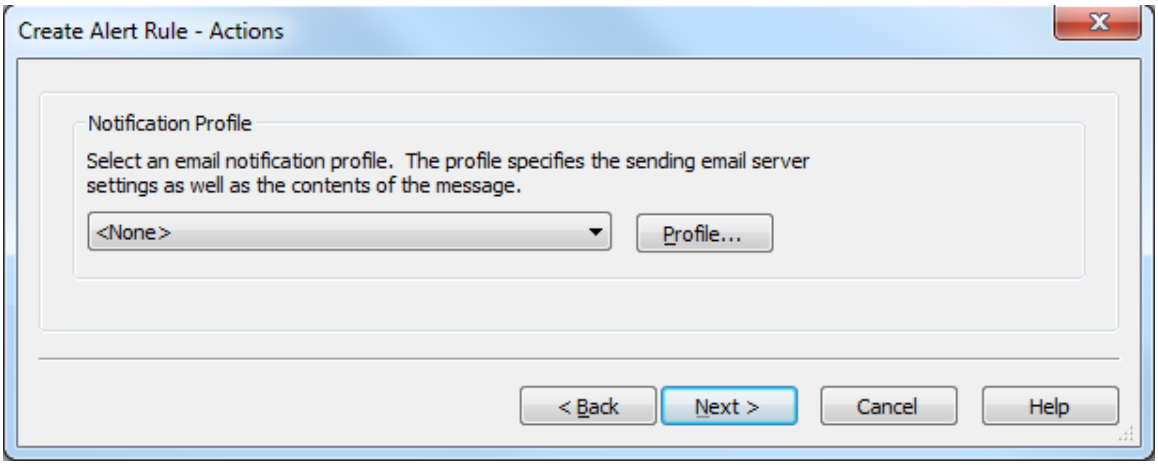


Select the Alert Rule Type and click Next.

Type	Description
Device Event	Trigger alerts based on an assortment of device specific conditions.
Device Status and Custom Data	Trigger alerts based on Custom Data vales that you have configured.
Geofence Event	Trigger alerts based on devices entering or exiting geofenced areas.
Deployment Server Event	Trigger alerts based on an assortment of Deployment Server events.
System Event	Trigger alerts based on an assortment of system events.

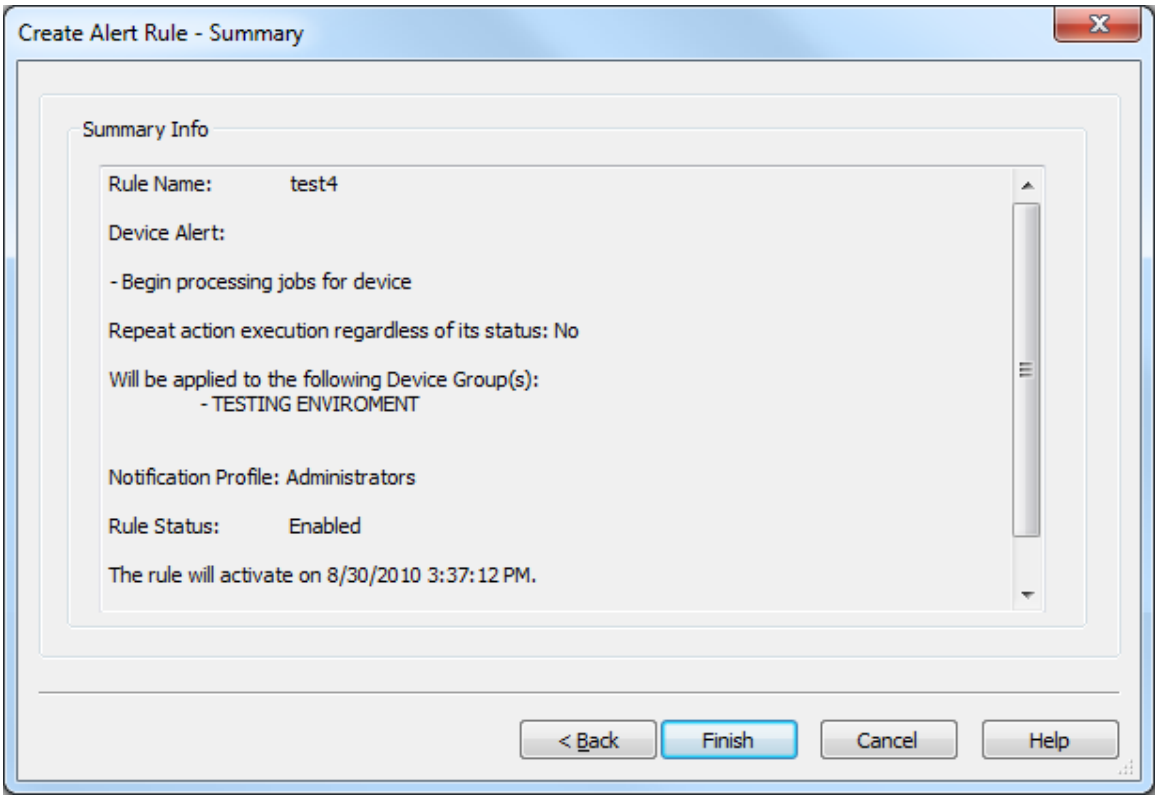
Notification Profile Settings

3. Once the Alert Rule is selected, you must select your Notification Profile.



Select an existing notification profile, or click New to create a new Notification Profile. For assistance with notification profiles click here. Once you have selected your notification profile click Next.

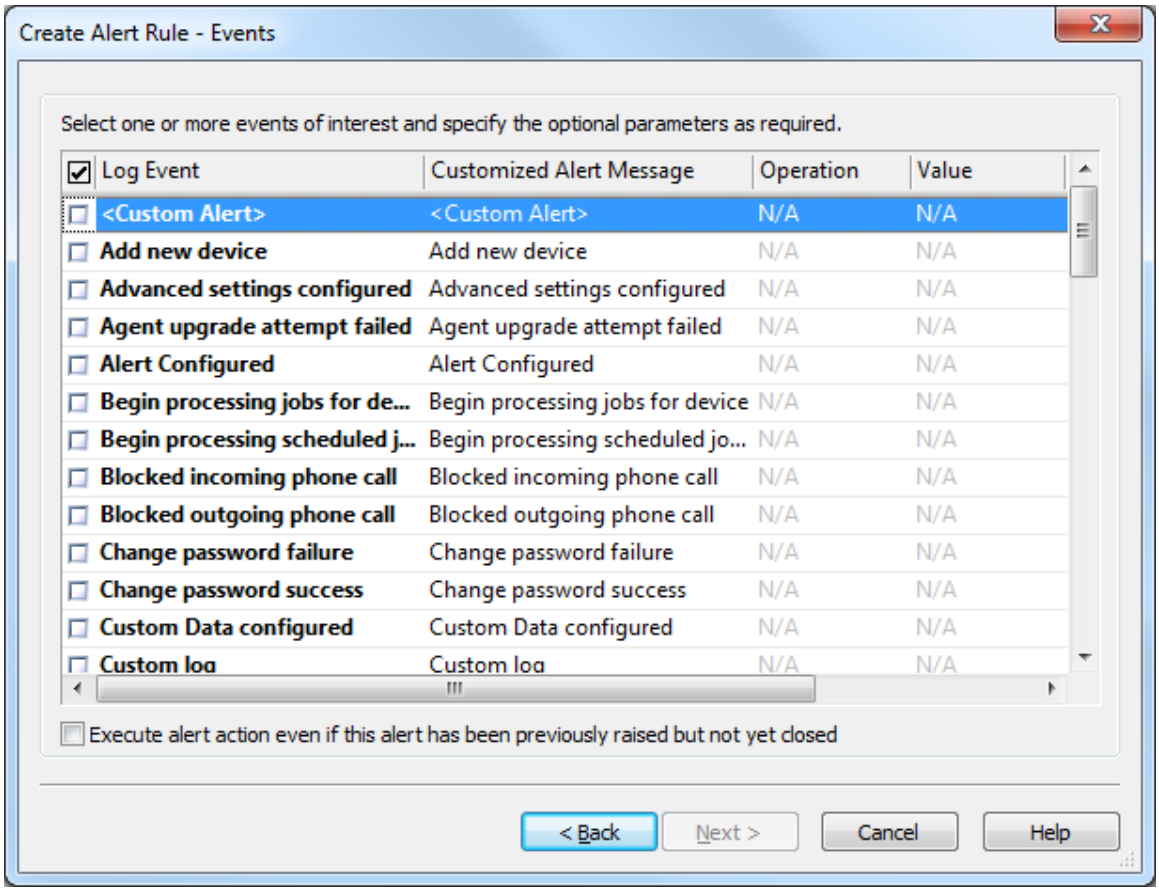
Review the summarized information.



4. Click **Finish** to complete the wizard.

Device Event

A Device Event is an alert triggered based on an assortment of device specific conditions. See below for a full list.



Device Event Notification Selection Window

Severity is set to Minor by default and can be altered.

The below table shows all available default Device events:

Log Event	**Alert Message (Customisable)**
<Custom Alert>	<Custom Alert>
Add new device	Add new device
Advanced settings configured	Advanced settings configured
Agent upgrade Attempt failed	Agent upgrade attempt failed
Alert Configured	Alert Configured
Begin processing jobs for device	Begin processing jobs for device
Begin processing scheduled jobs	Begin processing scheduled jobs
Blocked incoming phone call	Blocked outgoing phone call
Change password failure	Change password failure
Change password success	Change password success

Log Event	Alert Message (Customisable)
Custom Data configured	Custom Data configured
Custom log	Custom log
Data Collected	Data Collected
Data Collection configured	Data Collection configured
Dependent packages not installed	Dependent packages not installed
Device connected	Device connected
Device disabled	Device disabled
Device disconnected	Device disconnected
Device Enabled	Device Enabled
Device has not been connected for %VALUE% minutes	Device has not been connected for %VALUE% minutes
Device Manually relocated	Device Manually relocated
Device relocated	Device relocated
Device security configured	Device security configured
Error creating file on device	Error creating file on device
Error message received from device	Error message received from device
Error receiving file	Error receiving file
Error sending file	Error sending file
Error sending message	Error sending message
Error writing to file on device	Error writing to file on device
Exchange ActiveSync configured	Exchange ActiveSync configured
File synchronization failed	File synchronization failed
File synchronization was aborted by pre-sync script	File synchronization was aborted by pre-sync script
File(s) synchronized	File(s) synchronized
File synchronization was aborted by pre-sync script	File synchronization was aborted by pre-sync script
File synchronization failed	File synchronization failed
Geofencing Configured	Geofencing Configured
Inaccurate device date-time detected	Inaccurate device date-time detected
Incompatible platform, processor or OS version	Incompatible platform, processor or OS version
Installation aborted by user	Installation aborted by user
Installation was aborted by install script	Installation was aborted by install script

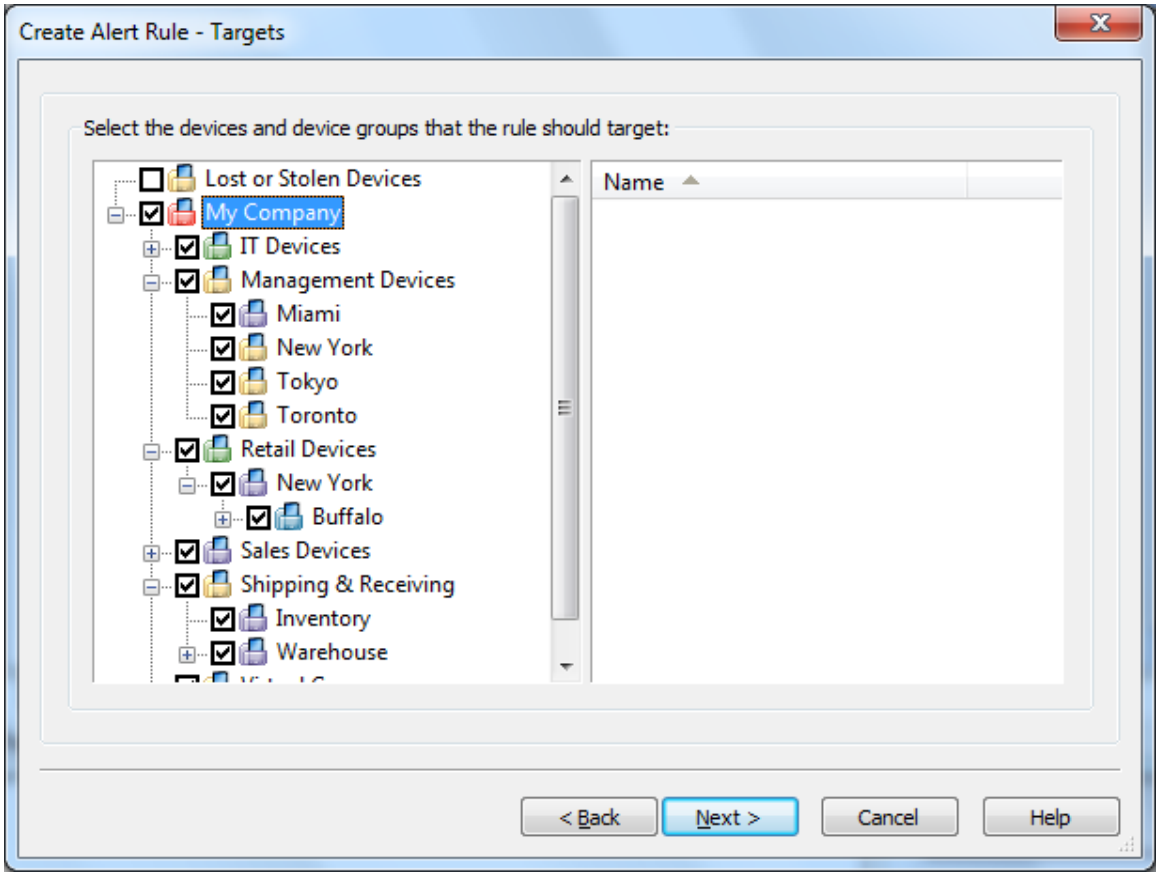
Log Event	Alert Message (Customisable)
Insufficient free space on device	Insufficient free space on device
Invalid device software version	Invalid device software version
Invalid message received from device	Invalid message received from device
Lockdown removed	Lockdown removed
Logon failure	Logon failure
Logon success	Logon success
Multiple packages with the same name in job list	Multiple packages with the same name in job list
No Package ID in installation report	No Package ID in installation report
Package file is corrupted	Package file is corrupted
Package file not found	Package file not found
Package uninstalled	Package uninstalled
Package with higher version number already installed on the device	Package with higher version number already installed on the device
Pending jobs cannot be processed until device user is authenticated	Pending jobs cannot be processed until device user is authenticated
Process Learned	Process Learned
Processed successfully	Processed successfully
Remote Control	Remote Control
Stopped illegal process	Stopped illegal process
Time Sync Configured	Time Sync Configured

The following list of variables are only available within the Customized Alert Message field:

Type	Description
%RULENAME%	The name of the rule
%PACKAGENAME%	The name of the package

Select devices.

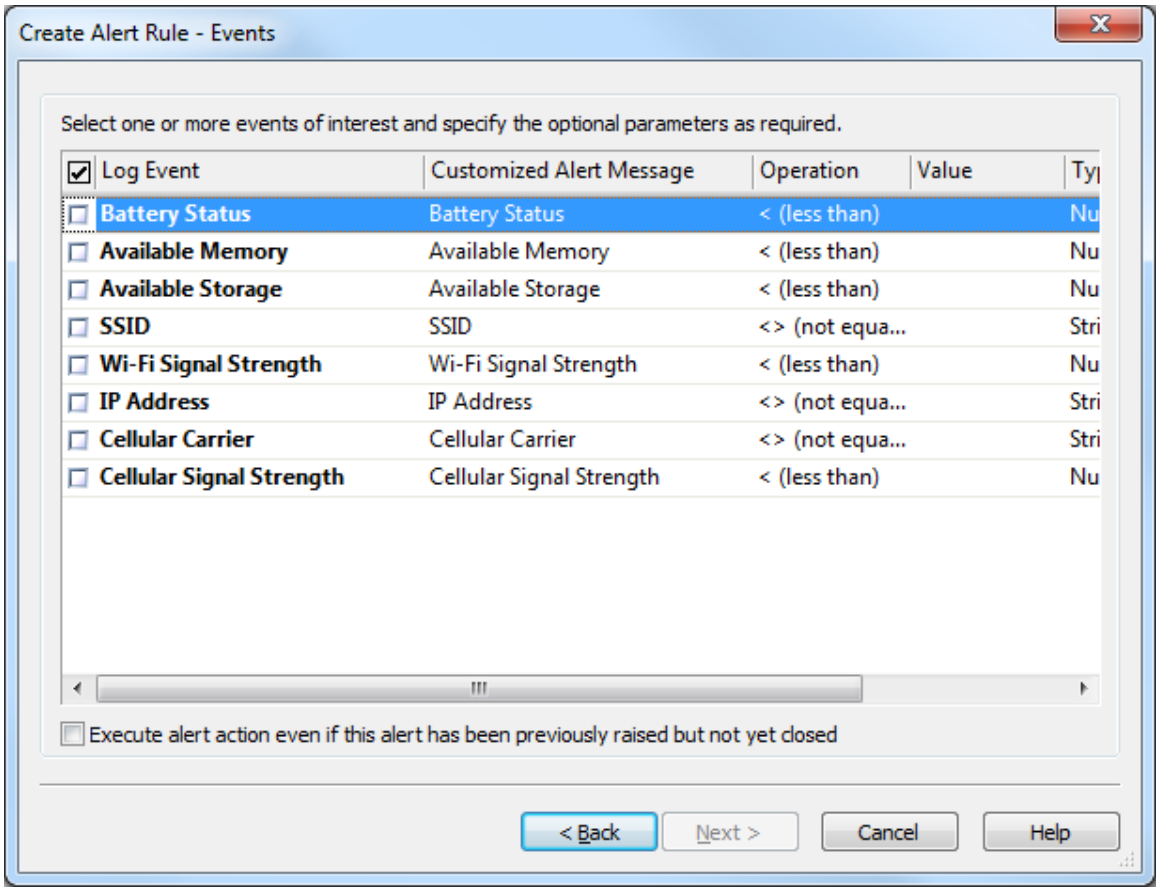
Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



After selecting your target devices, click Next and continue the Alert Rule Wizard here.

Device Status and Custom Data Event

A Device Status and Custom Data Event is an alert triggered based on an assortment of data values that you have set. See below for a full list.



Device Status and Custom Data Event Notification Selection Window

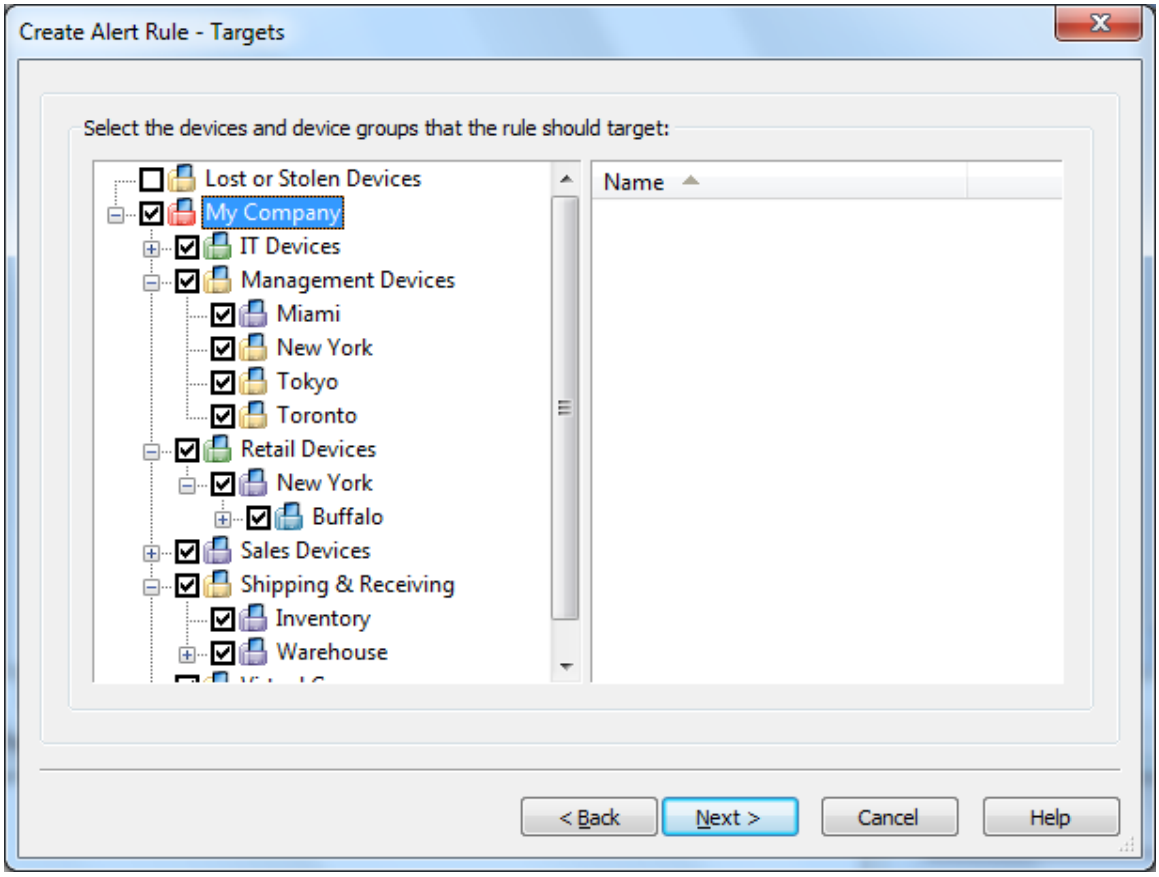
The Operation and Value fields allows to filter out Alerts based on specific values or value ranges. The Operation field specifies at which point an alert will be created for the data value you have specified. Severity is set to Minor by default and can be altered.

The below table shows all available default Device Status and Custom Data Event events:

Log Event	**Alert Message Alert Message (Customisable)**
Battery Status	Battery Status
Available Memory	Available Memory
Available Storage	Available Storage
SSID	SSID
Wi-Fi Signal Strength	Wi-Fi Signal Strength
IP Address	IP Address
Cellular Carrier	Cellular Carrier
Cellular Signal Strength	Cellular Signal Strength

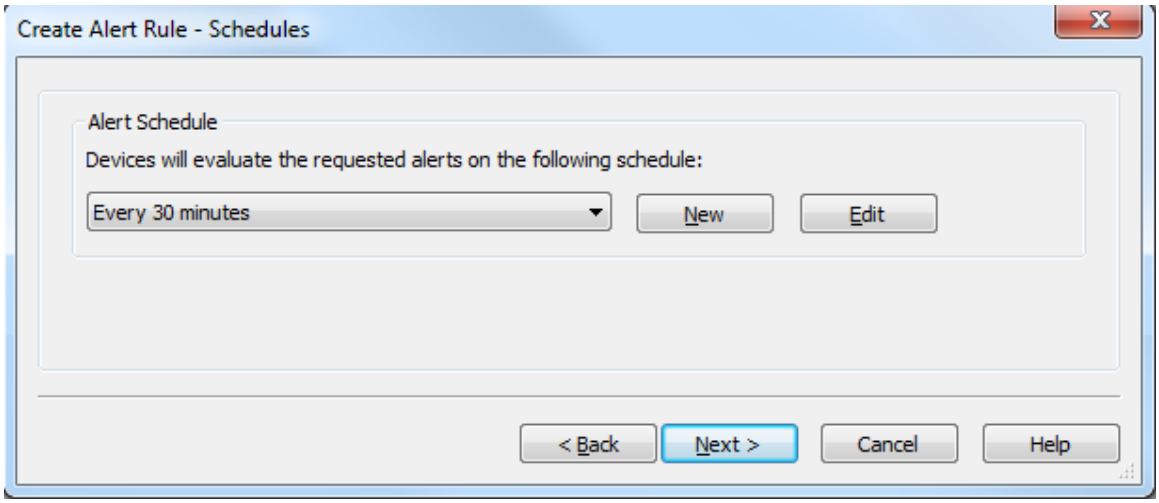
Select devices.

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



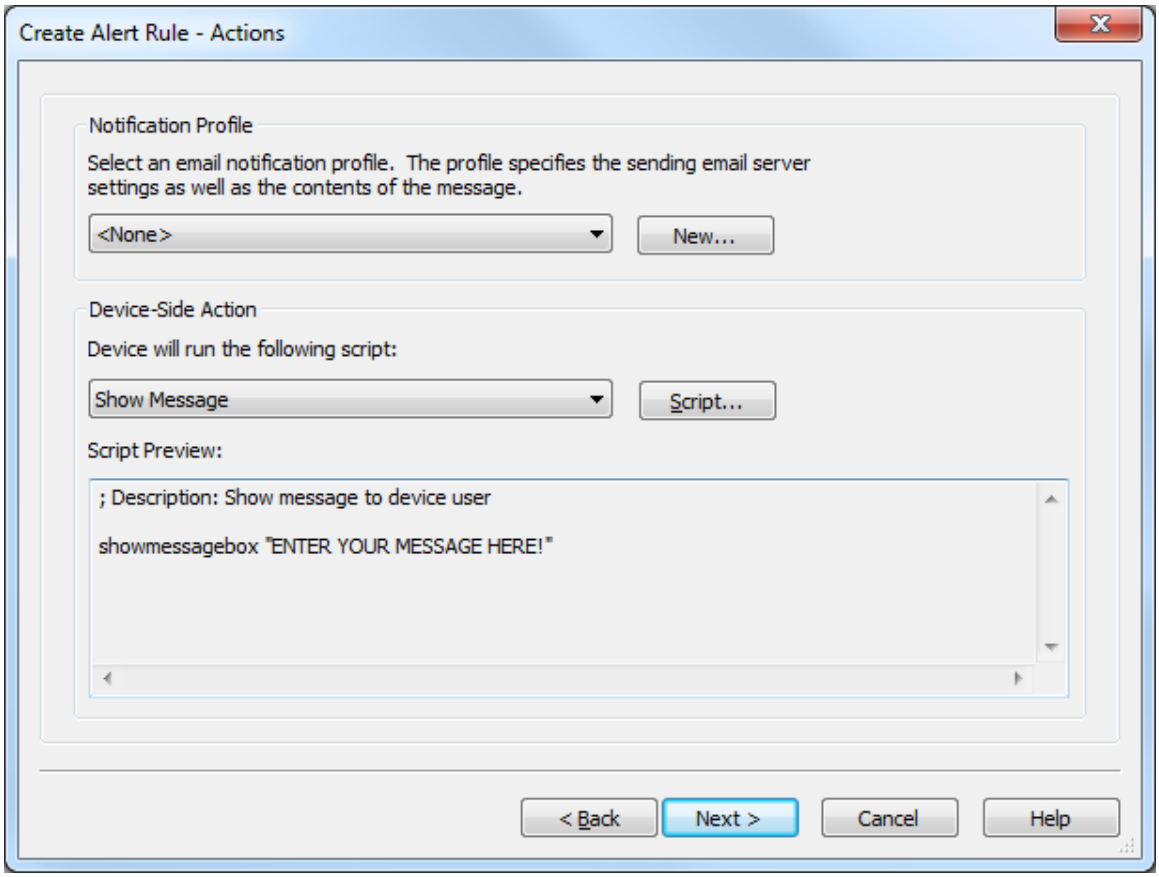
Select Schedule.

Select how frequently the devices should be checked for the requested Alert information. Once you have completed this section, click the **Next** button.



Select Actions.

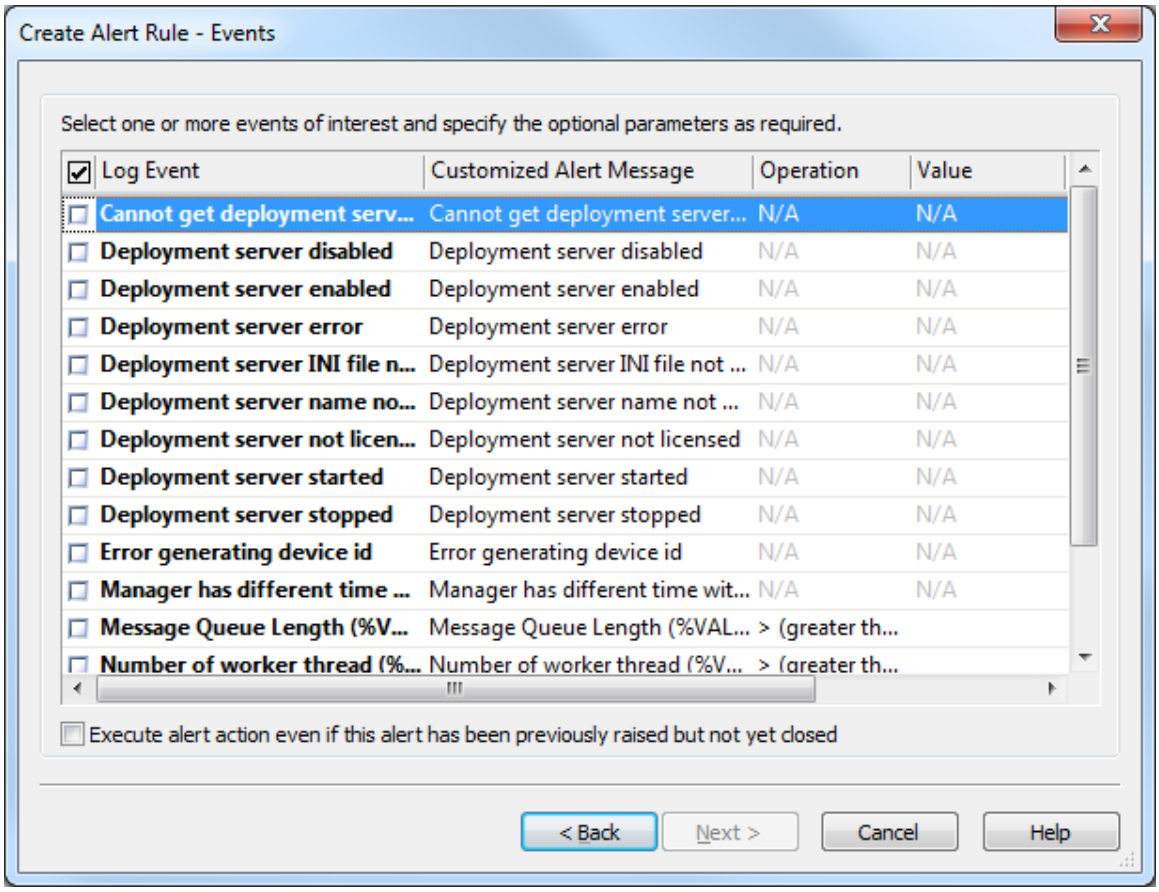
Select an existing notification profile, or click Profile to create a new Notification Profile. For assistance with notification profiles Click Here. Once you have selected your Notification Profile you can select a Device Side Action. This action is a script that will be launched on the device when certain criteria is met. For assistance with the Script Manager Click Here.



After selecting your Profile and Actions, click Next and continue the Alert Rule Wizard here.

Deployment Server Event

A Deployment Server Event is an alert trigger based on an assortment of Deployment Server Events. See below for a full list.



Deployment Server Event Notification Selection Window

The Operation and Value fields allows to filter out Alerts based on specific values or value ranges. The Operation field specifies at which point an alert will be created for the data value you have specified. Severity is set to Minor by default and can be altered.

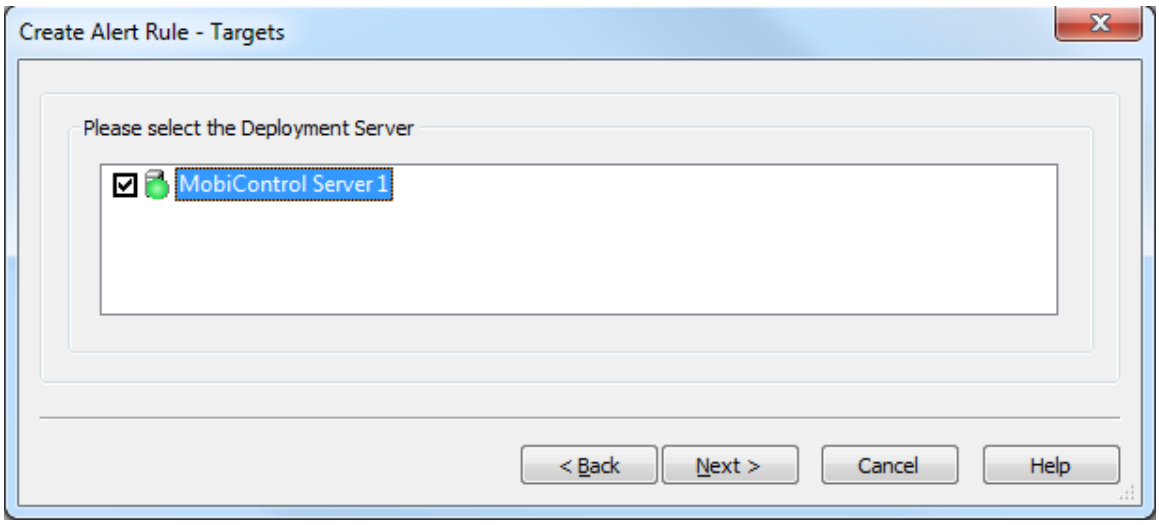
The below table shows all available default Deployment Server events:

Log Event	Description
Deployment server started	Deployment server started
Deployment server stopped	Deployment server stopped
Deployment server disabled	Deployment server disabled
Deployment server enabled	Deployment server enabled
Deployment server not licensed	Deployment server not licensed
Deployment server INI file not found	Deployment server INI file not found
Deployment server name not defined	Deployment server name not defined
Cannot get deployment server IP address	Cannot get deployment server IP address

Log Event	Description
Error generating device id	Error generating device id
Deployment server error	Deployment server error
Manager has different time with deployment server	Manager has different time with deployment server
Unknown device class name	Unknown device class name
Message Queue Length	Message Queue Length
Number of worker threads	Number of worker threads

Select Deployment Server.

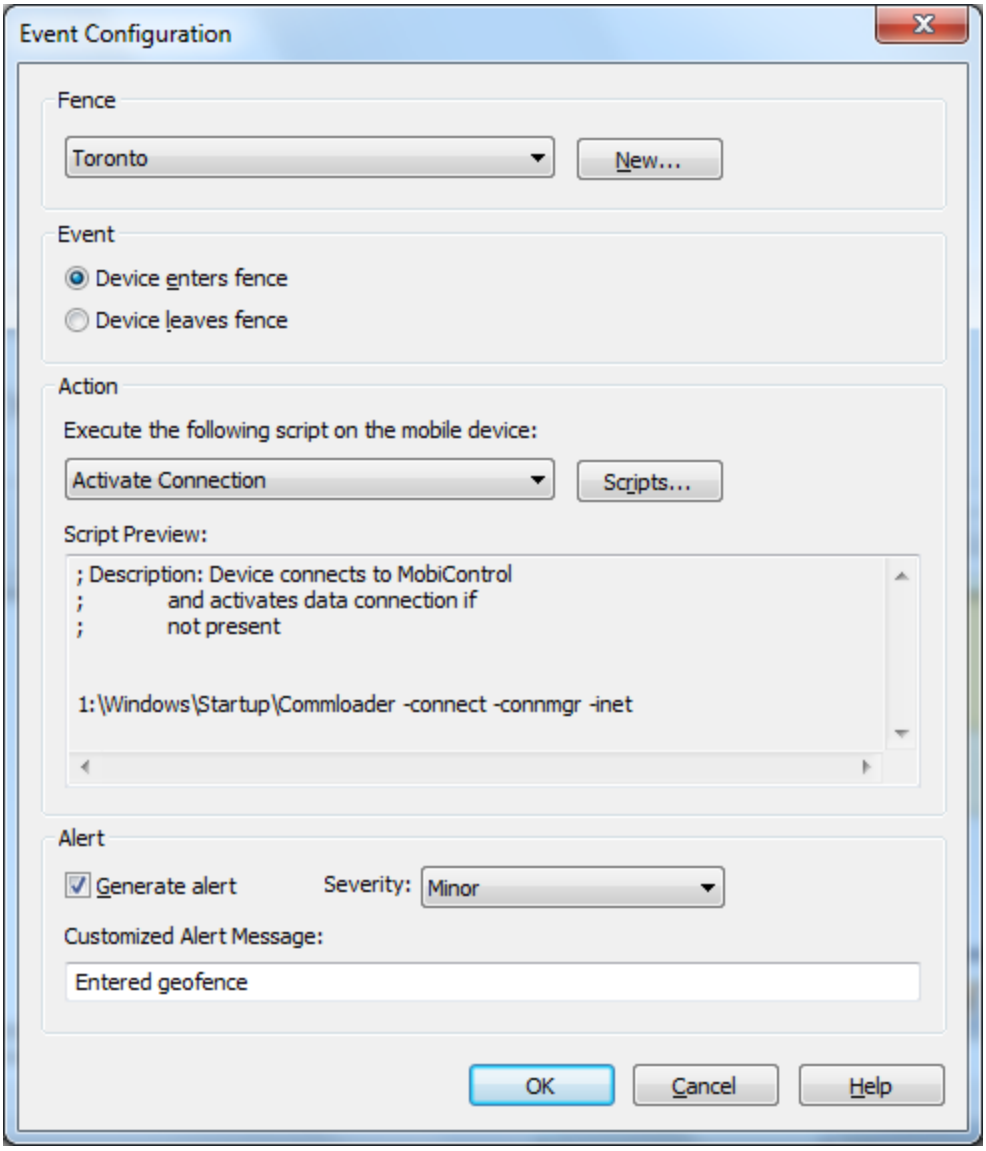
Select the Deployment Server(s) to which the rule will be applied. Once you have completed this section, click the **Next** button.



After selecting your target Deployment Server(s), click Next and continue the Alert Rule Wizard here.

Geofence Event

A Geofence Event is an alert trigger based on a GPS enabled device entering or leaving a Geofenced area defined by you. In order to create a Geofence event, you need to create an Alert Rule with a Type of Geofence Event.



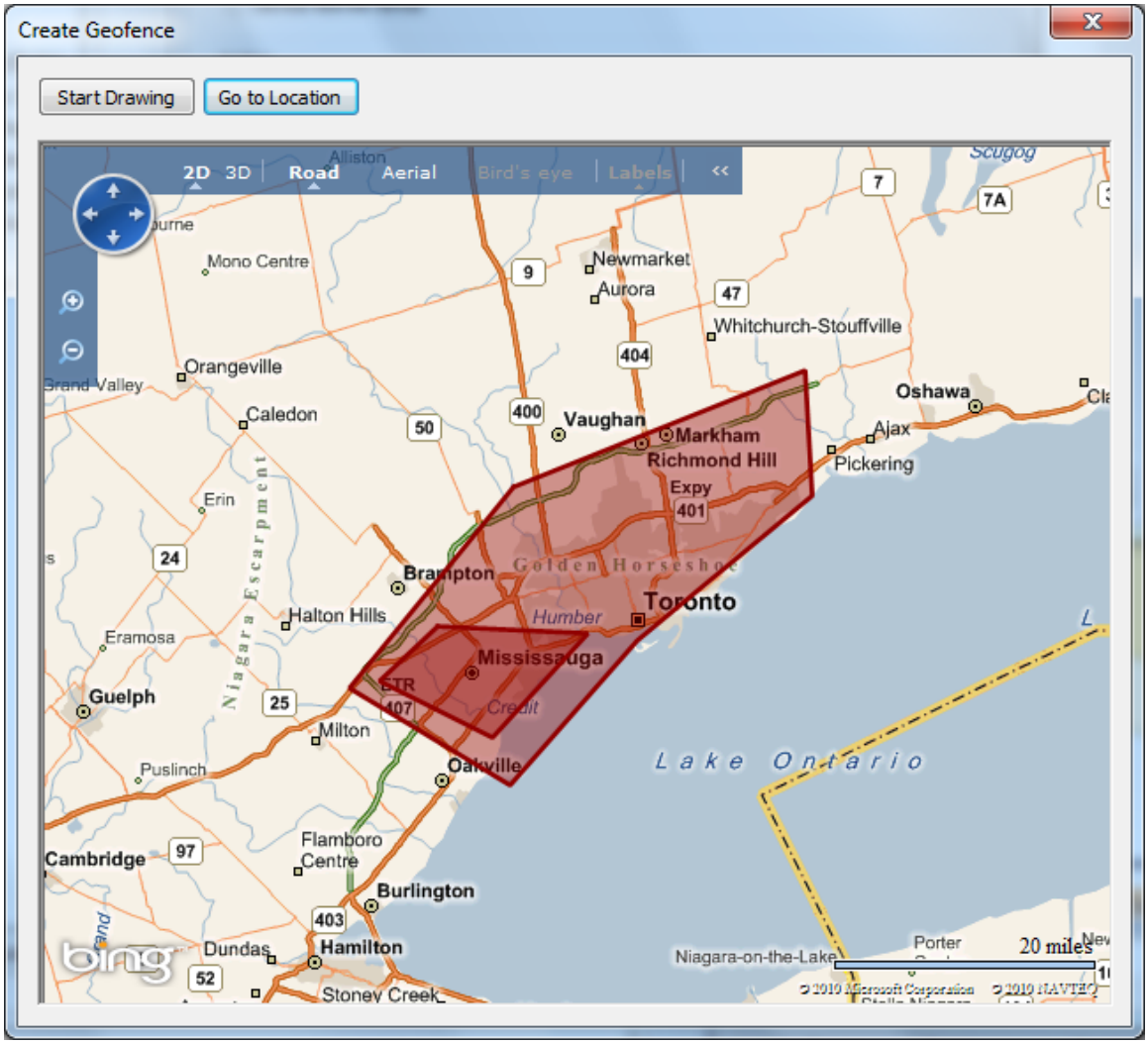
The **Fence** section allows you to create a geofence by clicking on the New button in the dialog box.

The **Event** section allows you to configure whether this event should be triggered on entry or exit of a fence.

The **Action** section allows you to configure what script you want to run on the mobile device when the event is triggered. This is optional, but you have for example the ability to run an Activate Connection, Log Event, Show Message or even wipe the device completely.

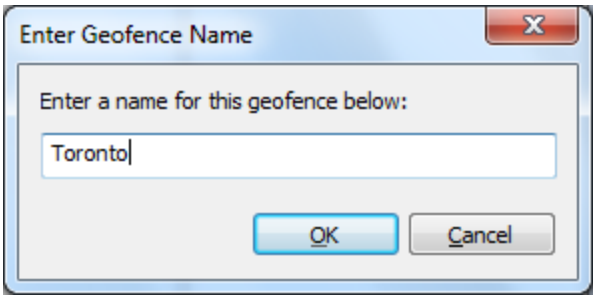
The **Alert** section allows you the option to Generate an alert, configuring its Severity (Minor, Serious and Critical) and add a Customized Alert Message, such as "Entered geofence".

When you click on the **New** button in the **Fence** section, the following Geofence Creation dialog box appears:



The two options available are to Start Drawing and Go to Location.

The **Start Drawing** option allows you to begin drawing on the map below the button. The area drawn on the map will be defined as the Geofence. The defined area must be a complete geometric shape, which means the Start Drawing point will be the same as the End Drawing point. When you have completed a proper geometric shape you be asked to name your geofenced area.



Prior to selecting the Start Drawing button, you have the ability to use the view control buttons in the map in order to move to a desired location, zoom in and out, switch to 3D, Road, Aerial and Bird's eye views among the many options. This allows you ease to create an appropriate view for your geofence.

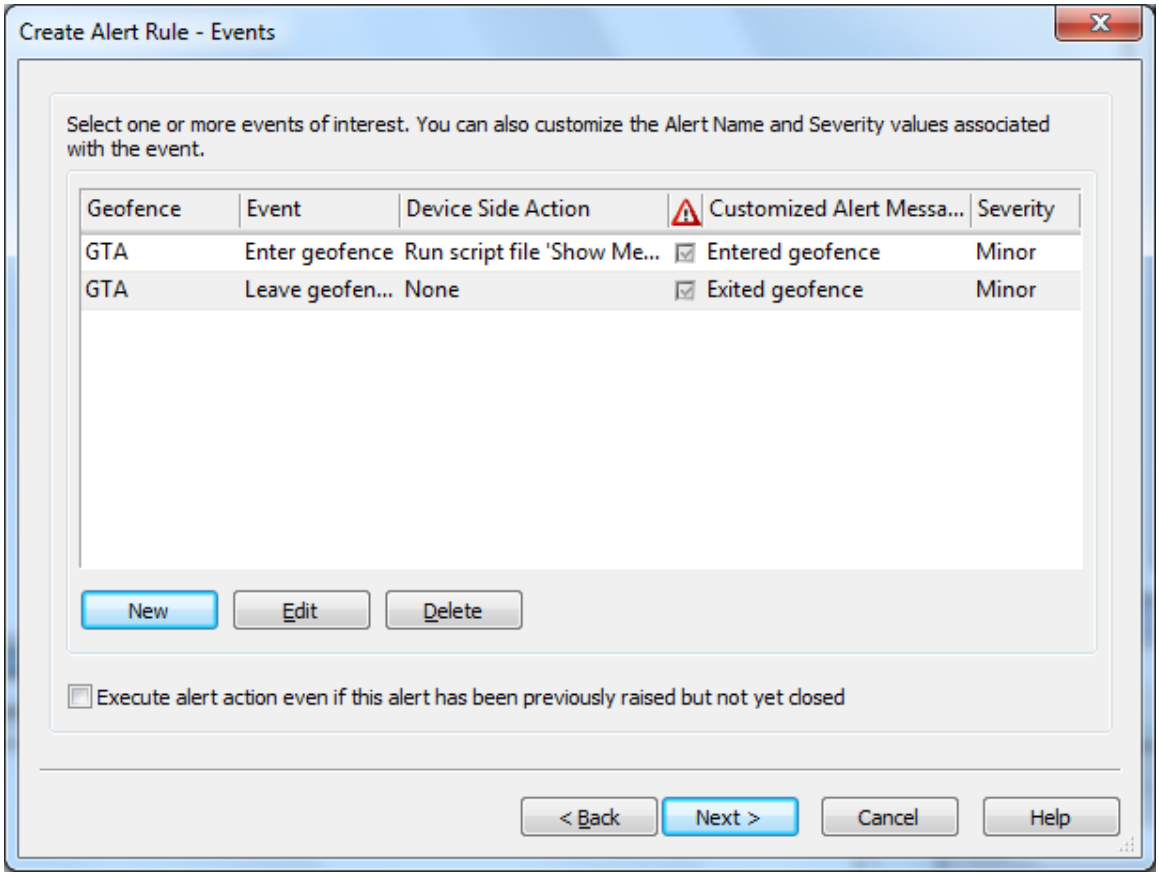
Alternatively to identify the appropriate view of the map, you can click on **Go to Location** which will allow you to specify a street address, location, landmark, or an existing geofence.

EXAMPLE:

- 350 Fifth Avenue, New York City
- Rome
- SFO (San Francisco International Airport)

Once you have the appropriate view displayed, you can click on Start Drawing and you are now able to create a fence. The first click of the mouse is first point of the fence. In order to complete the fence, you must have at least 3 distinct points selected on the map. In order to complete your fence, the last point must end off at the first point so it completes the closure of the fence. Once the last point is selected, a pop-up requesting the name of the geofence is shown. Here you should enter a meaningful name for that specific geofence in case you would like to use it again.

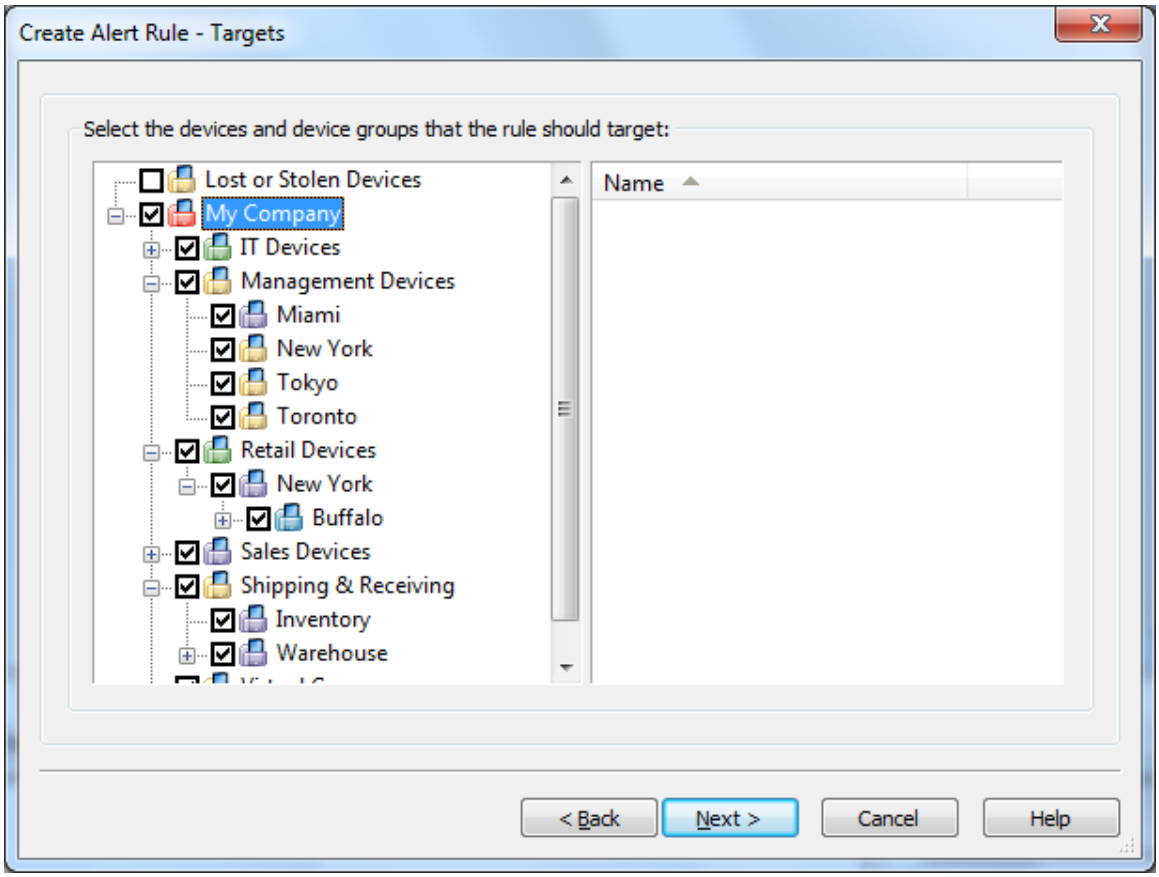
Select Geofence



Once the event is configured it will display as shown in the above diagram. Here you have the ability to create new events, edit existing events or delete events. Also, on this dialog box, there is a checkbox at the bottom allowing you to determine whether or not you want to Execute alert action even if this alert has been previously raised but not yet closed.

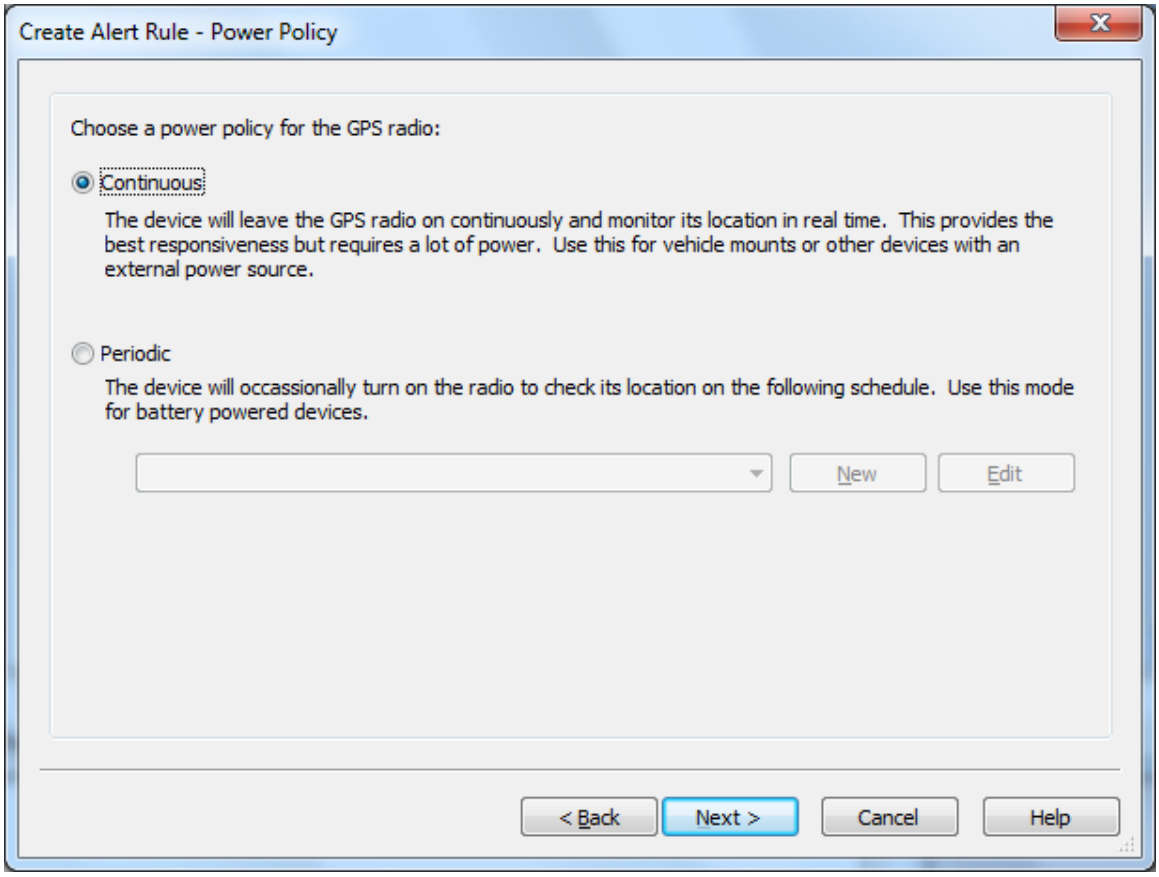
Select Devices

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



Select Power Policy

Clicking Next moves you to the Power Policy section as seen below.



The options available for the Power Policy are Continuous and Periodic.

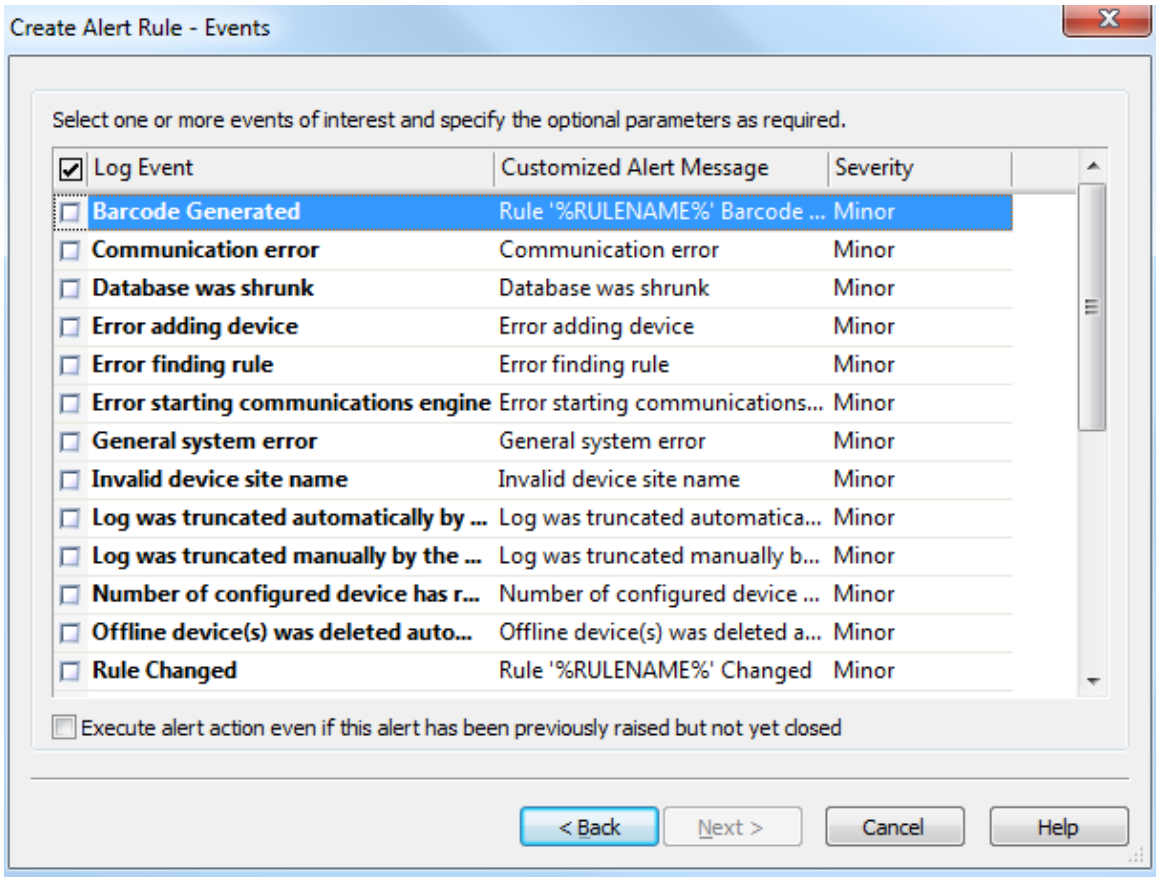
Continuous indicates the GPS radio is always on and the location will be monitored in real time. It is best to use this option with devices that have an external power source or are vehicle mounted because this option takes up a lot more power.

Periodic will turn on the radio based on a schedule that you define. Based on your business requirements, this can be as responsive as every 2 minutes, or every weekday all the way up to every year. It is best to use this option when you have battery powered devices in order to minimize the amount of power consumed with having this feature on.

After selecting your power policy, click Next and continue the Alert Rule Wizard here.

System Event

A System Event is an alert triggered based on an assortment of system events. See below for a full list.



System Event Notification Selection Window

Severity is set to Minor by default and can be altered.
The below table shows all available default System events:

Log Event	**Alert Message (Customisable)**
Site name changed	Site name changed
Log was truncated automatically by the Deployment Server	Log was truncated automatically by the Deployment Server
Manager has different time with deployment server	Manager has different time with deployment server
Log was truncated manually by the user	Log was truncated manually by the user
Database was shrunk	Database was shrunk
Number of configured device has reach licensed number	Number of configured device has reach licensed number
Invalid device site name	Invalid device site name
Error starting communications engine	Error starting communications engine
Attempting to upgrade database	Attempting to upgrade database

Log Event	Alert Message (Customisable)
Database upgrade completed	Database upgrade completed
Error finding rule	Error finding rule
Error adding device	Error adding device
General system error	General system error
Communication error	Communication error
Rule Created	Rule '%RULENAME%' Created
Rule Enabled	Rule '%RULENAME%' Enabled
Rule Disabled	Rule '%RULENAME%' Disabled
Rule Renamed	Rule '%RULENAME%' Renamed
Rule Changed	Rule '%RULENAME%' Changed
Rule Deleted	Rule '%RULENAME%' Deleted

The following list of variables are only available within the Customized Alert Message field:

Type	Description
%RULENAME%	The name of the rule
%PACKAGENAME%	The name of the package

After selecting your System Events, click Next and continue the Alert Rule Wizard here.

SMTP Notification Profile

When you configure an alert, you have the ability to get notified by sending an email to a user or users indicating the particular event. A **Notification Profile** allows you to configure the sending email server settings as well as the contents of the message.

From the Manage Profiles dialog, you have the ability to select an existing profile, create a new profile, edit or delete an already existing profile.

If no email notification profile exists, you'll need to specify a Profile Name, the SMTP Host, Port, and give the option of different levels of Authentication within the Create Notification Profile dialog. You have the option of having an Anonymous, basic, or NTLM authentication and the ability to enable the use of SSL.

The Sender dialog allows you to specify details of the email address that will be sending the notification. You must also specify a name for that sender which gets displayed in the From field. Optionally, you have the ability to setup a Priority for the email where the available options are Low, Medium and High.

Select the Recipients that should be notified when the particular alert event is triggered. When you click the Add button, you have the ability to setup recipients that would be in the To field, CC field and BCC field as well.

The **Message** dialog allows you to specify both the Subject and the Message. Variables can be added to both the Subject and the Message as shown in the screen shot above. The entire list of variables that can be used are described below:

Variable	Description
%%ALERT%	Displays the Alert name that was specified when the alert was created.
%SOURCE%	Display the Deployment Server name in the case it is a Deployment Server alert. Displays the “MobiControl System” in case it is a System alert. Displays the Device name in case it is a Custom Data alert. Displays the Device name in case it is a Device alert. Displays the Device name in case it is a Geofence alert.
%LOCATION%	Displays the Deployment Server name in the case it is a Deployment Server alert. Displays the “MobiControl System” in case it is a System alert. Displays the location in case it is a Custom Data alert. Displays the location in case it is a Device alert. Displays the location in case it is a Geofence alert.
%DATE%	Displays the date the alert was generated.
%TIME%	Displays the time the alert was generated.

The Create Notification Profile - Summary Information page summarizes the settings configured on the previous pages of the wizard. If you are satisfied with the configured settings, click on the Finish button to create the Create Notification Profile, otherwise use the Back button to go to previous screens and make adjustments. The Test button will send a test email to the recipients to ensure the settings are correct.

After completing the Notification Profile Wizard, click Finish and continue the Alert Rule Wizard here.

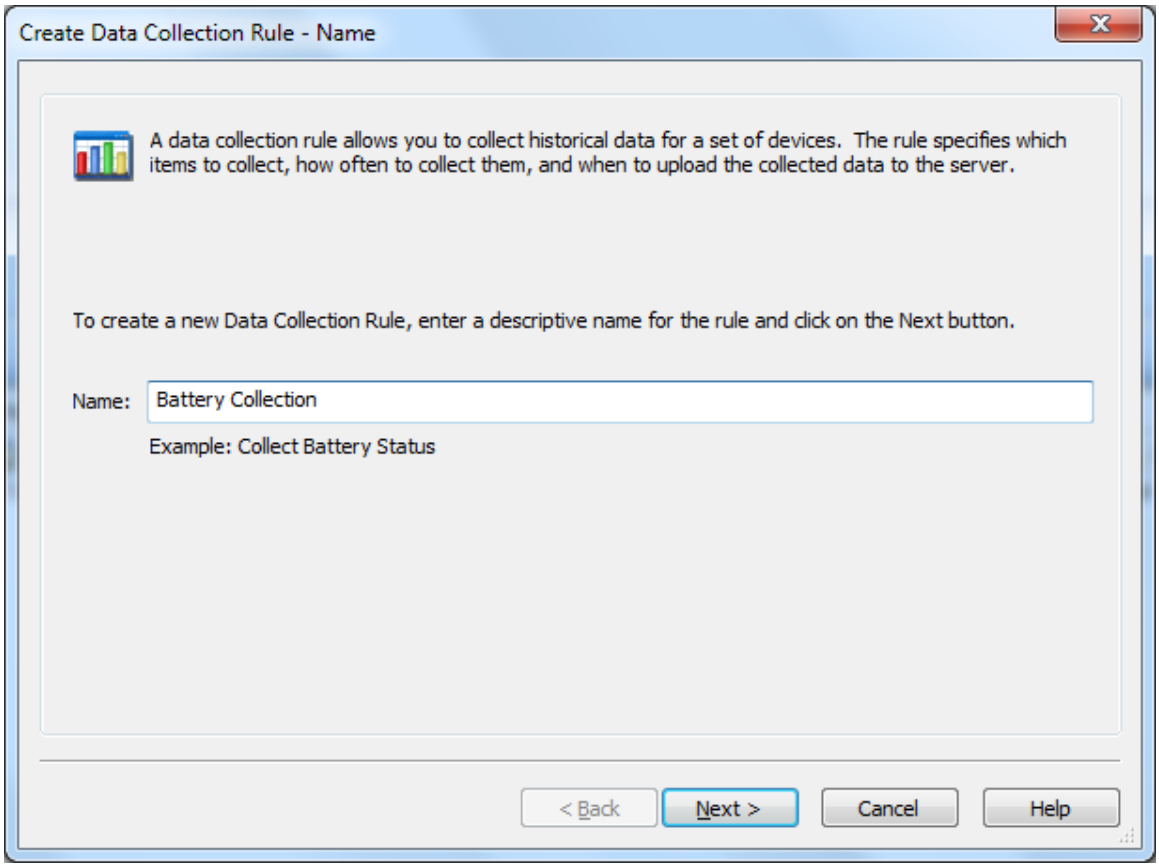
Creating Data Collection Rules

Data collection rules allow administrators to automatically collect a variety of data from mobile device(s).

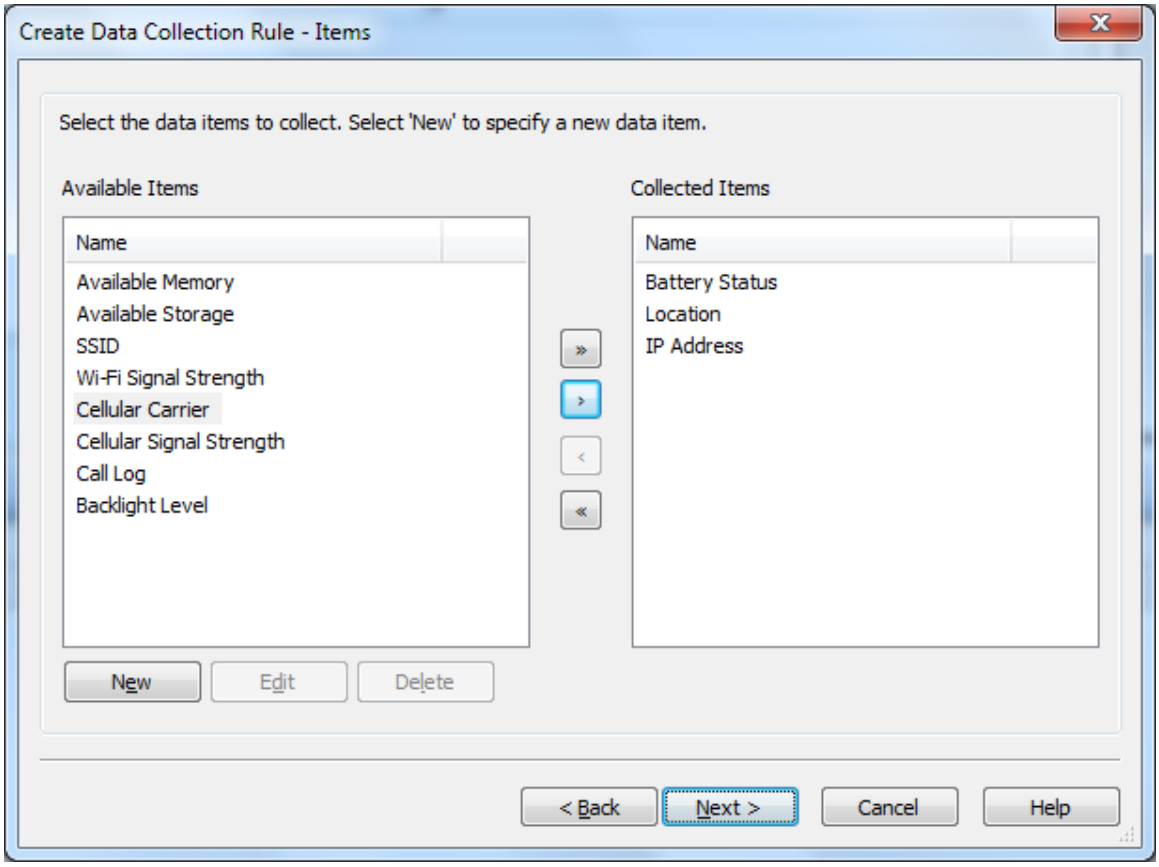
The following series of steps describes how to use the Create Data Collection Rule Wizard to create a data collection rule:

1. Start the wizard.

   From MobiControl Manager, select the Rules view (tab), then click **Rule,** click **Create Rule,** and click **Data Collection Rule**. Enter a meaningful name for your new data collection rule and then click **Next**.



2. Select data items to collect.



Select individual items or all items from the **Available Items** list by highlighting and then select the corresponding direction arrow(s). These items will move to the **Collected Items** list. If you have added something that you would like to remove from the **Collected Items** list, simply select the

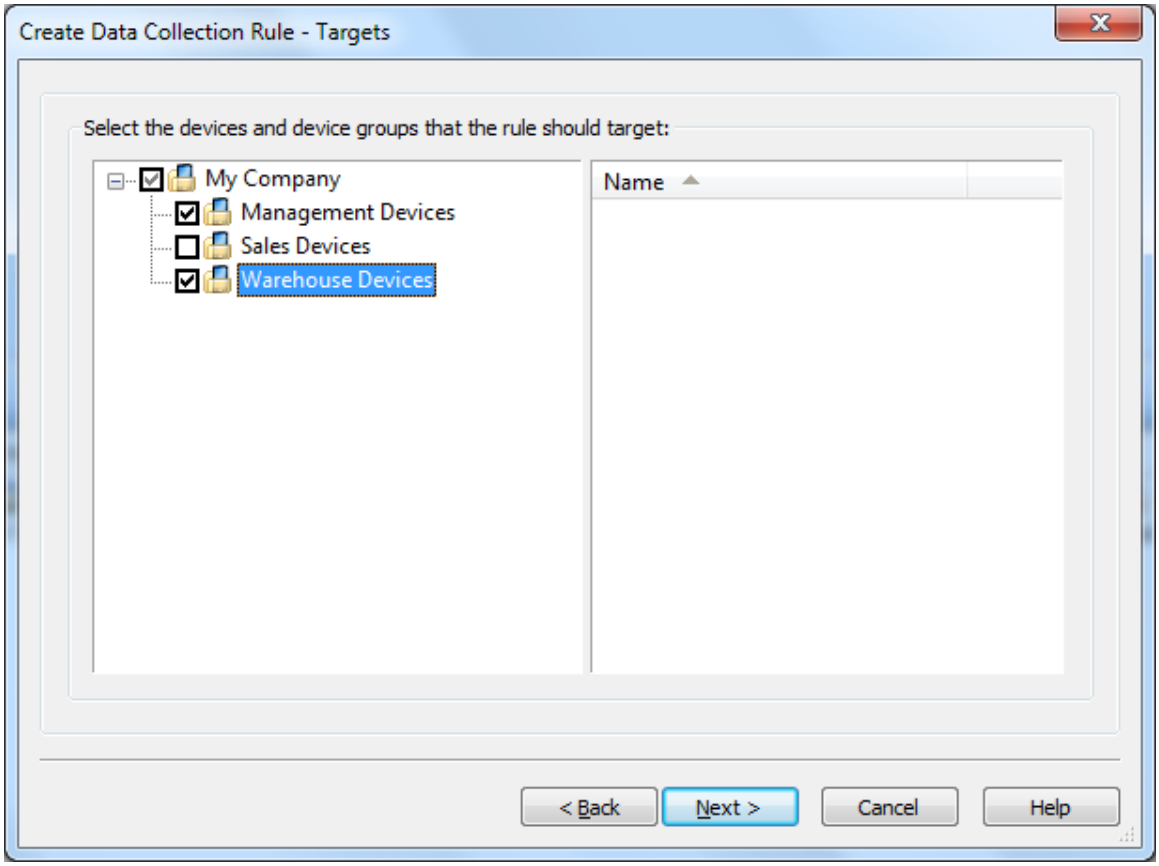
item and then click the direction arrow(s) to place the item(s) back into the **Available Items** list.

Item Name	Description
Available Memory	Shows the collected data is the combination of device memory, storage memory and virtual memory on the device
Available Storage	Shows the amount of room that is left on the main memory of the device
Battery Status	Shows what percent the battery was at the time the data collection rule ran
Call Log	Shows the incoming, outgoing and missed calls with call duration
Cellular Carrier	Shows what carrier the device is connected to at the time the data collection rule ran
Cellular Signal Strength	Shows what the signal strength is of the device at the time the data collection rule ran
IP Address	Shows the IP address of the device at the time the data collection rule ran
Location	Shows the GPS latitude, longitude, speed and heading
SSID	Shows the SSID that your device is currently connected to
Wi-Fi Signal Strength	Shows the signal strength of a wireless connection. A value of 0 is collected when there is no Signal listed in Manager

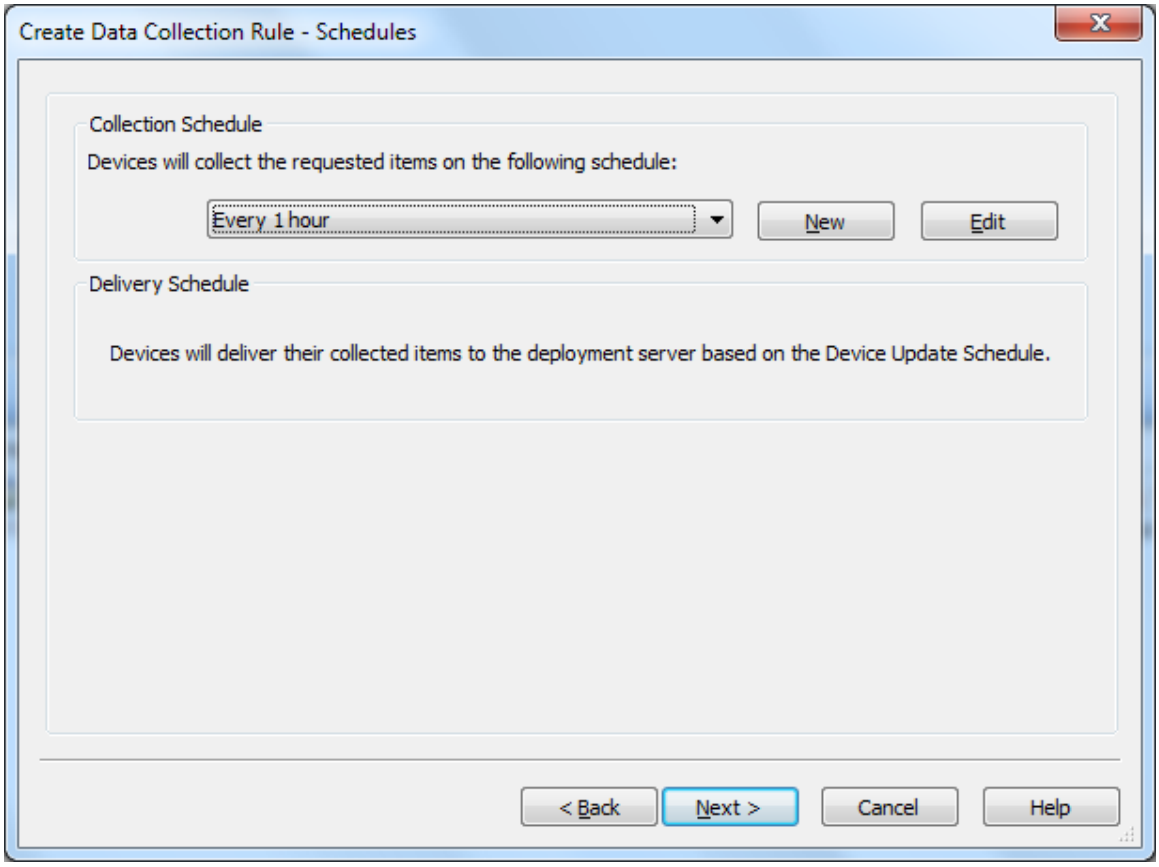
After selecting the choice(s), click the **Next** button.

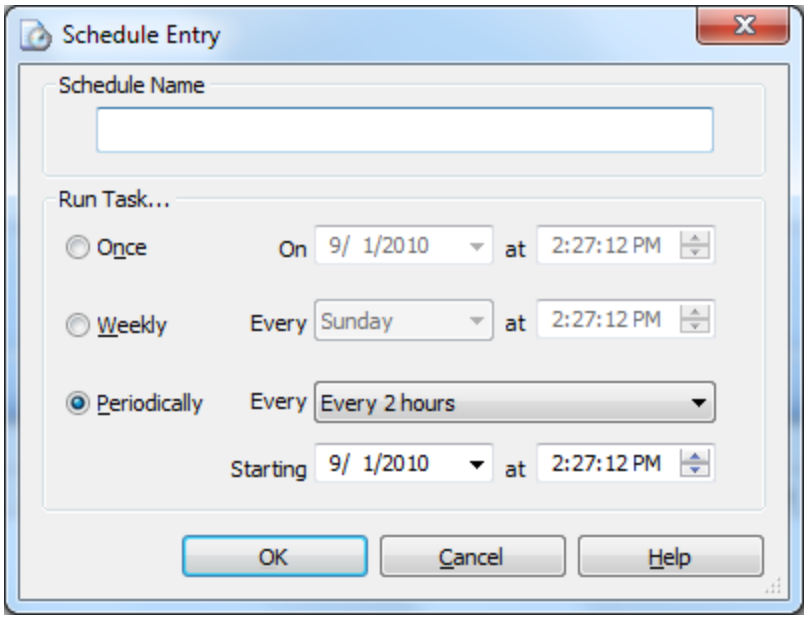
3. Select devices.

   Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



4. Configure data collection rule schedule and optional settings.





Section Name	Description
Collection Schedule	This option enables you to create a custom data collection schedule with a custom date and time. Select the **New** button to create the new schedule. This will open up the second dialog box above. If you already have a previously created schedule, you can select edit to open the second dialog box above.
Schedule Name	Enter a meaningful schedule name that will be used to identify your custom schedule(s).
Run Task	Select the frequency for which you want to initiate the data collection on your device (s).
Delivery Schedule	This option will deliver the data collected from the device to the Deployment Serverbased upon the set update schedule. Currently, this option uses device schedule as the delivery schedule and is not configurable.

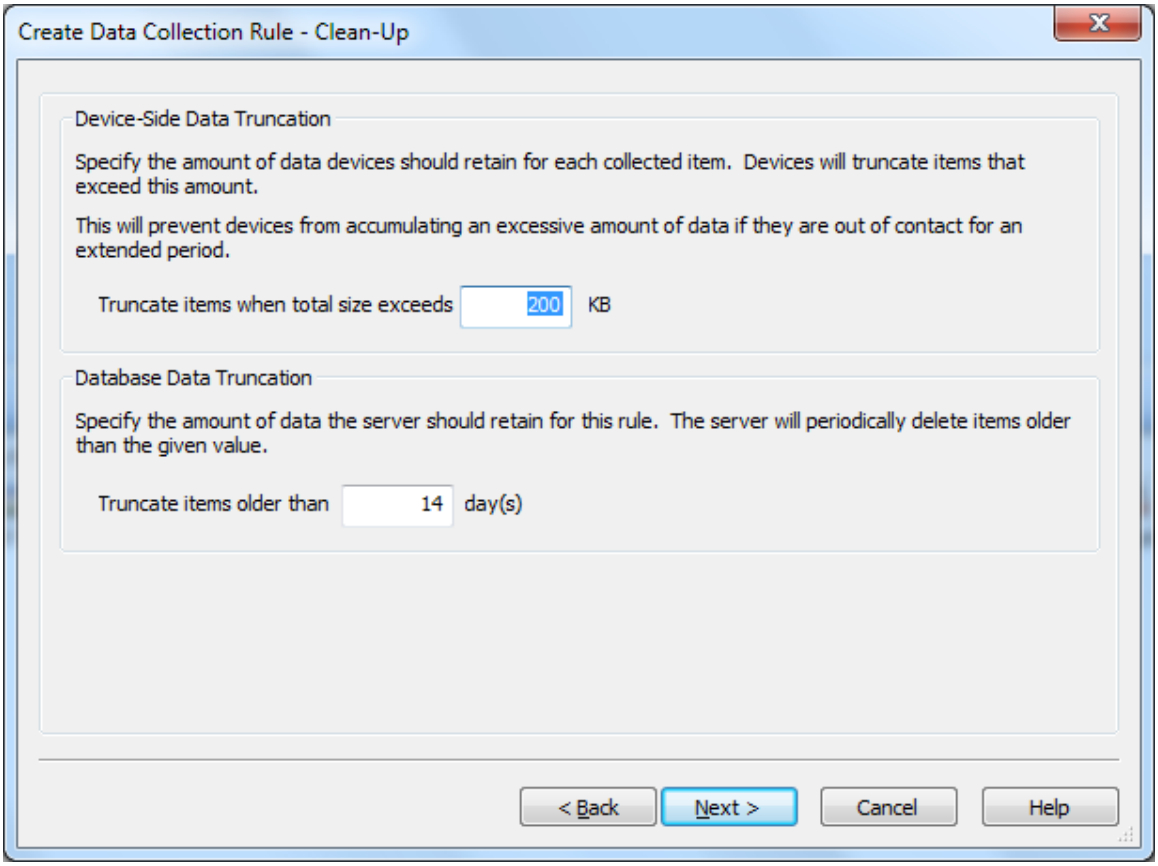
NOTE:

Creating a frequent collection schedule may affect the device's battery life. Also, frequent data collection can be managed with the truncation options available. This will help control how much data is kept on the device and in the database.

After entering your choice(s) in the above dialog box, click the **Next** button.

5. Configure data truncation settings.

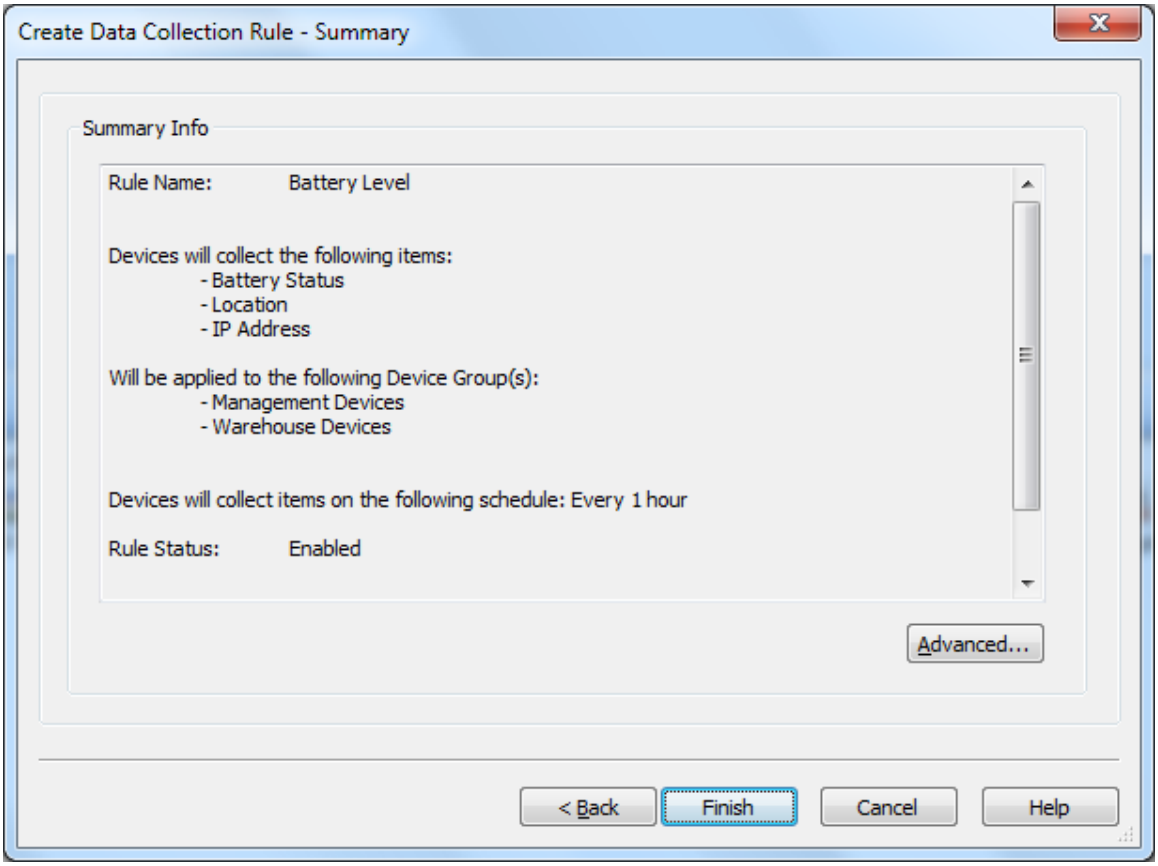
   Choose the size of the data being collected. This helps control memory used on the device and the number of days you would like to retain the data in the database.



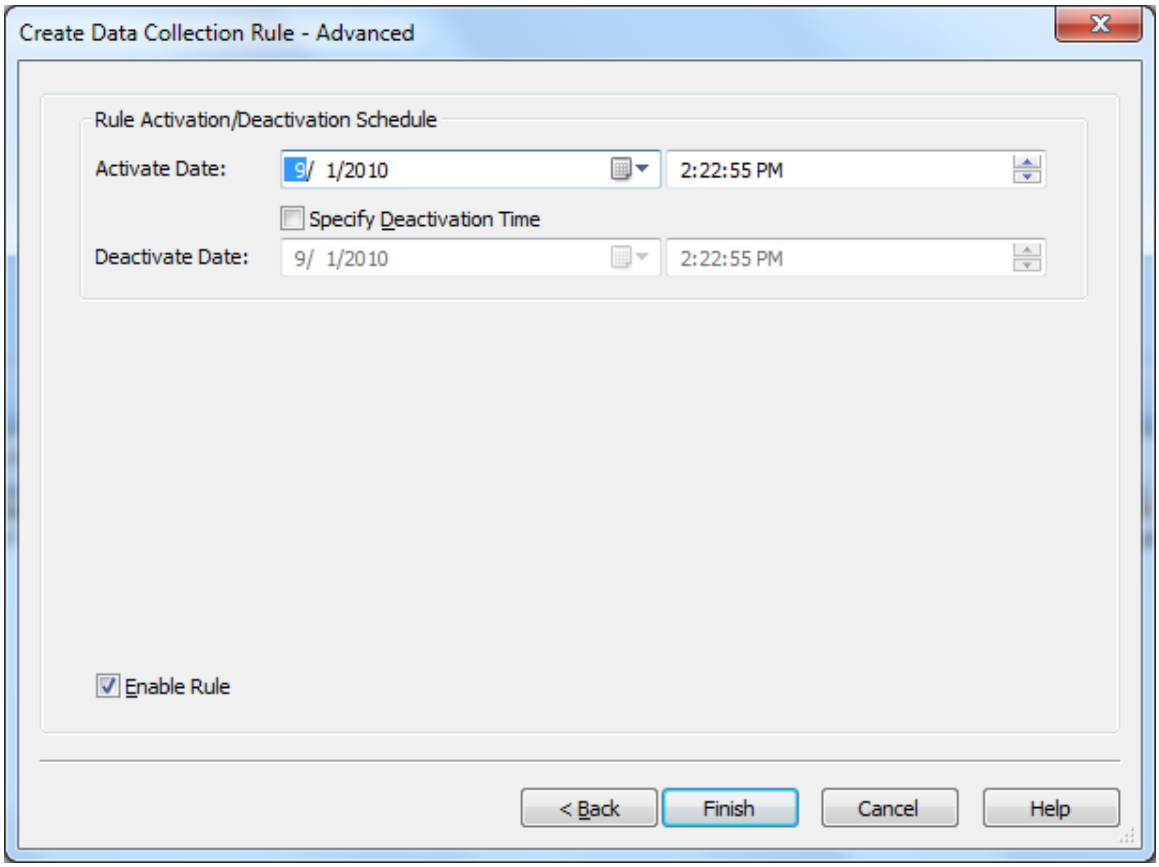
Section Name	Description
Device-Side Data Truncation	Specify the maximum size of data to be stored from the data collection ruleon the device(s).
Database Data Truncation	Specify the number of day(s) that you would like to retain the information in your database. Data collected older than the number of days listed will be deleted from the database

After entering your choice(s) in the above dialog box, click the **Next** button.

6. Review the summarized information.



By clicking on the Advanced button, the data collection rule Advanced window will appear. By default the rule will be activated immediately upon completion of the wizard. If you wish to delay the activation, you can modify the activate date. A deactivate date can optionally be entered to specify a date from which the rule will be disabled. A data collection rule can also be explicitly disabled by clearing the checkbox next to Enable Rule.



Section Name	Description
Activate Date	This option enables you to define a date and time when the rule will start collecting data from the selected devices
Deactivate Date	If the **Specify Deactivation time** box is checked, you can define the time at which you wish the data collection to stop.
Enable Rule	You can use this option to enable or disable the rule. This option is also available by right-clicking the rule.

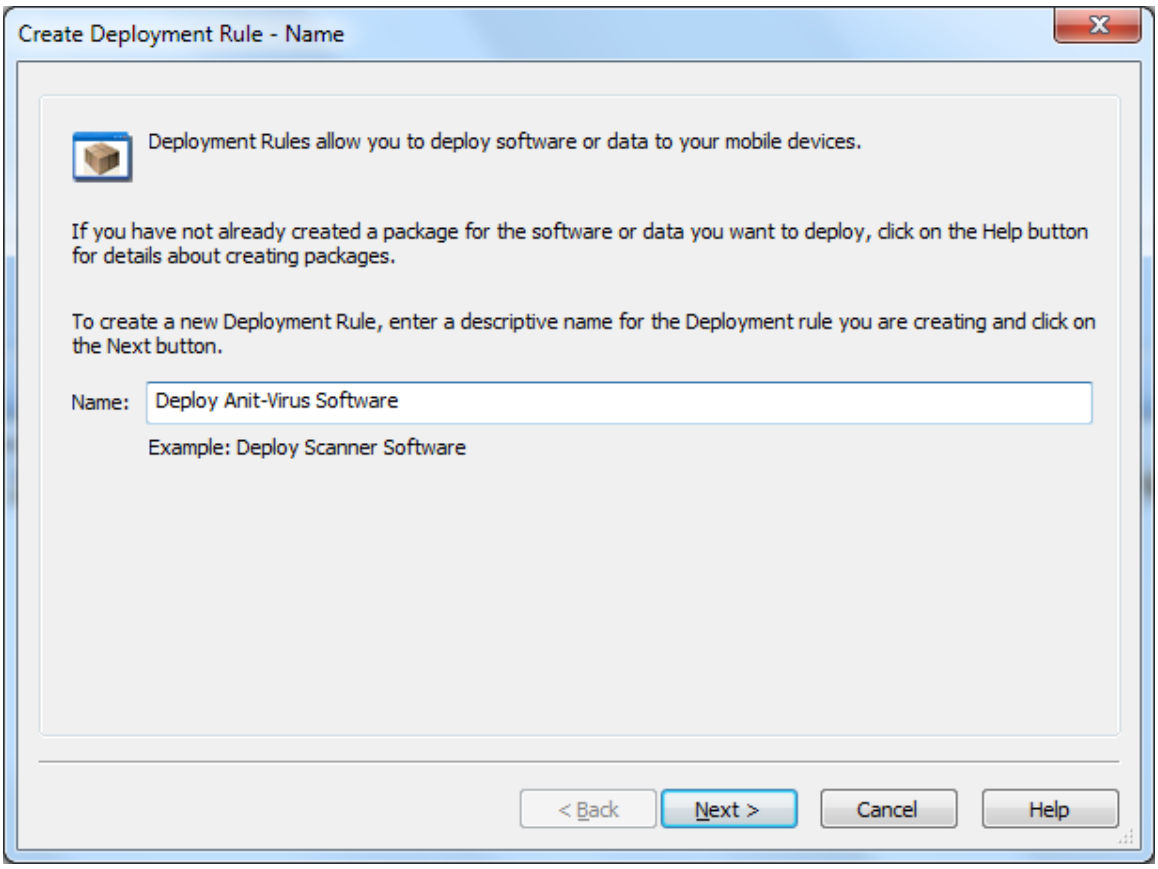
The data collection rule can be deployed real-time or at a pre-set time. The data collection rule, although set to be activated at a scheduled time, can also be set to be deactivated. The deactivation setting is optional.

Click **Finish** to complete the wizard.

Creating Deployment Rules

Deployment rules allow administrators to automatically provision mobile devices with packages that contain software or data. The following series of steps describes how to use the Create Deployment Rule Wizard to create a deployment rule.

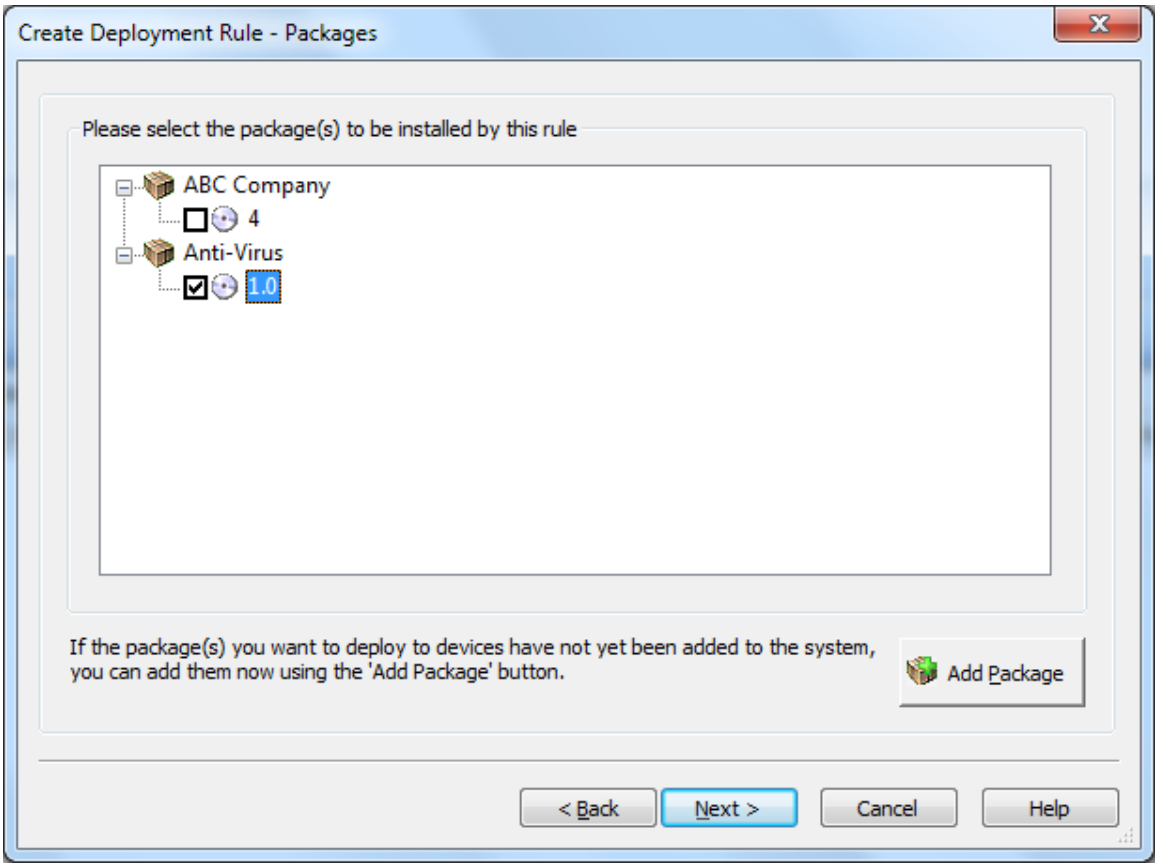
1. Start the wizard.



First page of the Create Deployment Rule Wizard

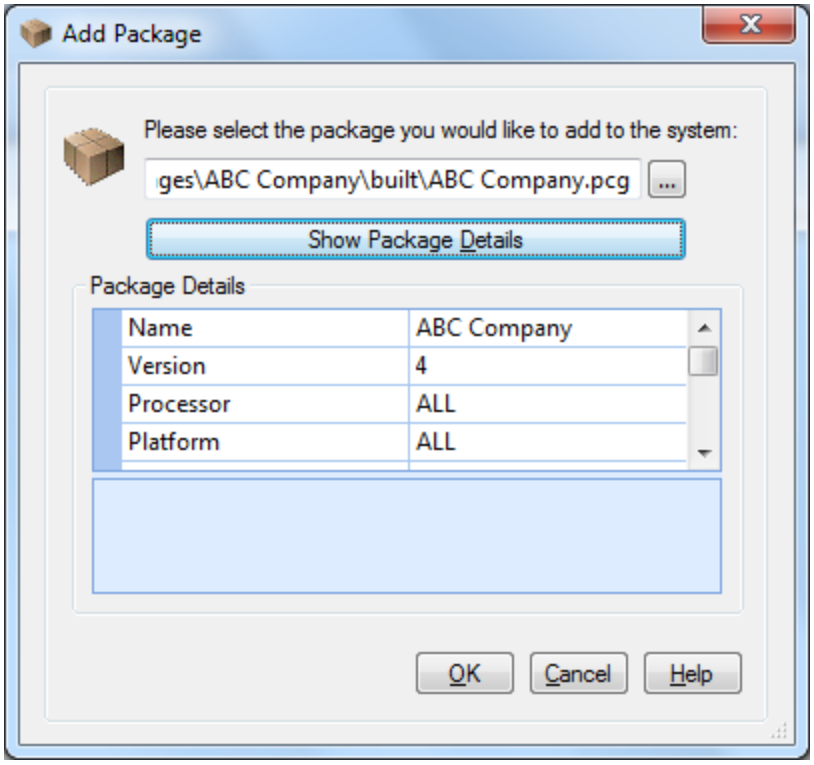
From MobiControl Manager select the **Rules view (tab)**, then click the **Rule** menu, click **Create Rule**, and click **Deployment Rule**. The first page of the Create Deployment Rule Wizard will be displayed. Enter a descriptive name for the deployment rule you are creating and click **Next**.

2. Select the package(s) to be deployed.



Select Package page

The dialog box displays a list of the packages that have been previously loaded into the MobiControl database. Select the relevant packages that need to be installed by this rule.



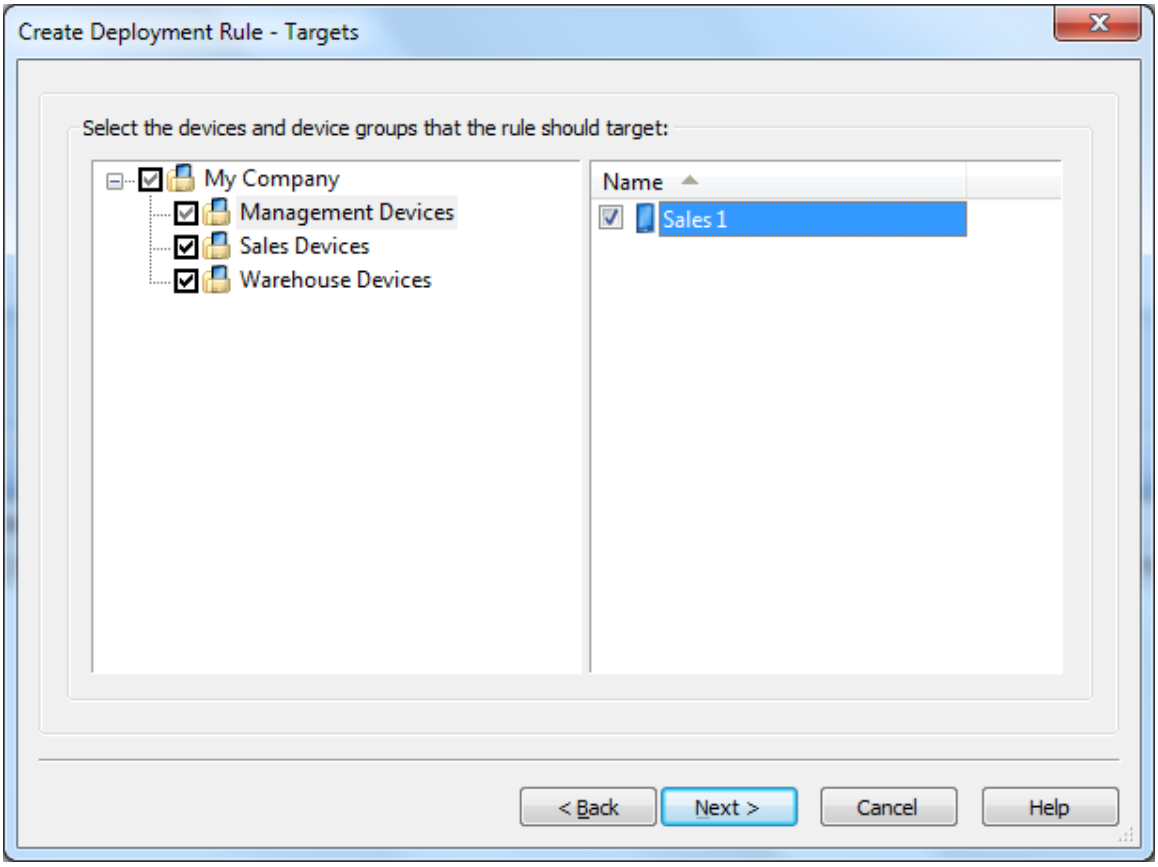
Add Package dialog

If the package to be installed has been created but not loaded into MobiControl, click the **Add Package** button and select the package file from the file system.

If the package has not yet been created, exit the wizard and use MobiControl Package Studio to create a package. (Please see the "MobiControl Package Studio" topic on page 413.)

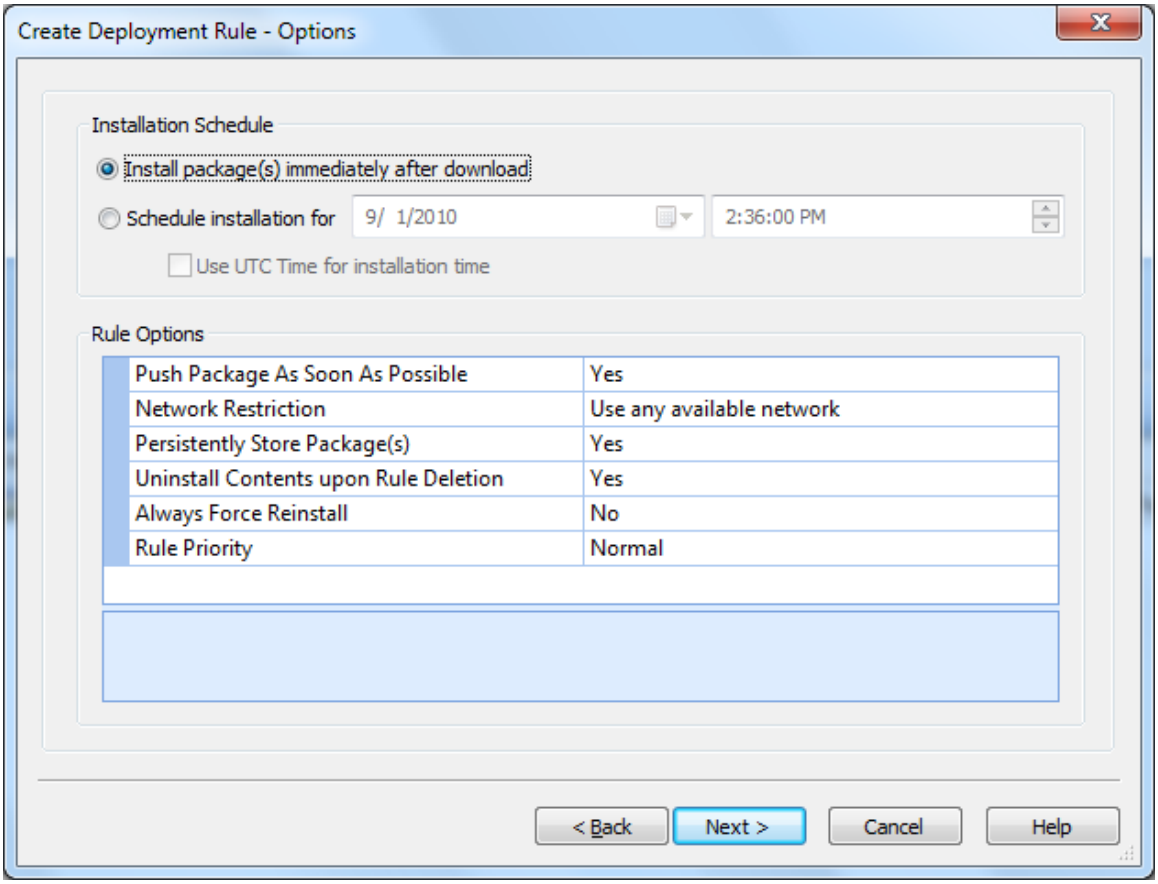
3. Select where the package(s) will be deployed.

   Select the device(s) or group(s) to which the package(s) will be deployed and click the **Next** button.



Device Group Selection page

4. Configure deployment rule activation schedule and optional settings.



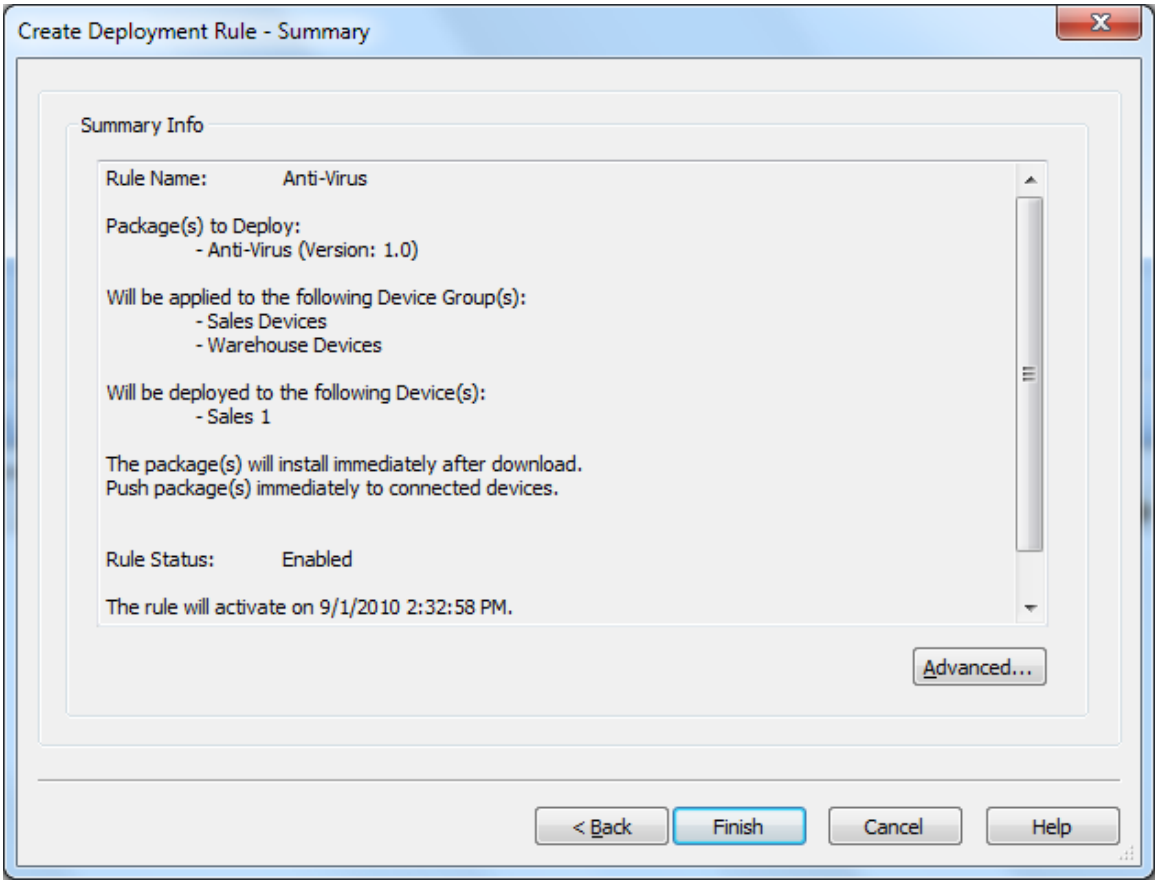
Device Settings Configuration page

The deployment rule can be deployed at real-time or at a pre-set time. The deployment rule, although set to be activated at a scheduled time, can also be set to be deactivated. The deactivation setting is optional.

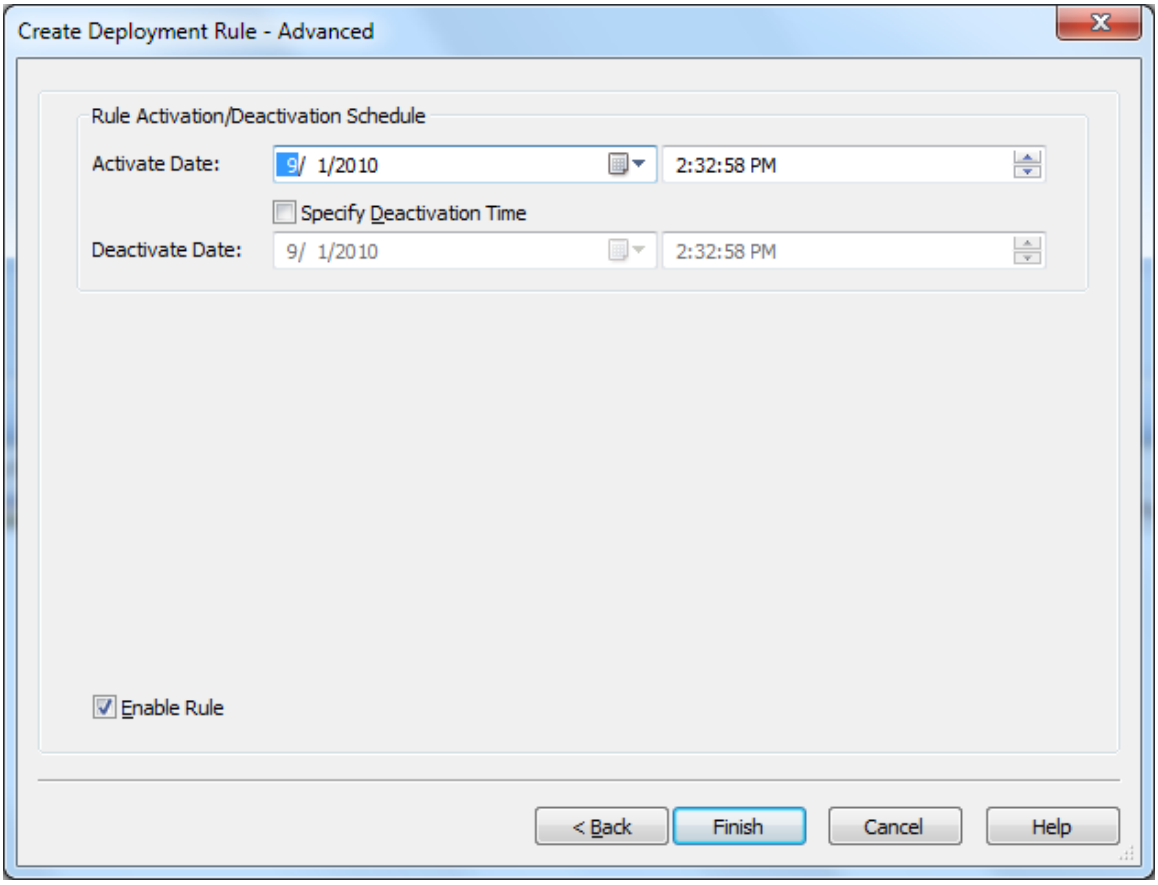
Field Name	Description
Install immediately after download	If this checkbox is cleared, the installation of a downloaded package will be delayed till the specified Installation Date. The Installation Date must be after the Activate Date. If a package depends on another package that is scheduled to install at a later time, then the Deployment Server will not push the package unless it is also scheduled to install at the same time or later. Please see the "Package Dependencies" topic on page 378.
Push Packages As Soon As Possible	By default, packages will be deployed to the devices according to the device synchronization schedule. The device synchronization schedule is specified by the add devices rule used to add the device to MobiControl. If this option is selected, package(s) will be deployed to the target devices immediately. If the devices are currently offline, the package(s) will be deployed as soon as the device connects to MobiControl.
Network Restriction	Restrict whether package deployment should take place over cellular data networks.
Persistently Store Package(s)	For devices with stable storage, persistently storing packages allows them to be reinstalled after a hard reset, without needing to connect to the Deployment Server.
Uninstall Contents upon Rule Deletion	This is relevant when the rule has been deleted or is no longer assigned to a device, for instance because it was moved to a new group or the rule was edited to target a different group. • If **Yes** is selected, the package will be removed from the device, and the uninstallation logic of the packages will be executed. • If **No** is selected, the package will be removed from the device, but no uninstallation logic will be executed. The uninstallation logic depends on what the package contains, for example, when a rule that deploys a package containing a `.cab` file is deleted. • If the **Uninstall Package(s) upon Rule Deletion** option is set to **Yes,** the application installed by the `.cab` file will be removed. • If the **Uninstall Package(s) upon Rule Deletion** option is set to **No**, the application installed by the `.cab` file will remain installed.
Always Force Reinstall	Packages will be reinstalled on to the device regardless of whether they are already installed.
Rule Priority	This option allows you to prioritize the deployment of the package(s). Package dependencies (introduced in version 3.06) are the recommended means to ensure the order in which packages are installed on the devices. Please see the "Package Dependencies" topic on page 378 for more information.
Enable Rule	If you wish to activate the rule, that is, to install the package(s), then this field needs to be checked. This option is also made available by right-clicking the rule in the Rules view (tab). When you disable a deployment rule, MobiControl will attempt to uninstall the packages that were being deployed by that rule. If the package(s) that were being deployed contained `.cab` files, MobiControl will try to uninstall the `.cab` files as well.

5. Review the summarized information.

   A **summary** of the deployment rule is displayed. Review the settings you have chosen and click **Finish** to complete the wizard.



Summary page



Advanced page

Field Name	Description
Activate Date	The date and time when the package will be deployed or downloaded to the device from the Deployment Servers view (tab)
Deactivate Date	The **Specify Deactivation Time** checkbox allows a time to be specified when deployment of the package should stop.

NOTE:

After five unsuccessful attempts to deploy the package, deployment to that device is temporarily deferred. In order to start deployment of that package again, you must right-click the package from the Package panel and select **Force Re-install**.

Creating Device Relocation Rules

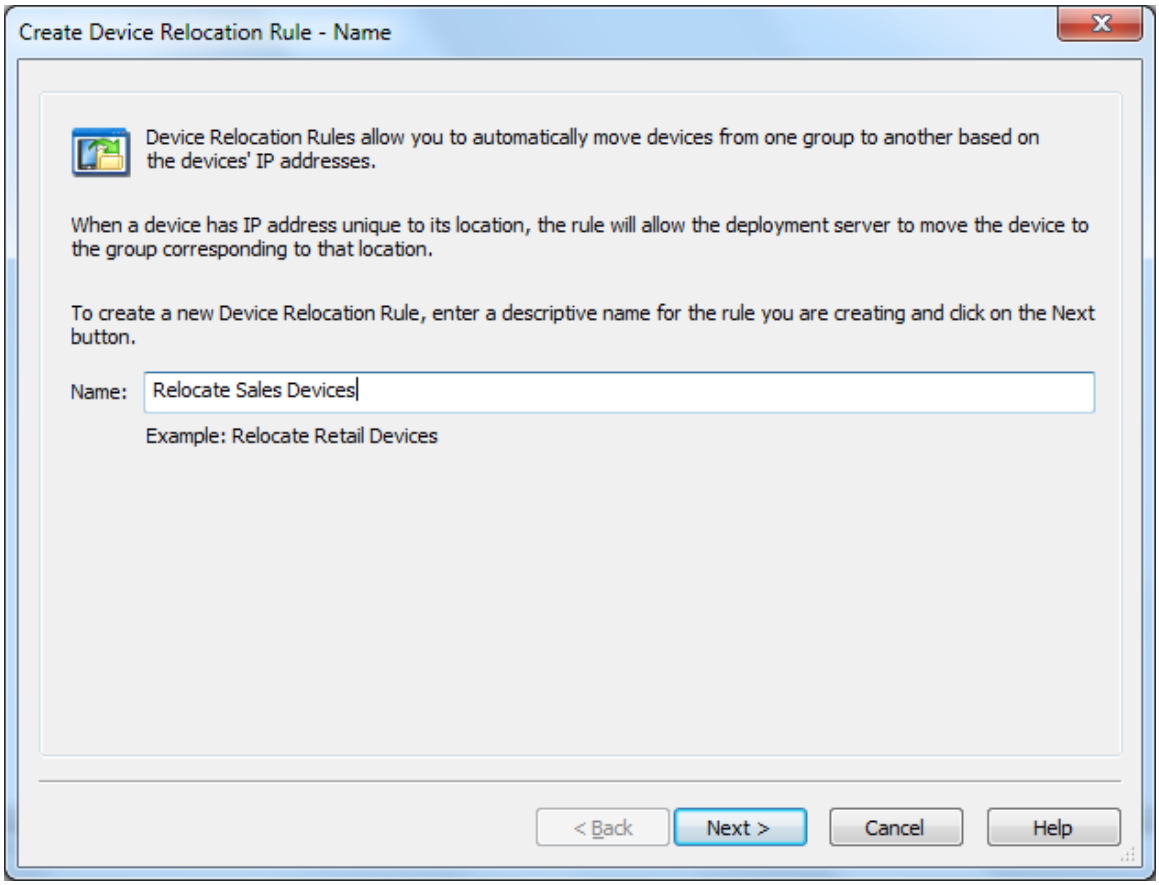
Dynamic device relocation allows you to set up rules to move your mobile devices automatically between different virtual groups or device groups in the MobiControl device tree based on the IP address or other custom criteria. This is useful when managing mobile devices in a deployment where the device tree is set up to represent different physical locations (e.g. retail stores, warehouses, regional offices, etc.).

In a deployment that has mobile devices connecting from and moving frequently between several different sites, properties or regions, the administrator needs visibility over the movement of mobile devices across different locations. Dynamic device relocation allows the MobiControl device tree to be updated automatically when a device moves to a different location (e.g. a mobile device that has moved from a warehouse or site in Chicago to a site in New York will automatically be relocated in the device tree on reconnection and will appear in the device group for devices in New York based on the new IP address information). Additionally, the devices can also be automatically reconfigured and any modifications to the mobile device settings, specific to the new location, will be sent to the device automatically.

The devices are relocated based on the IP address ranges specified for each location. You can also create a custom data identifier which can be the criterion that will be utilized to relocate the devices to the appropriate device group. (Please see the "Custom Data" topic on page 175 for detailed information on custom data identifiers.)

1. Start the wizard.

   From MobiControl Manager, select the Rules view (tab), then click **Rule,** select **Create Rule,** and click **Create Device Relocation Rule.** The first page of the Create Device Relocation Rule Wizard will be displayed. Enter a meaningful name for the rule and click **Next** to continue.



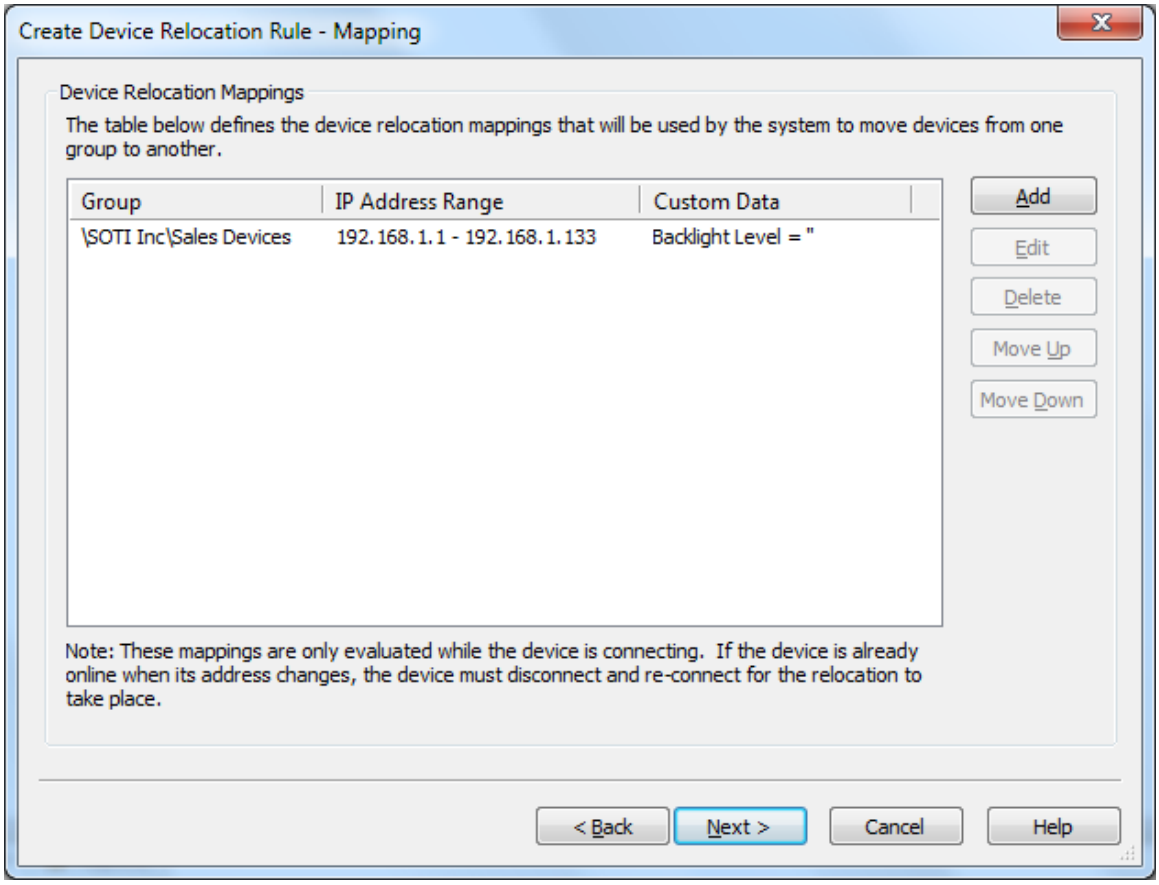
Create Device Relocation Rule Wizard startup dialog box

2. Review the device relocation mappings.

This page lists **device relocation mappings** that determine how the devices would be relocated and in which groups they would appear if the specified criteria is met. When a device connects to the MobiControl Deployment Server, its IP address and custom data information will be checked against all device relocation rules configured, and it will be moved to the appropriate device group based on the information in the relocation mappings.

NOTE:

Devices that are already connected and online in MobiControl will be relocated when they disconnect and re-connect to the MobiControl Deployment Server.

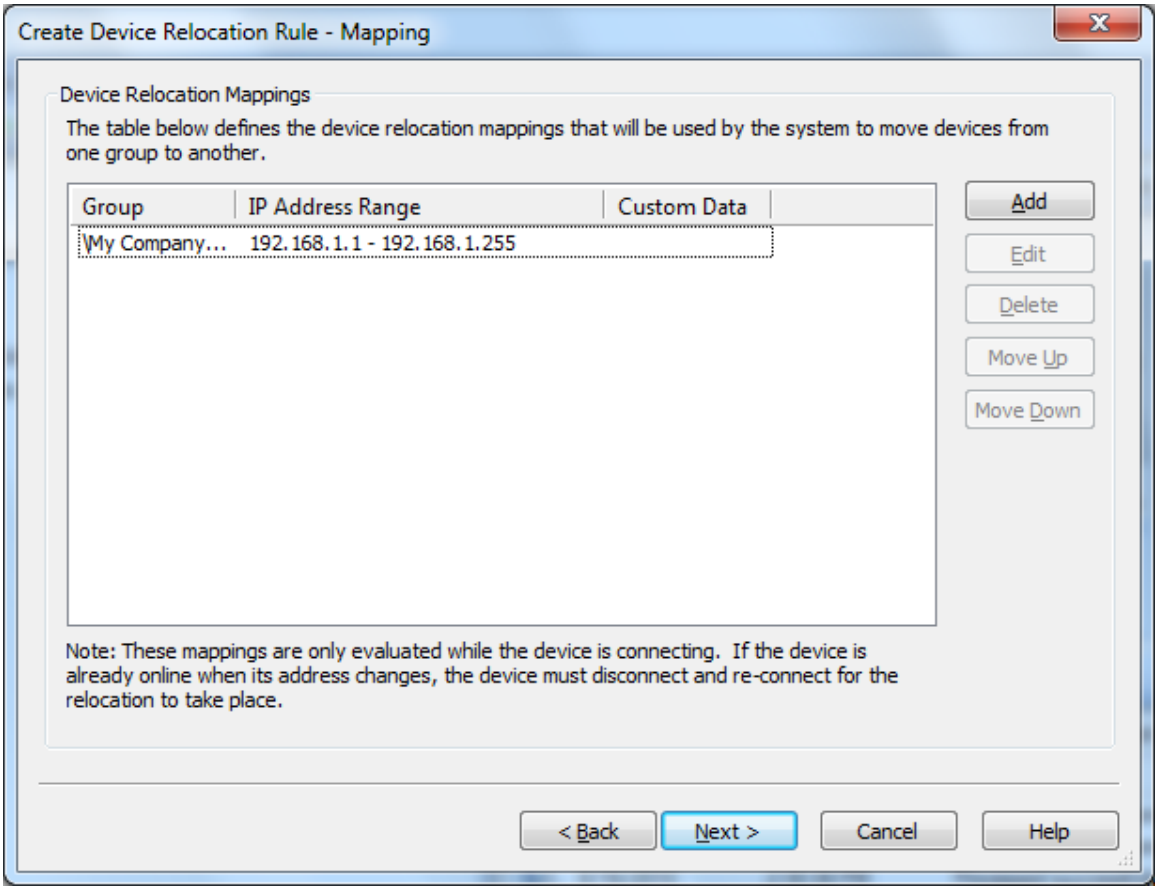


Edit Device Relocation Rule dialog box

The buttons on the **Edit Device Relocation Rule** dialog box are explained below:

Button Name	Description
Add	Click the **Add** button to add an entry for the relocation mapping.
Edit	Click the **Edit** button to change the settings for an existing relocation mapping entry.
Delete	Click the **Delete** button to delete a relocation mapping entry.
Move Up / Move Down	Click these buttons to change the order of the relocation mappings. The entry listed higher in the list have a higher priority and take precedence over entries listed lower in the list. For more details, read about relocation mappings priority below.

A relocation mapping can use just the IP address or the custom data entry to specify the relocation rule for mobile devices. If a relocation mapping has both the IP address and custom data entry specified as the criteria, the mobile devices would be relocated only if both these conditions are satisfied. If a device is affected by more than one relocation mapping, the one higher in the list of mappings will have a higher priority and will be effective. You can use the **Move Up** and **Move Down** buttons to change the precedence of the relocation mappings if multiple mappings apply to a device.

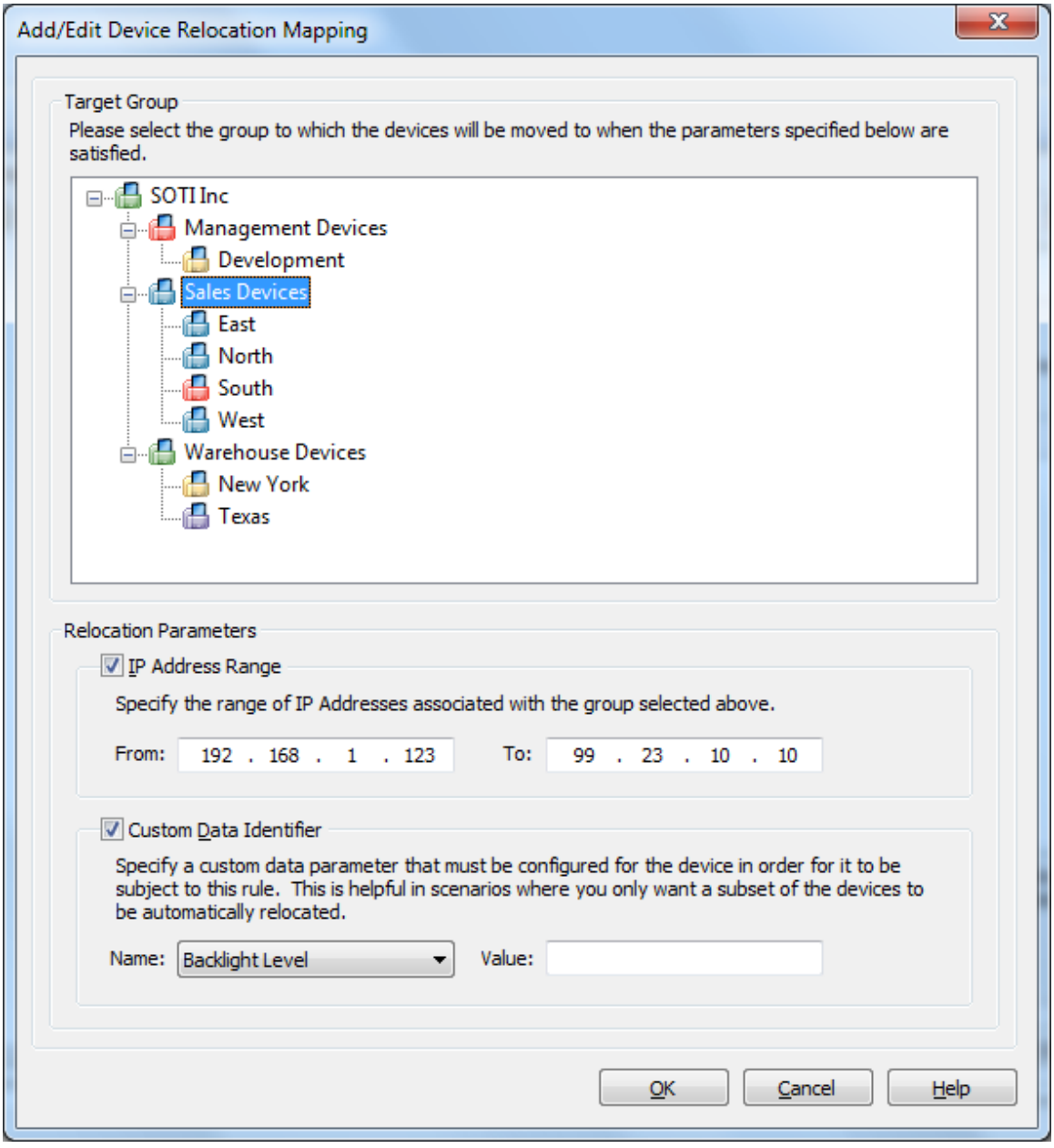


Device Relocation Mappings dialog box

The first two relocation mappings in the previous screenshot have been defined: one is for relocating all devices with IP addresses between 192.168.1.1 and 192.168.1.255 to the Management Devices group and another mapping for relocating all the devices for which the custom data item "Location" has a value of "Region A" to the Warehouses group. Since the relocation mapping with the IP address filter is listed above the mapping with the custom data filter, the IP address mapping will take precedence. If a device satisfies both conditions (e.g. has an IP address 192.168.1.10 and a value "Region A" for "Location"), it will be relocated to the Management Devices group.

3. Add or edit device relocation mappings.

A relocation mapping includes the target or destination group (which can be a virtual group) to which the devices would be relocated. It also includes the conditions or the relocation parameters that must be satisfied for a device to be relocated.



Add/Edit Device Relocation Mapping dialog box

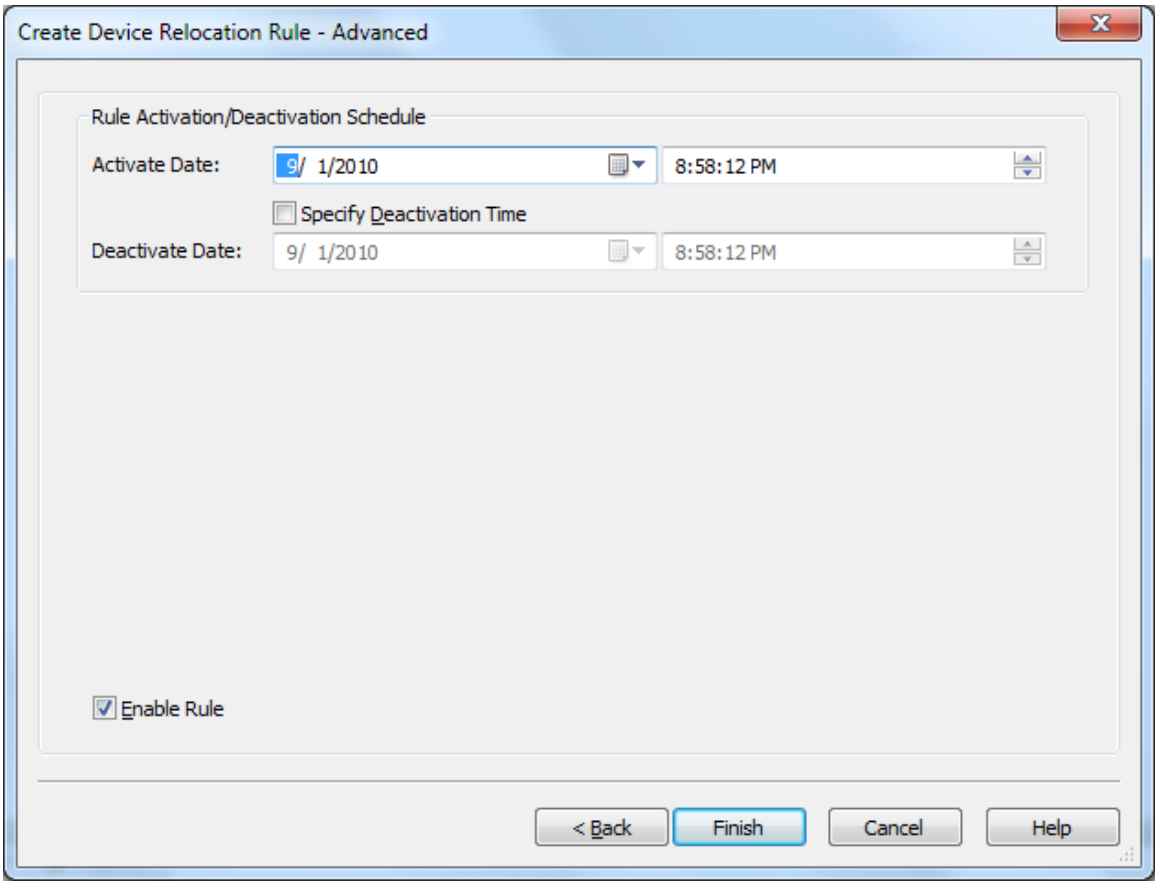
The **target group** is the group, sub-group, or virtual group to which devices will automatically be relocated when connecting to the Deployment Server if the conditions specified in the relocation parameters are met.

Multiple **relocation parameters** can be specified to manage the dynamic relocation of devices. A single parameter can be specified or both parameters can be used for a relocation mapping, in which case the device will be relocated if it satisfies both parameters.

The following table describes the fields of the **Add/Edit Device Relocation Mapping** dialog box:

Field Name	Description
IP Address Range	Devices can be automatically relocated based on the IP address information of the device at the time it connects to a Deployment Server. A range of IP addresses can be specified and if the device's IP is within that range, the device will be relocated to the target group.
Custom Data Identifier	You can use a custom data value as one of the criteria for relocating devices from one device group to another. MobiControl allows you to retrieve arbitrary data from the device's registry, files on the device and other sources using custom data. Please see the "Custom Data" topic on page 175 for more information.

4. Specify the rule activation or deactivation schedule.



Edit Device Relocation Rule Activation/Deactivation Schedule dialog box

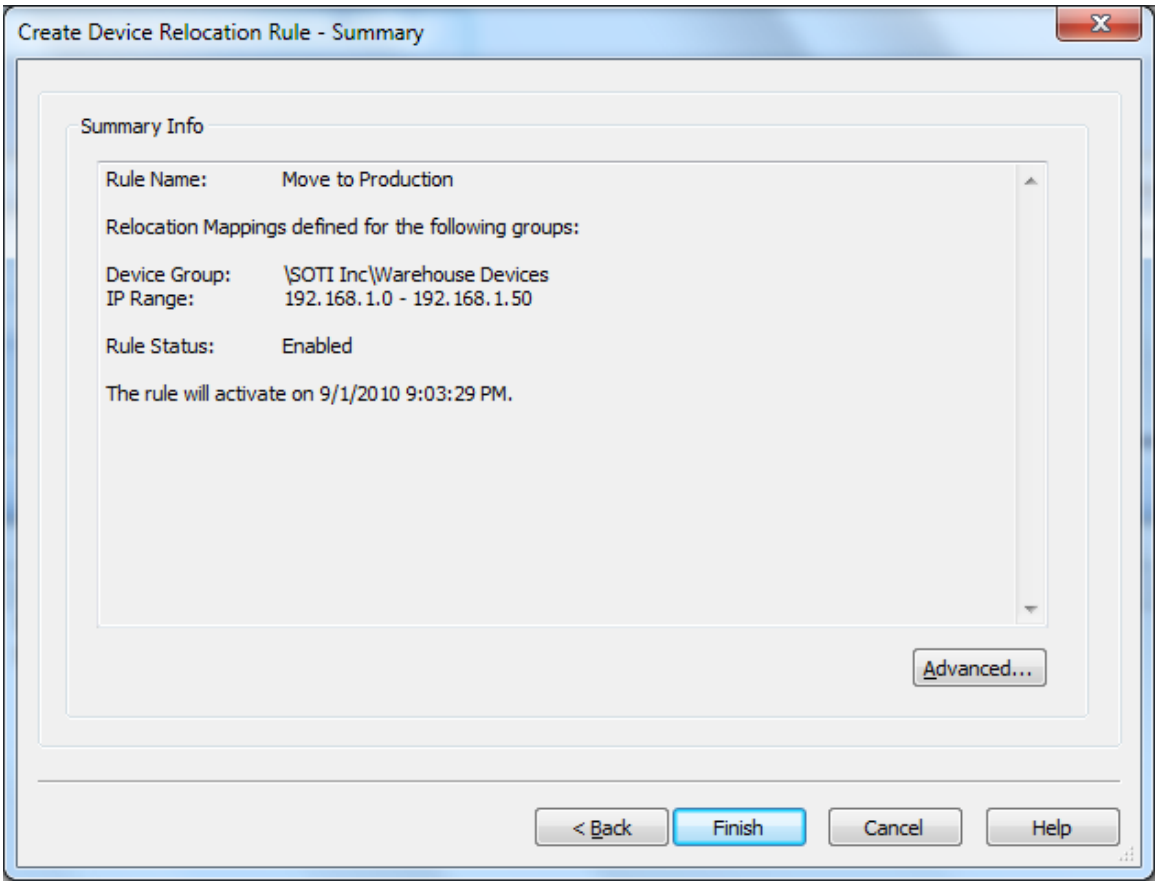
By default, the device relocation rule will be activated immediately upon completion of the wizard. If you wish to delay the activation, you can modify the activate date. A deactivate date can optionally be entered to specify a date from which the rule will be disabled.

A device relocation rule can also be explicitly disabled by clearing the checkbox next to **Enable Rule.**

After entering the fields in the above dialog box, click the **Next** button to continue.

5. Review the summarized settings.

   This page gives you an opportunity to review the settings of the device relocation rule before committing them to the database. If you wish to make any corrections, click the **Back** button, otherwise click **Finish** to complete the wizard.



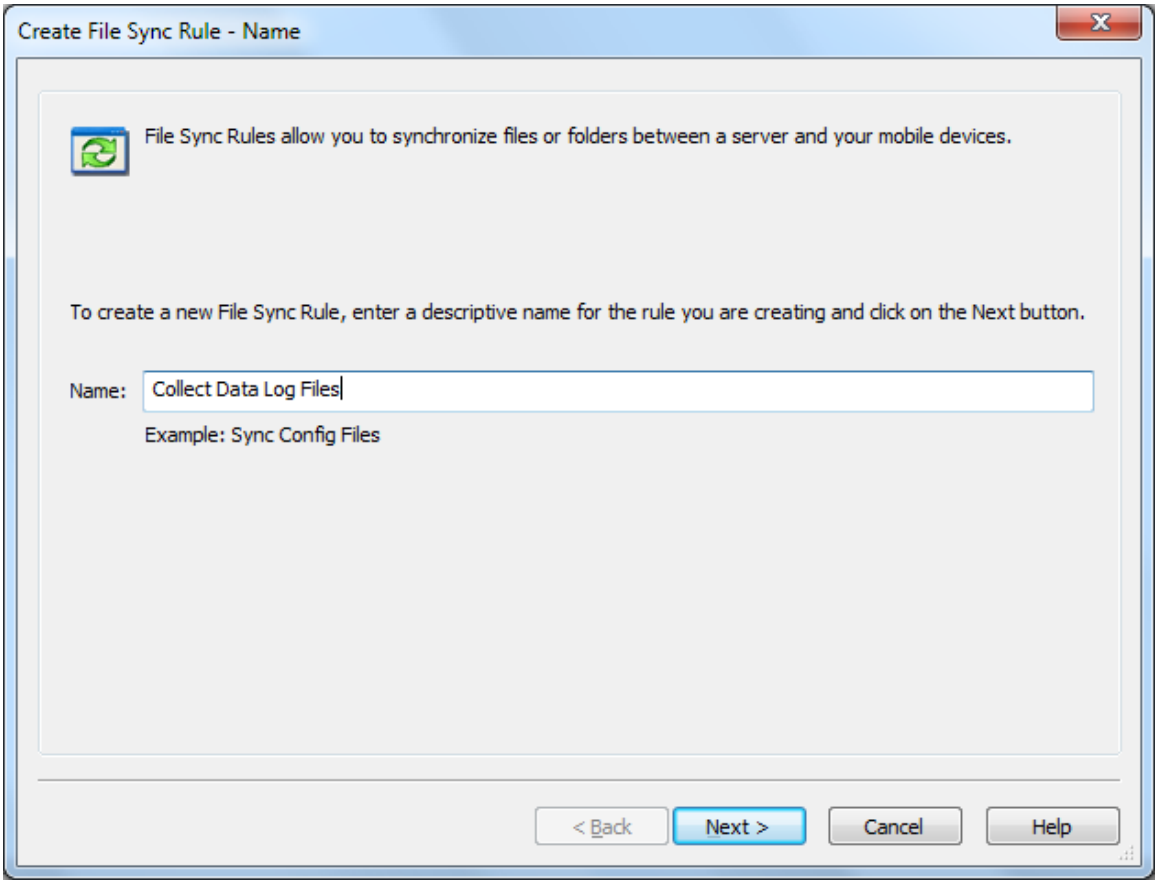
Edit Device Relocation Rule Summary dialog box

Creating File Sync Rules

File sync rules allow you to synchronize files and folders between your devices and a server. File collection, also referred to as file uploading, is a very convenient method for gathering information from devices, for example a transaction log file. File dissemination, also referred to as file downloading, is a quick and easy way to send one or more files to a set of devices such as an updated product listing or configuration file.

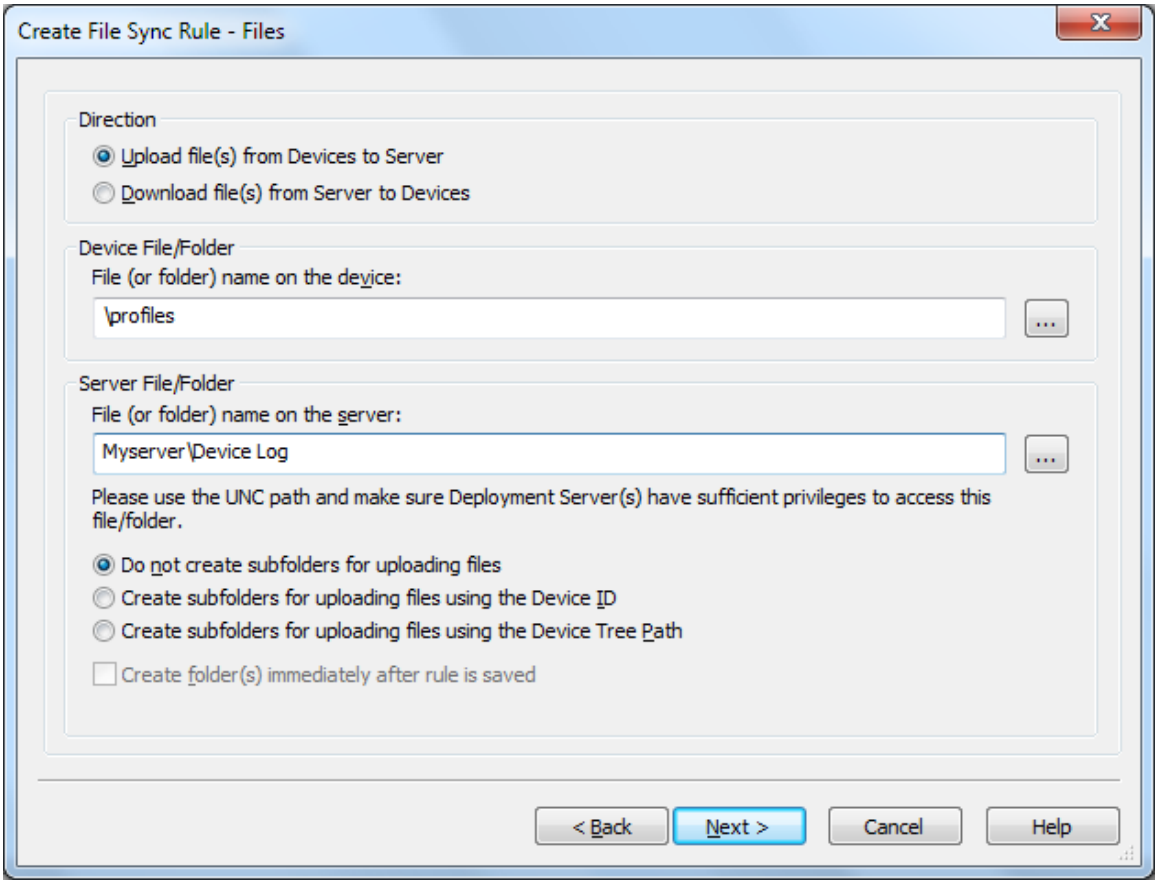
1. Start the wizard.

   Select the Rules view (tab), then click **Rule,** point to **Create Rule,** and click **File Sync Rule.** Enter a meaningful name for the rule.



First page of the Create File Sync Rule Wizard

2. Configure file synchronization source and destination.



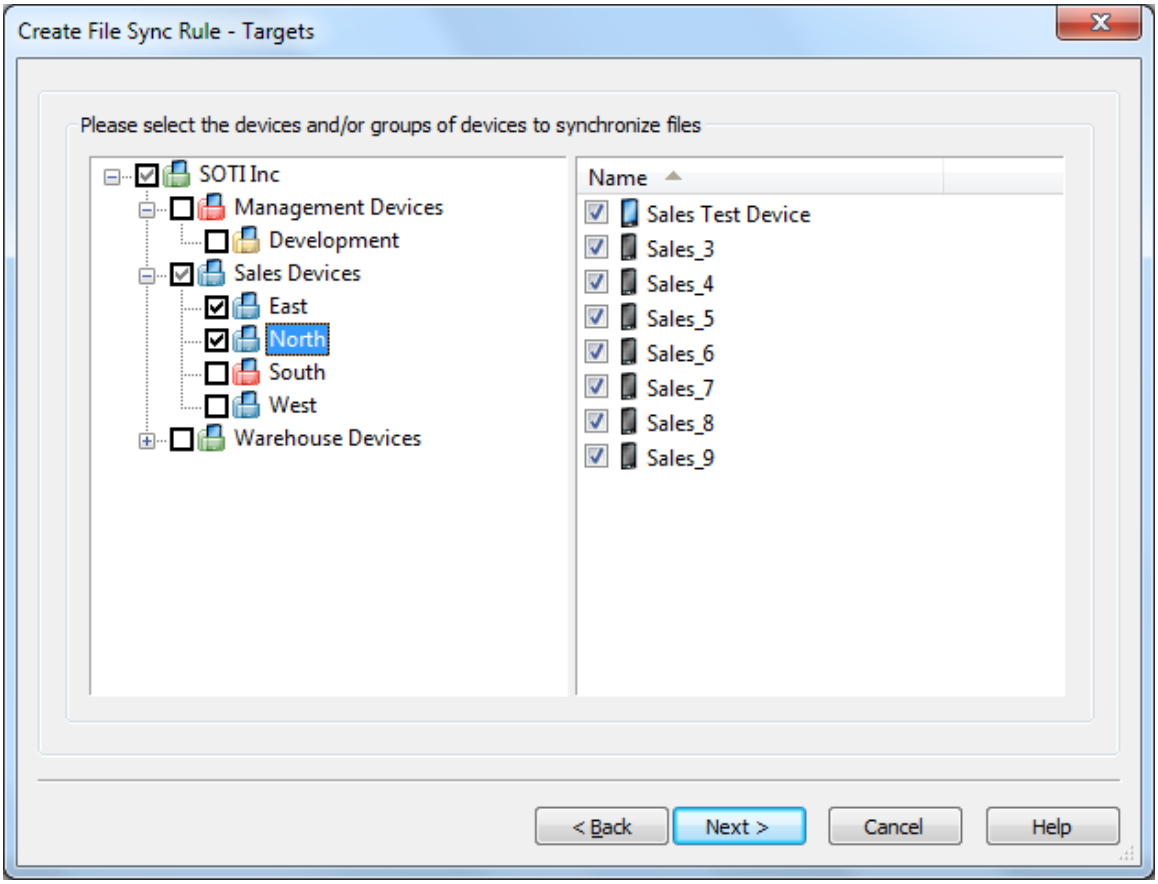
Configure file sync source and destination

The following table describes the fields of this page of the wizard:

Field Name	Description
Direction	• **Upload** (File collection) The rule will be used to upload files from the devices to a server. • **Download** (File dissemination) The rule will be used to download files from the server to devices.
Device File/Folder	Specifies the complete file system path to the files or folders being synchronized on the device
Server File/Folder	Specifies the complete file system path to the files or folders being synchronized on the server It is strongly recommended that a UNC (Universal Naming Convention) path be used. A local path (i.e. `C:\MyFiles`) can be used if only one Deployment Server is being used and the local path is on the computer running the Deployment Server. **NOTE:** It is important that the Deployment Servers have sufficient permission to read and write to the source or destination UNC path. Best practice is to run the Deployment Server under its own Active Directory user profile.
Server-side Folder Options	For **upload rules,** files collected from the devices can be written to: • A single shared folder, meaning files could potentially be overwritten if they have the same name. • A per-device subfolder, named using the device ID (i.e {00135304-41D7-019E-5800-0050BF3F5173}) • A per-device subfolder, named using the device tree path (i.e. `.\Management Devices\Device 0001`) For **download rules,** files disseminated from the server can be read from: • A single shared folder, meaning all devices get the same file(s). • A per-device subfolder, named using the device ID (i.e. {00135304-41D7-019E-5800-0050BF3F5173}) • A per-device subfolder, named using the device tree path (i.e. `.\Management Devices\Device 0001`) When the **Create folder(s) immediately after rule is saved** option is enabled, the server-side folders will be created immediately after the file sync rule is saved. This allows adding files to the folders on the servers that are synchronized with the devices when the file sync event occurs.

3. Select devices.

   Select the device(s) and group(s) for which the file sync rule will apply.



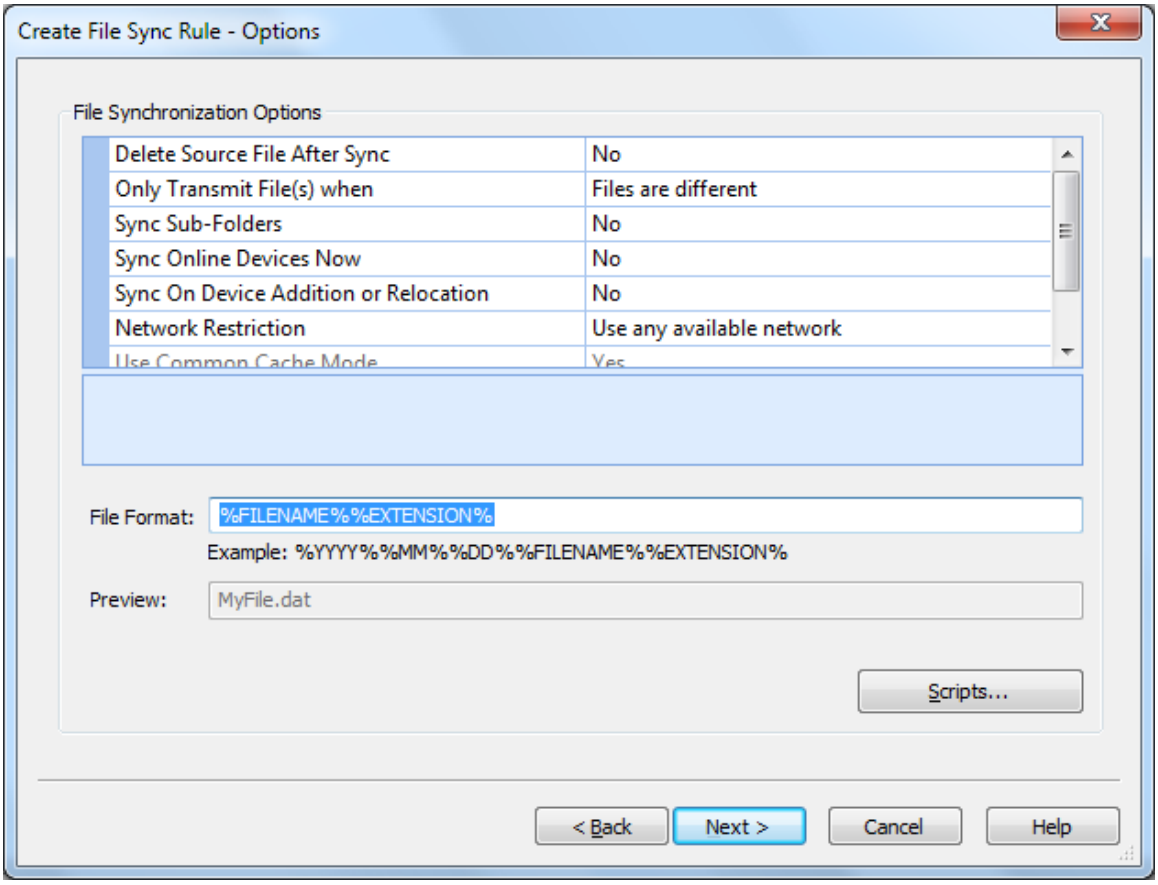
Device Group selection page

4. Specify the synchronization options.

   The following table describes the file synchronization options on this page of the Create File Sync Rule Wizard:

Field Name	Description
Delete Source File After Sync	(This applies only to upload rules.) When selected, the source file(s) on the device are transmitted to the server and then deleted from the device.

Field Name	Description
Only Transmit File (s) when	• The **Always Transmit** option will cause file(s) to be uploaded or downloaded regardless of whether or not the source and target are different or the same. • The **Files are different** option will cause file(s) to be uploaded or downloaded only if the source file is different from the destination file. • The **Source file is newer** option will cause file(s) to be uploaded or downloaded only if the source file has a more recent date-time stamp. • The **Destination file does not exist** option will cause file(s) will cause file(s) to be uploaded or downloaded only if the destination file does not exist.
Sync Sub-Folders	Synchronize files in sub-folders in addition to the files located in the target folder
Sync Online Devices Now	File synchronization will be executed immediately following the completion of the wizard for online devices.
Sync On Device Addition or Relocation	Perform file synchronization when a device is added or relocated to a device tree group for which this rule has been configured This setting is useful to easily invoke file synchronization when a device is moved from one group to another in the device tree.
Network Restriction	Restrict whether file synchronization should take place over cellular data networks (i.e. GPRS)
Upload File Name Format	Allows you to customize the names of the files that are uploaded from the devices For example, you can augment a file name with the date-time stamp of when it was uploaded. These are available file-name macros: • **%YYYY%** is for the year (e.g. 2006). • **%MM%** is for the month of year (e.g. 12 is December). • **%DD%** is for the day of month (e.g. 31). • **%H%** is for the hour in the 24-hour format (e.g. 14). • **%M%** is for the minutes (e.g. 30). • **%S%** is for the seconds (e.g. 55). • **%FILENAME%** is for the original file name (e.g. `mylogfile`). • **%EXTENSION%** is for the original file extension (e.g. `.txt`).
Use Common Cache Mode	The option to use the new, advanced caching mode of the files being disseminated is applicable only when syncing files from the server to the device. This option is set to **Yes** by default. When enabled, a single, shared, cached copy of each file being disseminated is stored on the Deployment Server. If you are experiencing issues with file synchronization, set this option to **No.**

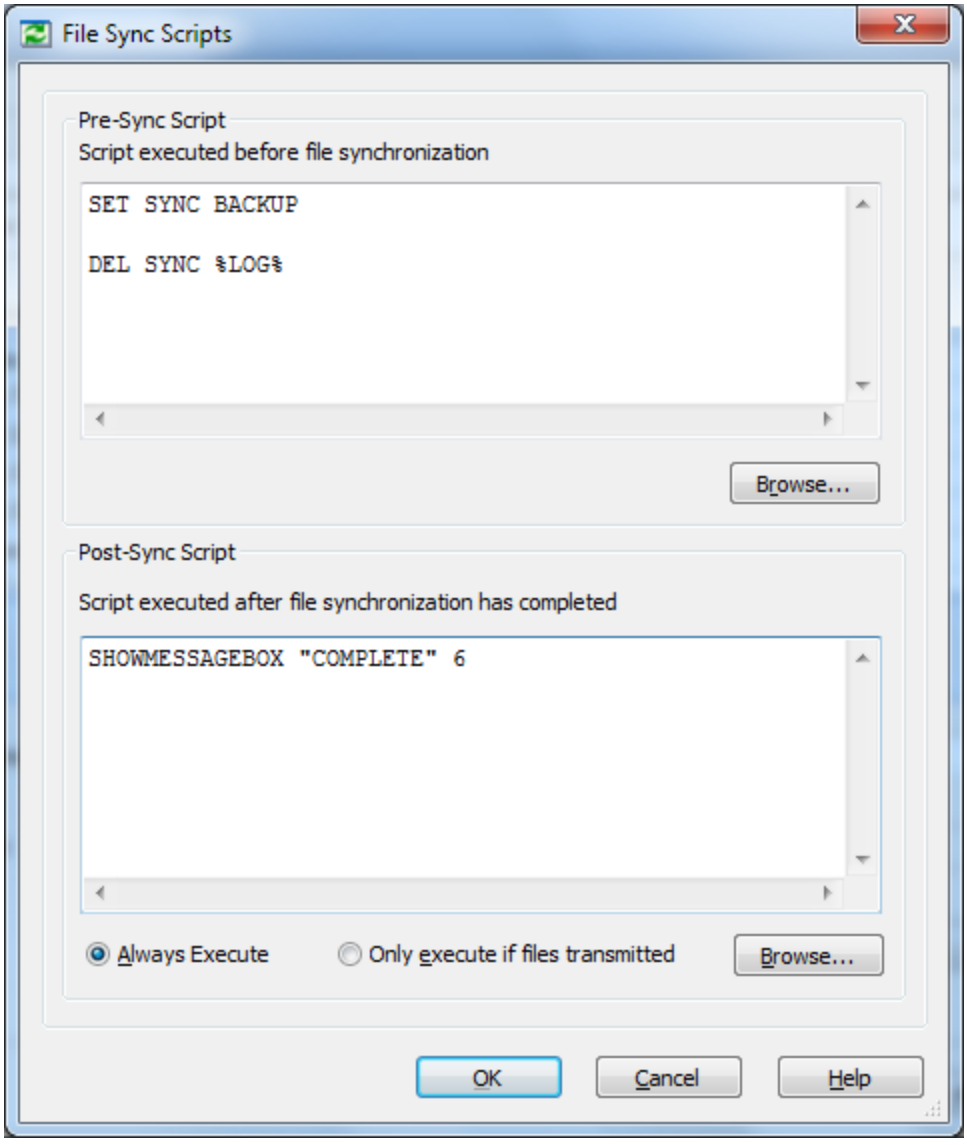


File synchronization options

Click the **Scripts** button to configure file synchronization scripts.

File Synchronization Scripts

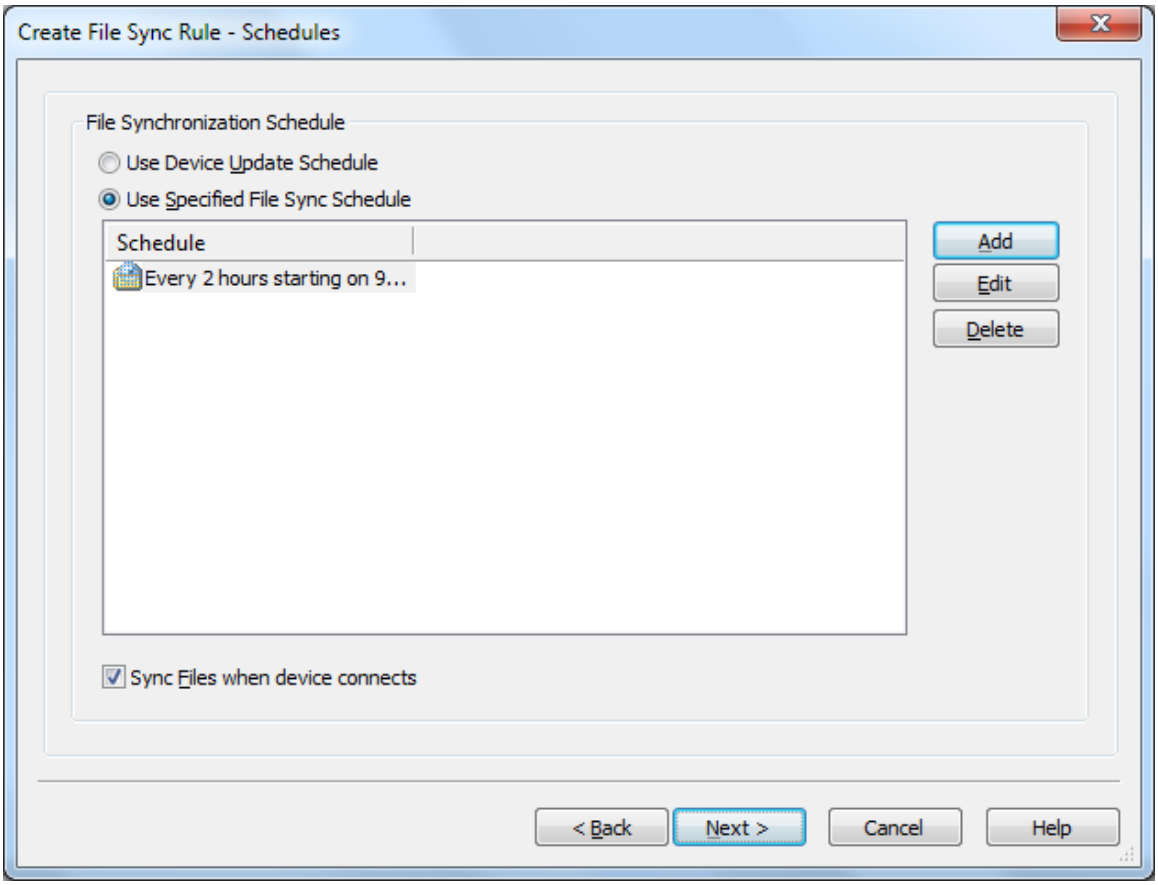
File synchronization scripts provide flexibility in automating actions on the device pre or post file synchronization. For example: Before collecting a log file from the device, stop a certain running process (e.g. `kill abc.exe`). After the file has been collected, restart the process (e.g. `start abc.exe`). Please see the "Script Command Set" topic on page 72 and the "Script Variables" topic on page 424.



File synchronization advanced options

Field Name	Description
Always execute	Will execute the script every time there is a scheduled sync, even if the files are updated or not
Only execute if files transmitted	Will execute the script when files have been updated by the sync schedule
Browse	Will allow you to import previously created scripts

5. Specify the synchronization and activation or deactivation schedule.



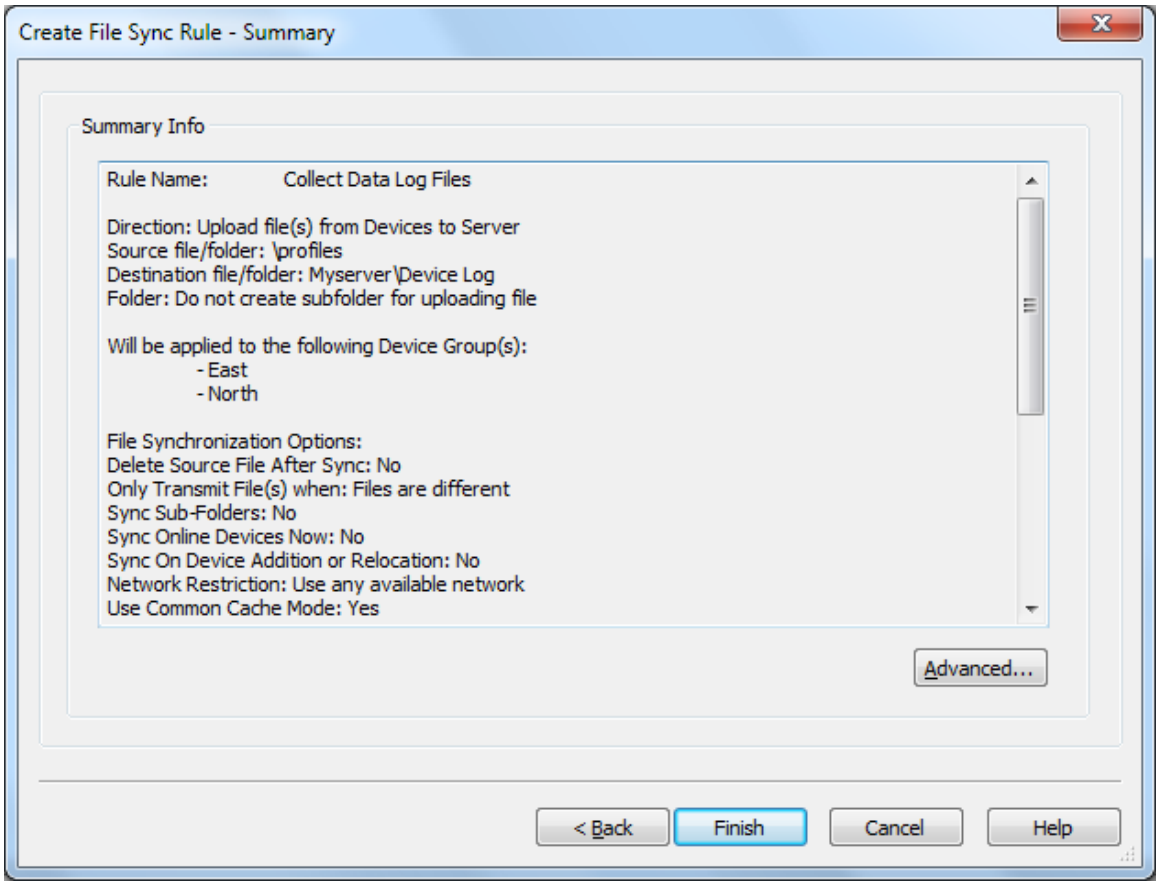
Rule activation schedule

Field Name	Description
Use Device Update Schedule	By default, the device update schedule (specified by the add devices rule used to add the devices to the system) triggers file synchronization
Use Specified File Sync Schedule	If you specify a file synchronization schedule in this dialog box, only that schedule will be used, and the device synchronization schedule will not trigger file synchronization. To Specify the custom schedule click the **Add** button. Please see the "File Synchronization Schedule" topic on page 354 for more information about creating a custom file sync schedule.

By default, the file sync rule will be activated immediately upon completion of the wizard. If you wish to delay the activation you can modify the activate date. A deactivate date can optionally be entered to specify a date from which the rule will be disabled. A file sync rule can also be explicitly disabled by clearing the **Enable Rule** check box.

6. Review summarized information.

   Review information on the **Add devices rule summary page**. This page gives you an opportunity to review the settings of the file sync rule before committing them. If you wish to make any corrections, click the **Back** button.



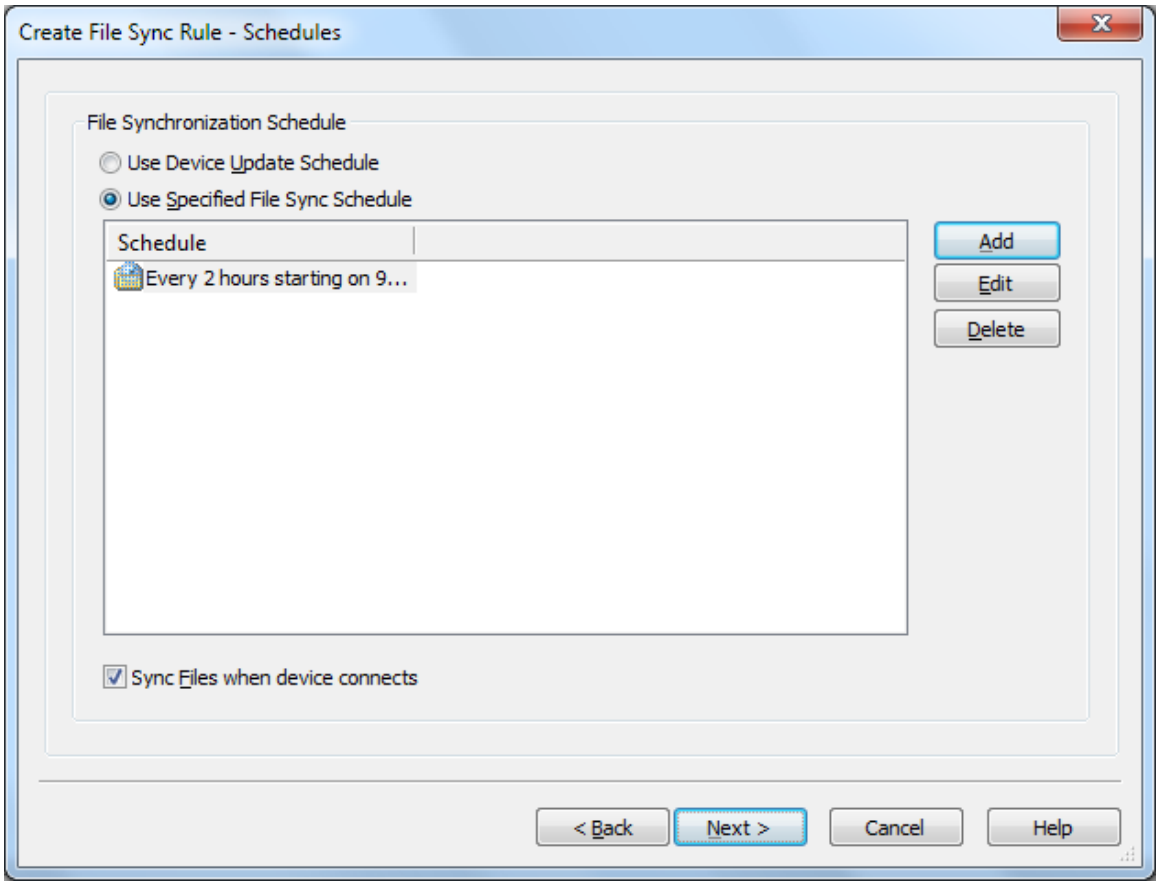
Summary page

File Synchronization Schedules

The file synchronization schedule specifies when the Deployment Server(s) should check device(s) for synchronization.

If the Deployment Server identifies an inconsistency, such as a mismatch in the file size or finds the new file, the Deployment Server will act according to the file sync rule.

By default, the device synchronization schedule, specified by the add devices rule used to add the devices to the system, is selected for file synchronization. You may add, edit or delete the custom schedule using the following dialog box.



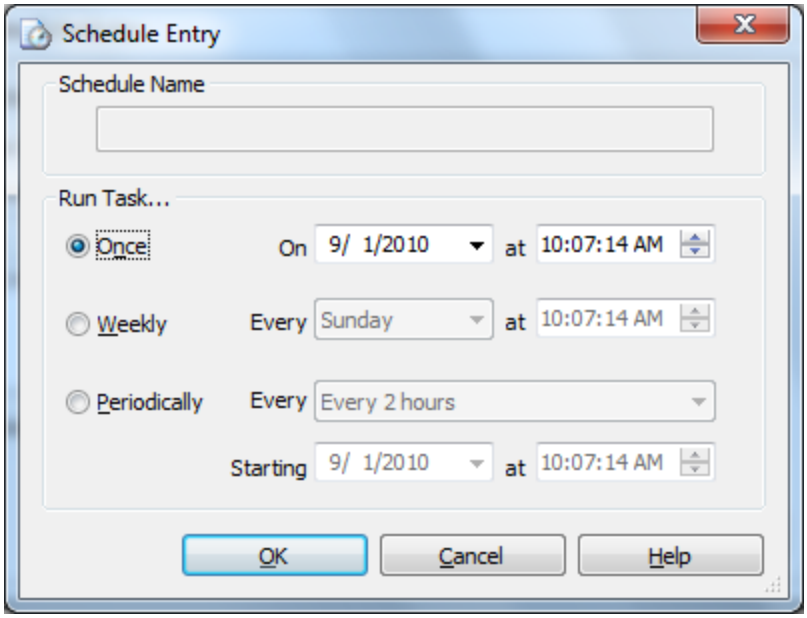
Create File Sync Rule Wizard dialog box

The following table describes the fields of the Create File Sync Rule Wizard dialog box.

Field Name	Description
Add	Specify your own file synchronization intervals. When you select **Add,** the **Schedule Entry** dialog box is displayed. **EXAMPLE:** To sync twice a week (Monday at 06:00 and Friday at 19:00), create two weekly schedule entries.
Edit	Select **Edit** to modify an existing schedule entry. The **Schedule Entry** dialog box is will be displayed.
Delete	Permanently remove a file sync schedule entry from the dialog box
Sync Files when device connects	Sync whenever devices under this rule connect to a Deployment Server (i.e. transition from offline to online)

Schedule Entry

The **Schedule Entry** dialog box allows you to specify schedule entries as one-time or periodic events.



Schedule Entry dialog box

Field Name	Description
Once	Device will check for file synchronization once at the specified date and time.
Weekly	Device will check for file synchronization once a week, on a specified day and time.
Periodically	Device will check for file synchronization periodically at the specified interval from the set, start date-time.

Packages View

The Packages view (tab) provides a list of the packages that have been imported into the MobiControl system, and the status of their distribution to the devices in the deployment. From this tab, you also have the opportunity to create a package to distribute cloned device settings.

The left panel lists all of the packages that have been imported into the MobiControl system. Package are created using MobiControl Package Studio. Please see the "MobiControl Package Studio" topic on page 413 for more information.

If multiple versions of a package have been imported, each is listed with its own unique version number. The version number is set when creating or editing a package using MobiControl Package Studio.

Adding or Deleting a Package

To add a package to MobiControl, click **Package,** and then click **Add Package.** Please see the "Adding Packages" topic on page 359 for more information.

To delete a package from MobiControl, select the version number node for the package, click **Package,** and then click **Delete.**

Creating a Cloning Package

A cloning package is a special type of package that captures settings from one 'master' device, allowing you to easily replicate those settings across other devices. For example, you can replicate Wi-Fi, power or scanner settings.

To create a new cloning package, click **Package,** and then click **Add Cloning Package.** Please see the "Clone Settings Package Wizard" topic on page 361 for information about creating the clone settings package.

Package Dependencies

Package dependencies are a way to ensure the correct sequence of installation of packages on a device. To establish a package dependency, click **Package,** and then click **Add Package Dependencies.**

Please see the "Package Dependencies" topic on page 378 for information about establishing package dependencies.

Panels in the Packages Tab

Info Panel

The Info panel provides detailed information about the package that is currently selected in the listing panel. Information includes the meta-data associated with the package that was specified when it was created, for example, processor, platform or OS version, and vendor information. Please see the "Create Package Project" topic on page 415 for a detailed explanation of these fields.

The content displayed in this panel is stored in the MobiControl database. You can select **Refresh** or press F5 on this tab to retrieve updated information from the database.

Devices Panel

The Devices panel lists the devices that have the selected package installed, or marked as pending for installation/uninstallation.

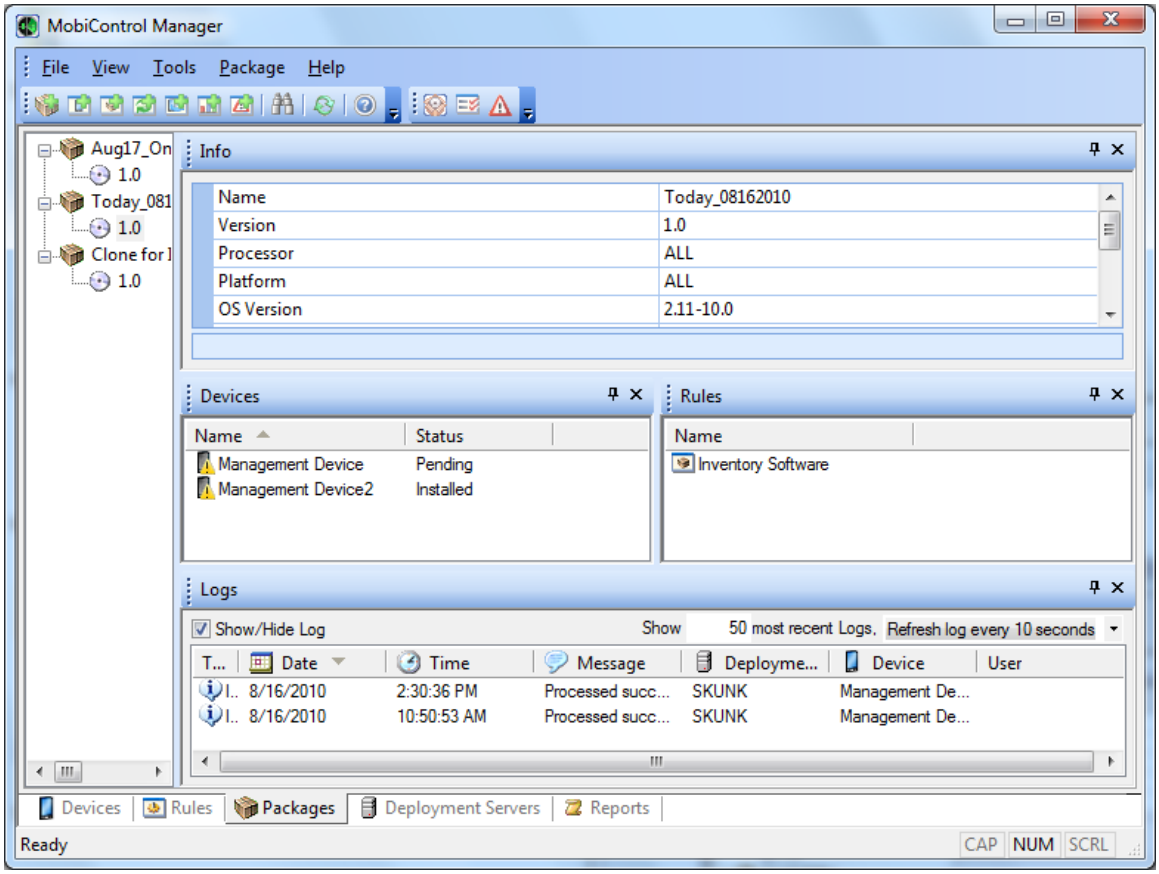
Rules Panel

The Rules panel lists the deployment rules that are configured to deploy the selected package.

Logs Panel

The Logs panel lists events occurring in the MobiControl system. This listing is filtered based on the package that is selected in the package listing.

You have the option to enable or disable logging, as well as adjust the maximum number of logs displayed and frequency with which the Manager should refresh the log panel.



MobiControl Manager Packages view (tab)

Deploying Packages to Devices

The following steps describe how you can use MobiControl to deploy packages onto mobile devices.

1. Create a package.

   A package is a set of software and data files that have been packed into a single compressed file. MobiControlprovides a tool called MobiControl Package Studio that allows you to quickly and easily create packages. For complex packages, Package Studio allows users to add scripts that get automatically executed at various points in the installation or uninstallation of the package. Please see the "Creating Packages" topic on page 414 for more information.

2. Create a deployment rule.

   When you create a deployment rule, you need to specify the package(s) to be deployed, and the devices to which the package(s) will be deployed. Please see the "Deployment Rule" topic on page 327 for more information.

3. Check the rule execution status.

   Once you have created a deployment rule, you may want to check to see if all of the devices have been provisioned with the packages specified in the rule. The execution status of the deployment rule is graphically represented in the execution chart on the Rules view (tab). MobiControl also provides a report called the "Deployment Rule Execution Summary Report." Please see the "Generate Reports" topic on page 390 for more information.

MobiControl Tutorial

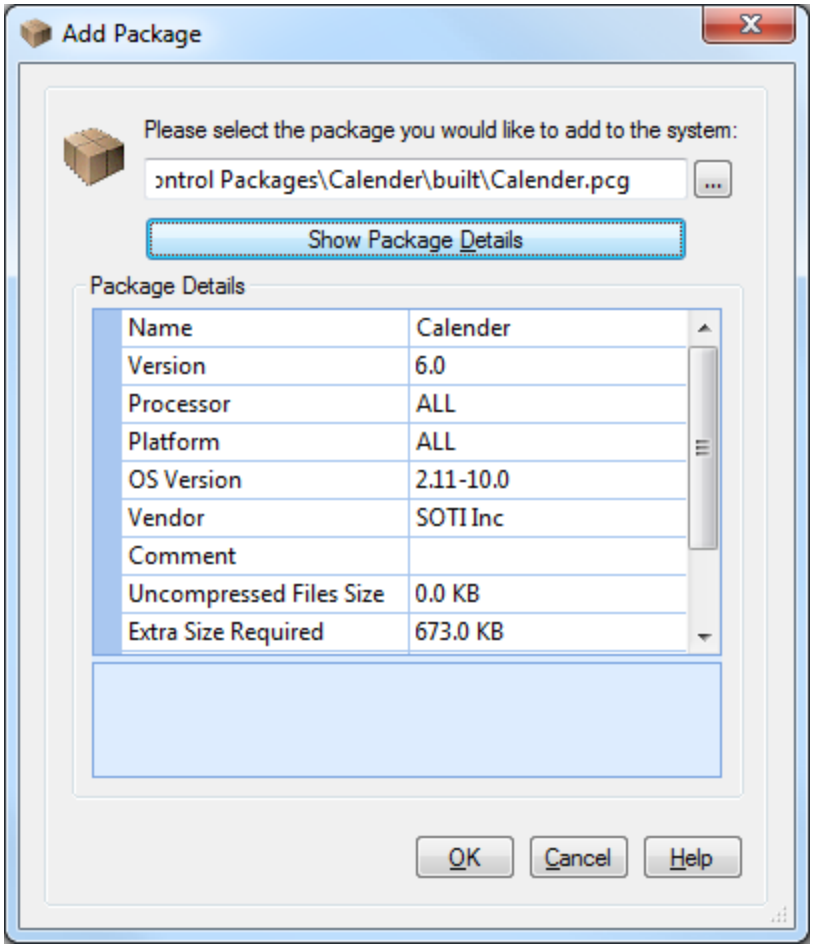
This is step 3 of the MobiControl Tutorial. Please see the "Help Desk" topic on page 28 for the next step.

Adding Packages

Before a package can be deployed to mobile devices, it must be added into MobiControl Manager. Packages are created by the MobiControl Package Studio component of MobiControl. Please see the "Creating Packages" topic on page 414 for more information on how to create a package.

To add a package, select the Packages view (tab) in MobiControl, then click on the **Device** menu and select **Add Package**. An **Add Package** dialog box will appear as shown in the figure above. Use the browse button and select the package.

If you want to see detailed attributes of selected packages, click the **Show Package Details** button.



Add Packages dialog box

UPGRADE NOTE:

When deploying updates to existing packages, if you do not want to uninstall the old version before installing the new version of the package, you need to first create a deployment rule to deploy the new version and then delete the old deployment rule. In this way MobiControl will install the new version of the package over the old version, without uninstalling the old version. Make sure you do not change the package name when you create the new version of the package, otherwise MobiControl will think it is a completely different package. If you delete the old deployment rule first, MobiControl will uninstall the old version and then deploy the new version when you add the new rule.

Device Cloning Wizard

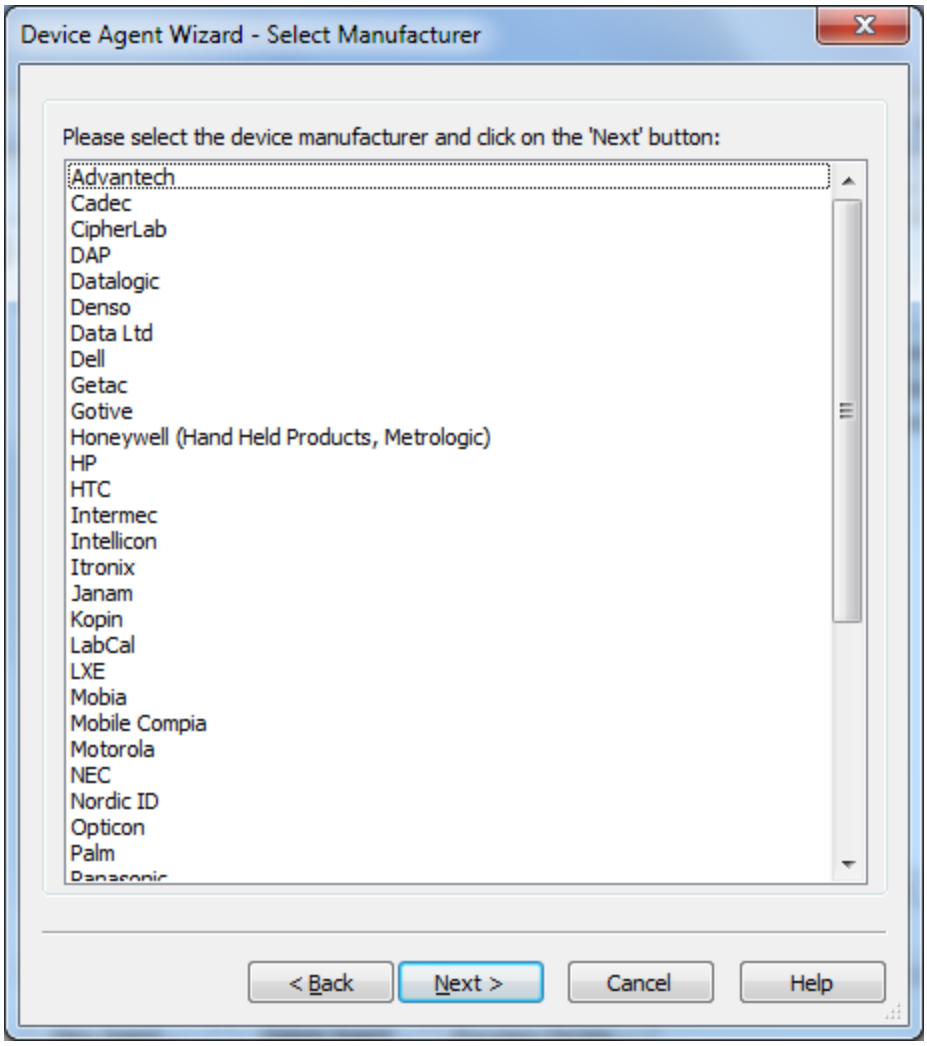
Cloning settings (e.g. Wi-Fi, power, scanners) from one master device to a set of other devices can be done by creating a package that contains the desired settings, and then deploying the package. The steps below describe the dialog boxes you must follow in the Device Cloning Wizard to create a package that captures the settings you wish to clone.

To launch the Device Cloning Wizard, select the Packages view (tab) in the MobiControl Manager and click on **Add Cloning Package** in the **Package** menu.

TIP:

To clone settings, configure a master device in the manner that you want all of your devices to be configured and dock it via ActiveSync.

1. Select the device manufacturer.
   Select **Other Manufacturers** if you don't see the manufacturer of your device listed.



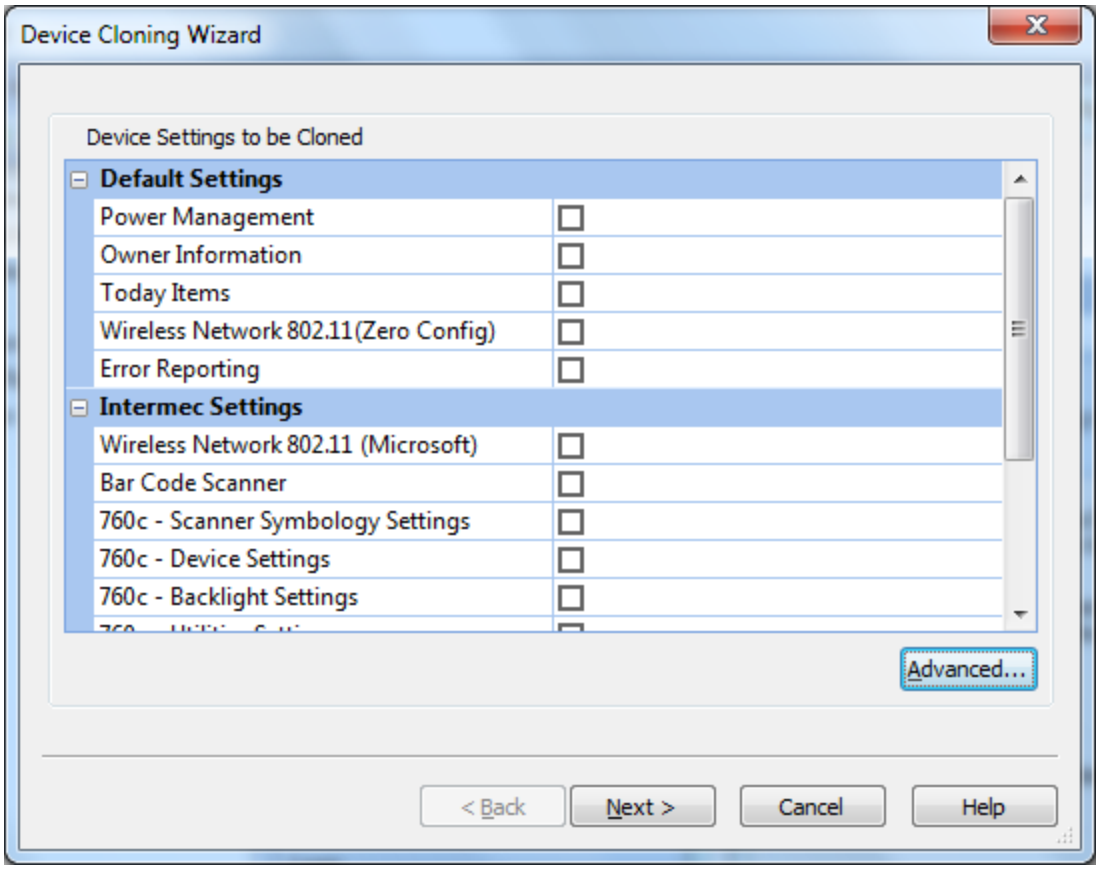
Select Device Manufacturer

IMPORTANT:

Devices that treat every boot as a cold boot cause the agent to reinstall every time. This would be a cause of concern if a cloning package included a cloning option like Wi-Fi which requires a reset and/or an initially included package that includes a reset as this would cause the device to go into an endless reset loop.

2. Select the device configuration.

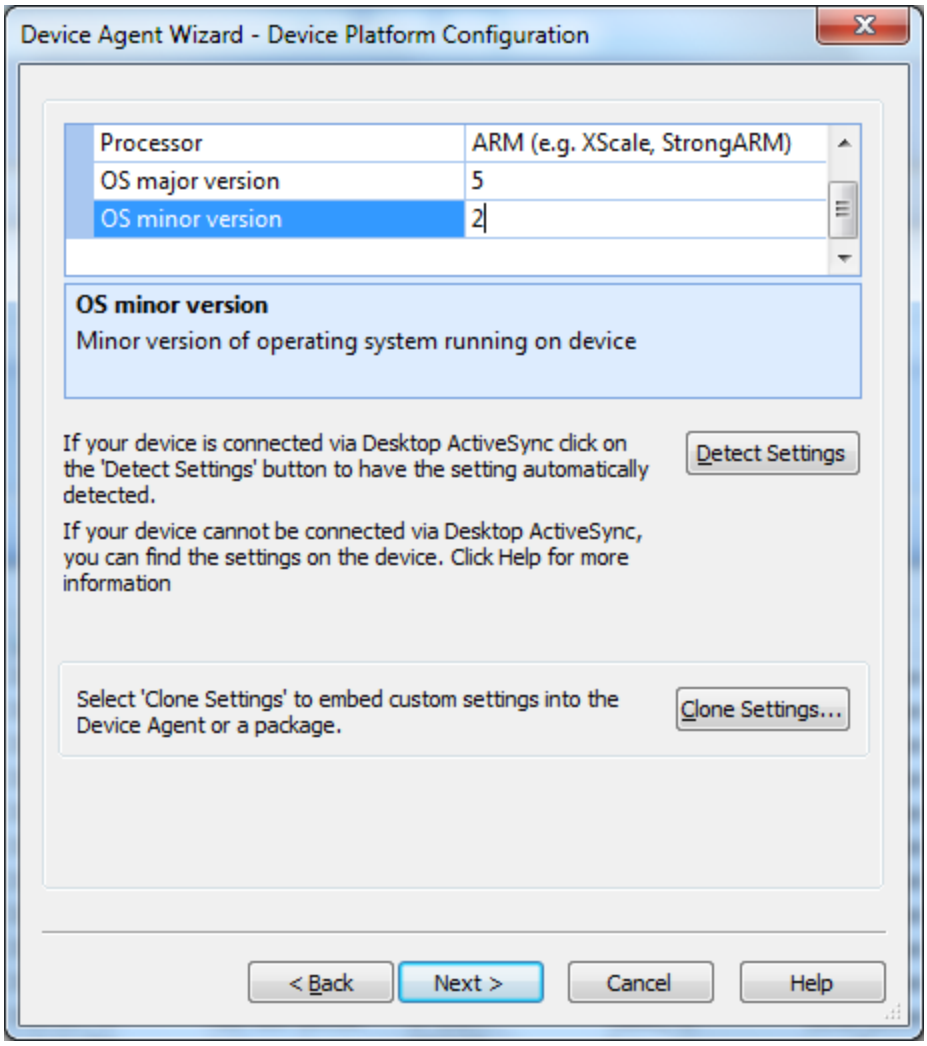
   Depending on the manufacturer selected, the wizard may display the screen below, or may skip directly to the next step.



Device Clone Options

3. Configure device type settings.

   Select the appropriate platform, processor and operating system. If you dock one of your devices via ActiveSync and click the **Detect Settings** button, the wizard can automatically detect most of the device settings. If your device is not docked, you can enter the settings manually.

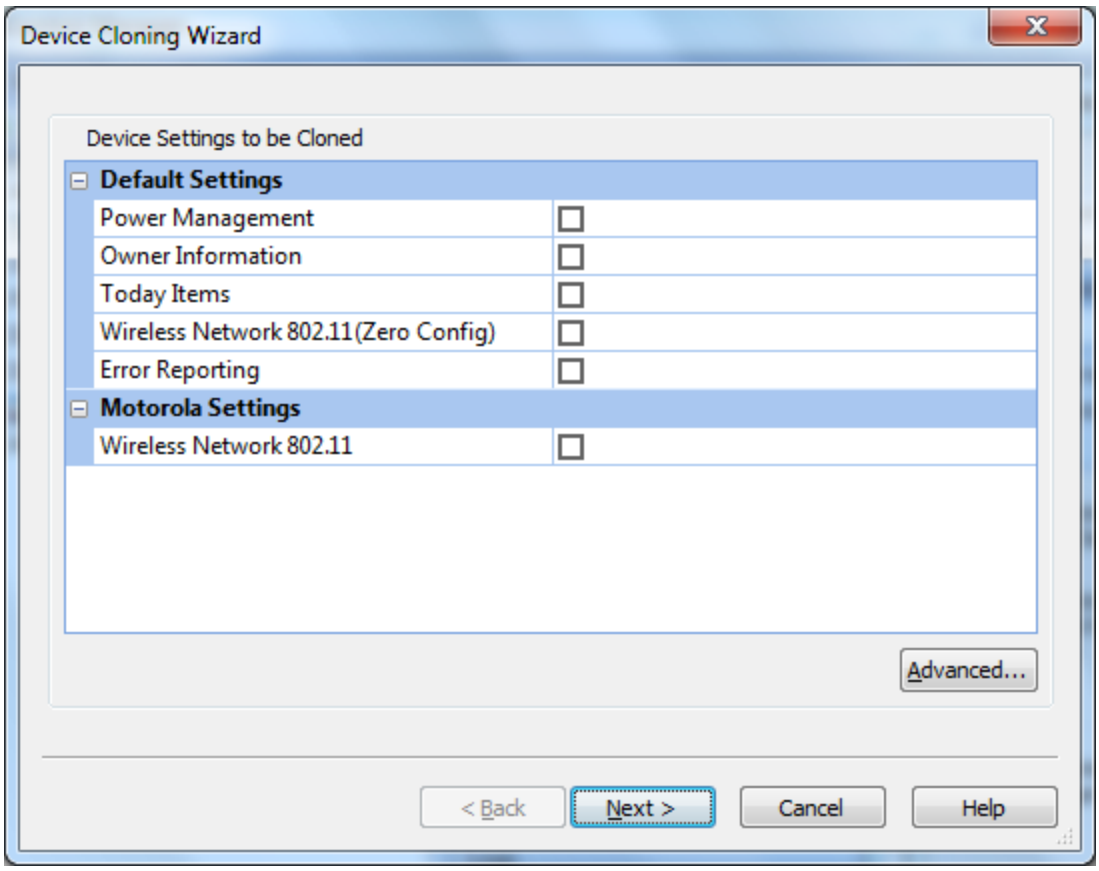


Device Clone Options

4. Select the settings to be cloned.

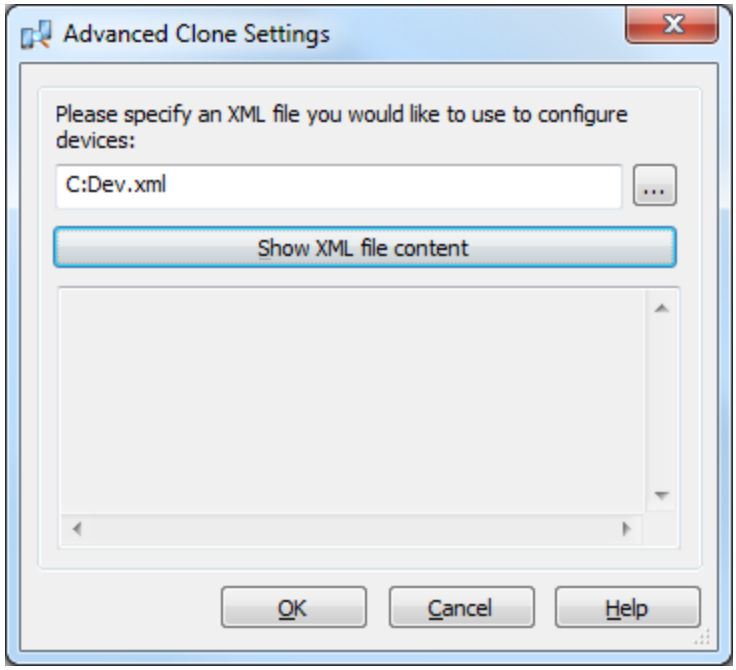
Check the items in the displayed list. MobiControl will then read the configured settings for the selected items and inject them into the MobiControl package that gets generated. In this way, when you deploy the package to your other devices all of the settings that were cloned from the master device will be applied to those devices.

Please see the "Intermec SmartSystems Settings" topic on page 368 for more information on cloning Intermec SmartSystems settings.



Device Clone Options

Click the **Advanced** button to open the **Advanced Clone Settings** dialog box.



XML Device Cloning

XML device cloning can be used to load advanced configuration options to the device via an `.xml` file. The provided `.xml` file is not parsed by MobiControl, but is passed over to the operating system. Beginning in Pocket PC 2003, there is a configuration management system which allows for easy configuration through a standardized `.xml` file. Almost every aspect of the device can be configured by this method, from encryption certificates to Wi-Fi settings. Please see the "Advanced XML Setup Script" topic on page 370 for a sample script.

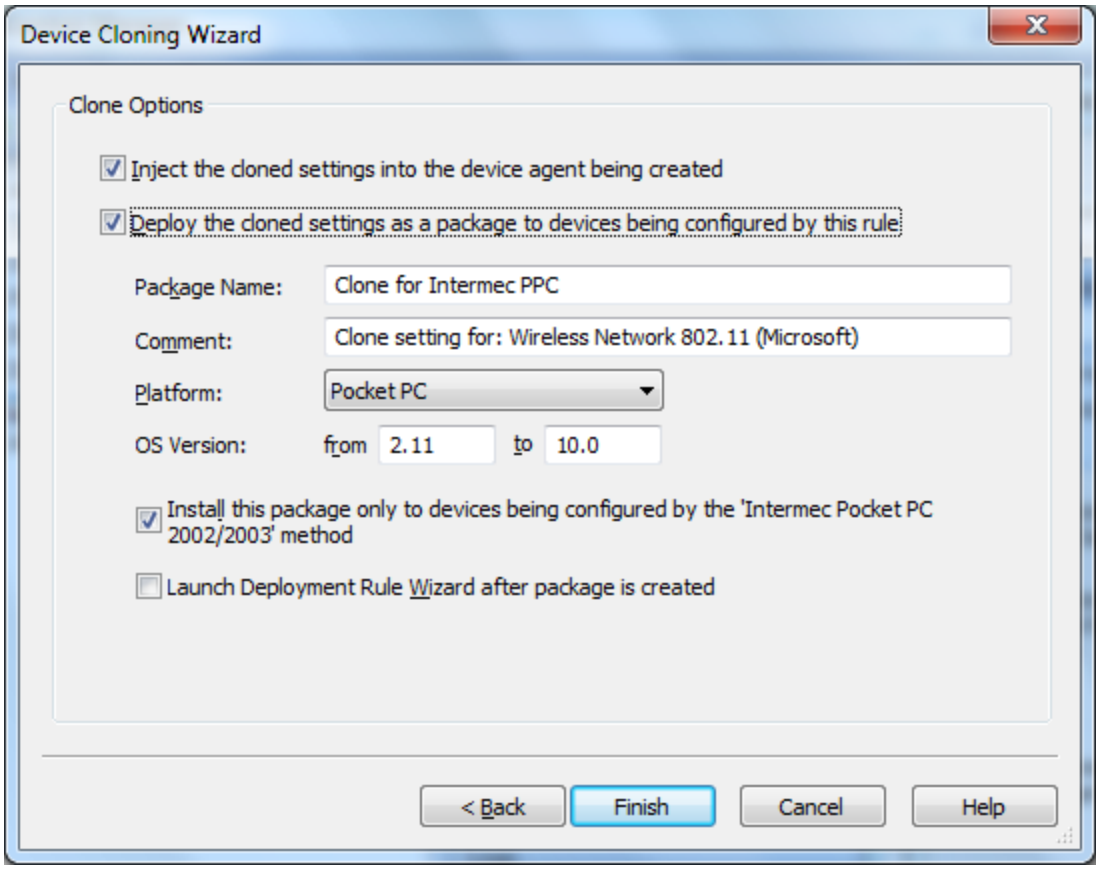
5. Specify package details.

   Provide a name for the package and a comment that describes what it contains. You can specify platform and OS version constraints.

   Click **Finish** to complete the wizard. Now, the new package that you have created will be added to the MobiControl database and will be listed on the Packages view (tab) of the Manager window. If you selected the **Launch** Create Deployment Rule Wizard **after package is created** check box, then you will be immediately guided to the wizard for deploying the new package to your devices. If you did not select this check box, you can switch to the Rules view (tab) and select **Create Deployment Rule** from the **Rule** menu.

NOTE:

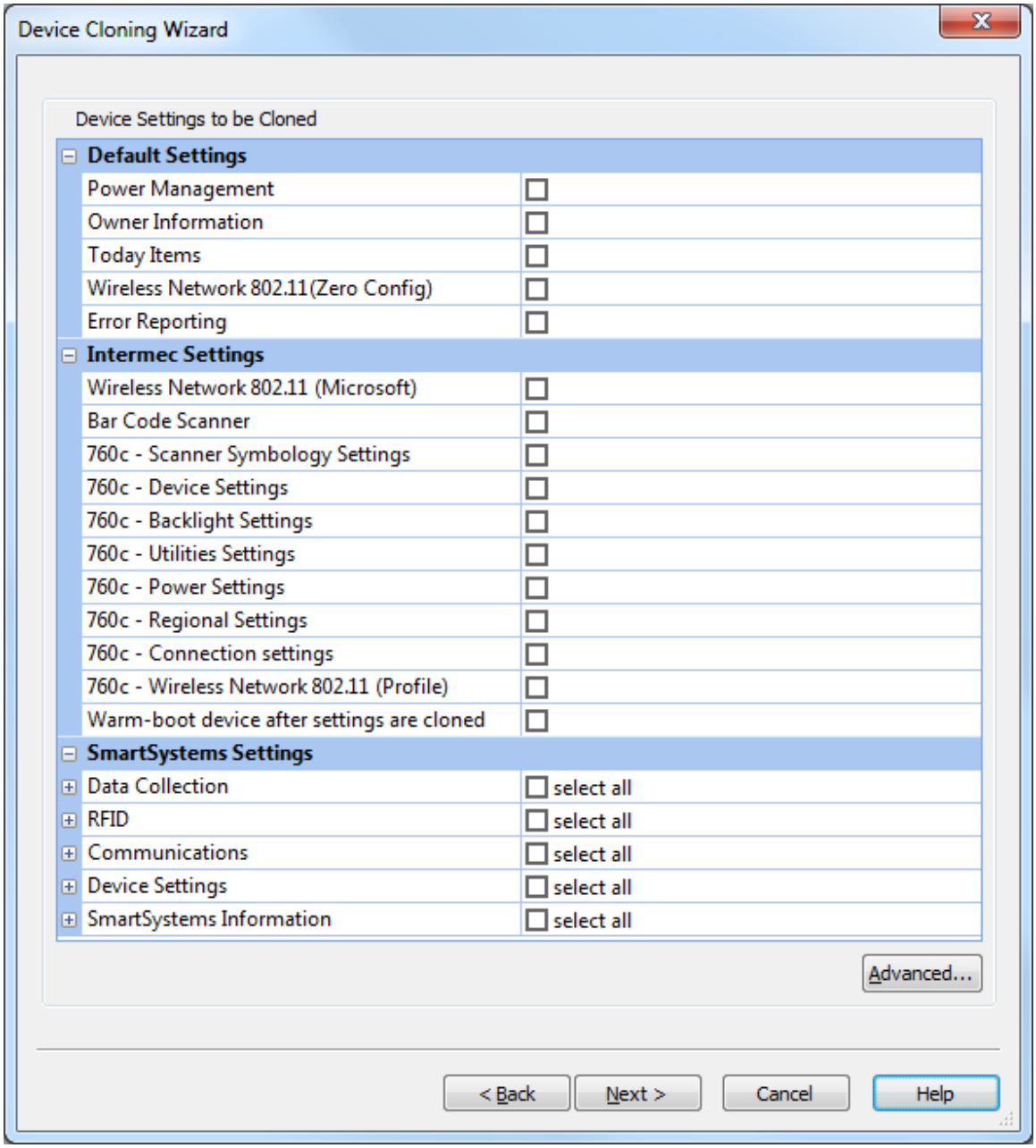
The settings that can be cloned depend on the profile that has been set up for a type of device. If there are settings for your mobile device that you would like to clone but are not listed in the Device Cloning Wizard, please contact us.



Device Clone Options

Intermec SmartSystems Settings

For Intermec devices, we have added a function to clone SmartSystems settings. From the Device Cloning Wizard, you will be able to select the appropriate SmartSystems settings that you wish to clone among your devices. By checking the box, those settings are read from the Intermec device and inserted into the cloning package. As this cloning package is deployed to other Intermec devices, the selected SmartSystems settings get deployed and configured on your mobile devices automatically.



Device clone options

Advanced XML Scripting is also available for configuration of Intermec SmartSystems-enabled devices. Intermec SmartSystems-enabled devices use XML to perform all configuration operations. Any item configurable with SmartSystems Intermec Settings can be set and retrieved with the new SmartSystems configuration APIs (Application Programming Interfaces). Please see the "Intermec SmartSystems Settings: Advanced XML Scripting" topic on page 376 for more information.

Advanced XML Setup Script

On this page, there are examples of XML scripts for any Windows Mobile device, and examples for devices with Windows Mobile 6.1 or later.

Scripts for all Windows Mobile Devices

The following script is a sample advanced XML script that does three things:

- Sets up the GPRS connection
- Adds a browser favorite for www.something.com
- Sets up MMS settings:

    ISP Name: XYZ Inc.
    Gateway: 10.10.10.22
    MMSC URI: http://mms.xyz.com
    GPRS APN: internet.xyz.com
    User name: nnn
    Password: ppp

```
<wap-provisioningdoc>
<characteristic type="CM_GPRSEntries">
 <characteristic type="XYZ MMS">
  <parm name="DestId" value="{F28D1F74-72BE-4394-A4A7-4E296219390C}"
/>
  <parm name="UserName" value="nnn" />
  <parm name="Password" value="ppp" />
  <characteristic type="DevSpecificCellular">
   <parm name="GPRSInfoAccessPointName" value="internet.xyz.com" />
  </characteristic>
 </characteristic>
</characteristic>
<characteristic type="CM_GPRSEntries">
 <characteristic type="XYZ Internet">
  <parm name="DestId" value="{436EF144-B4FB-4863-A041-8F905A62C572}"
/>
  <parm name="UserName" value="nnn" />
  <parm name="Password" value="ppp" />
  <characteristic type="DevSpecificCellular">
   <parm name="GPRSInfoAccessPointName" value="internet.xyz.com" />
  </characteristic>
 </characteristic>
</characteristic>
<characteristic type="CM_GPRSEntries">
 <characteristic type="XYZ WAP">
  <parm name="DestId" value="{7022E968-5A97-4051-BC1C-C578E2FBA5D9}"
/>
  <parm name="UserName" value="nnn" />
  <parm name="Password" value="ppp" />
  <characteristic type="DevSpecificCellular">
   <parm name="GPRSInfoAccessPointName" value="internet.xyz.com" />
  </characteristic>
 </characteristic>
</characteristic>
```

```
<characteristic type="BrowserFavorite">
 <characteristic type="Something">
  <parm name="URL" value="http://www.something.com/"/>
  <parm name="Order" value="0"/>
 </characteristic>
</characteristic>
<characteristic type="Registry">
 <characteristic type="HKLM\SOFTWARE\ArcSoft\ArcSoft MMS
UA\Config\mm1">
  <parm name="2" value="44000" datatype="string" />
 </characteristic>
</characteristic>
<characteristic type="Registry">
 <characteristic type="HKLM\SOFTWARE\ArcSoft\ArcSoft MMS
UA\Config\mm1">
  <parm name="TotalSettings" value="2" datatype="integer" />
  <parm name="DefaultSetting" value="2" datatype="integer" />
 </characteristic>
</characteristic>
<characteristic type="Registry">
  <characteristic type="HKLM\SOFTWARE\ArcSoft\ArcSoft MMS
UA\Config\UI">
   <parm name="ConnectionVia" value="Secure WAP Network"
datatype="string" />
 </characteristic>
</characteristic>
<characteristic type="Registry">
 <characteristic type="HKLM\SOFTWARE\ArcSoft\ArcSoft MMS
UA\Config\mm1\44000">
  <parm name="SendDefault" value="102400" datatype="integer" />
  <parm name="RecvDefault" value="102400" datatype="integer" />
  <parm name="MmscURI" value="http://mms.xyz.com" datatype="string"
/>
  <parm name="Gateway" value="10.10.10.22" datatype="string" />
  <parm name="Name" value="xyz MMSC" datatype="string" />
  <parm name="GatewayPort" value="9201" datatype="integer" />
</characteristic>
</characteristic>
</wap-provisioningdoc>
```

Scripts for Devices with Windows Mobile 6.1 or later

The following scripts are only for Windows Mobile 6.1 devices. Please see http://msdn.microsoft.com/en-us/library/bb882210.aspx for more information and examples.

Disable Bluetooth

```
<wap-provisioningdoc>
<characteristic type="NetworkPolicy">
 <characteristic type="Bluetooth">
    <characteristic type="Settings">
      <parm name="Disabled" value="1"/>
    </characteristic>
  </characteristic>
</characteristic>
</wap-provisioningdoc>
```

Enable Bluetooth

```
<wap-provisioningdoc>
<characteristic type="NetworkPolicy">
  <characteristic type="Bluetooth">
    <characteristic type="Settings">
      <parm name="Disabled" value="0"/>
    </characteristic>
  </characteristic>
</characteristic>
</wap-provisioningdoc>
```

Disable Camera

```
<wap-provisioningdoc>
<characteristic type="Camera">
      <parm name="Disable" value="-1"/>
   </characteristic>
</wap-provisioningdoc>
```

Enable Camera

```
<wap-provisioningdoc>
   <characteristic type="Camera">
      <parm name="Disable" value="0"/>
   </characteristic>
</wap-provisioningdoc>
```

Disable Email

```
<wap-provisioningdoc>
<characteristic type="SecurityPolicy">
<parm name="4148" value="0"/>
</characteristic>
</wap-provisioningdoc>
```

Enable Email

```
<wap-provisioningdoc>
<characteristic type="SecurityPolicy">
<parm name="4148" value="1"/>
</characteristic>
</wap-provisioningdoc>
```

Block Applications

```
<wap-provisioningdoc>
<characteristic type="SoftwareDisable">
  <characteristic type="DisabledSystemFiles">
    <parm name="calc.exe" value="These files have been blocked." />
    <parm name="pword.exe" />
  </characteristic>
</characteristic>
</wap-provisioningdoc>
```

Unblock Applications

```
<wap-provisioningdoc>
<characteristic type="SoftwareDisable">
  <characteristic type="DisabledSystemFiles">
    <noparm name="pxl.exe" />
    <noparm
```

```
 name="pword.exe" />
  </characteristic>
</characteristic>
</wap-provisioningdoc>
```

POP3 and IMAP4 Email

```
<wap-provisioningdoc>
<characteristic type="EMAIL2">
   <characteristic type="{D671C70B-8EE3-4881-8045-2AEE6F731B55}">
      <parm name="SERVICENAME" value="MyIMAP"/>
      <parm name="SERVICETYPE" value="IMAP4"/>
      <parm name="INSERVER"    value="Imapserver"/>
      <parm name="OUTSERVER"   value="smtpserver"/>
      <parm name="AUTHNAME"    value="alias"/>
      <parm name="AUTHSECRET"  value="password"/>
      <parm name="DOMAIN"      value="oceana"/>
      <parm name="REPLYADDR"   value="emailAddress"/>
   </characteristic>
   <characteristic type="{4FE84006-9E8A-4158-864D-A2E1E98C3786}">
      <parm name="SERVICENAME" value="MyPOP"/>
      <parm name="SERVICETYPE" value="POP3"/>
      <parm name="INSERVER"    value="popserver"/>
      <parm name="OUTSERVER"   value="smtpserver"/>
      <parm name="AUTHNAME"    value="alias"/>
      <parm name="AUTHSECRET"  value="password"/>
      <parm name="DOMAIN"      value="oceana"/>
      <parm name="REPLYADDR"   value="emailAddress"/>
   </characteristic>
</characteristic>
</wap-provisioningdoc>
```

Set Speed Dial Number

```
<wap-provisioningdoc>
<characteristic type="SpeedDial">
  <characteristic type="Firstname Lastname">
     <parm name="Key" value="2"/>
      <parm name="Tel" value="4255550111"/>
  </characteristic>
</characteristic>
</wap-provisioningdoc>
```

Exchange ActiveSync

```
<wap-provisioningdoc>
   <characteristic type="Sync">
      <characteristic type="Settings">
         <parm name="BodyTruncation" value="1024"/>
         <parm name="PeakStartTime" value="0800"/>
         <parm name="PeakEndTime" value="1800"/>
         <parm name="PeakFrequency" value="0"/>
         <parm name="AutoSyncWhenCradled" value="1"/>
         <parm name="SyncAfterTimeWhenCradled" value="120"/>
      </characteristic>
      <characteristic
```

```
 type="Connection">
        <parm name="Domain" value="thephone-company"/>
        <parm name="Server" value="TestServer"/>
        <parm name="User" value="username"/>
     </characteristic>
     <characteristic type="Mail">
        <parm name="EmailAgeFilter" value="1"/>
        <parm name="Enabled" value="1"/>
        <parm name="MailBodyTruncation" value="1024"/>
        <parm name="MailFileAttachments" value="1024"/>
     </characteristic>
     <characteristic type="Calendar">
        <parm name="CalendarAgeFilter" value="1"/>
        <parm name="Enabled" value="1"/>
     </characteristic>
     <characteristic type="Contacts">
        <parm name="Enabled" value="1"/>
     </characteristic>
   </characteristic>
</wap-provisioningdoc>
```

GPRS Setup

```
<wap-provisioningdoc>
<characteristic type="CM_GPRSEntries">
   <characteristic type="GPRS1">
      <parm name="DestId"   value="{436EF144-B4FB-4863-A041-
8F905A62C572}" />
       <characteristic type="DevSpecificCellular">
         <parm name="BearerInfoValid" value="1" />
         <parm name="GPRSInfoValid" value="1" />
         <parm name="GPRSInfoProtocolType" value="2" />
         <parm name="GPRSInfoL2ProtocolType"  value="PPP" />
         <parm
name="GPRSInfoAccessPointName"  value="internet3.thephone-
company.com" />
         <parm name="GPRSInfoAddress"  value="" />
         <parm name="GPRSInfoDataCompression"  value="1" />
         <parm name="GPRSInfoHeaderCompression"  value="1" />
         <parm name="GPRSInfoParameters" value="" />
      </characteristic>
    </characteristic>
  </characteristic>
</wap-provisioningdoc>
```

Set up a Proxy Server

```
<wap-provisioningdoc>
<characteristic type="CM_ProxyEntries">
    <characteristic type="HTTP-{A1182988-0D73-439e-87AD-2A5B369F808B}
">
      <parm name="SrcId" value="{A1182988-0D73-439e-87AD-
```

```
2A5B369F808B}" />
      <parm name="DestId" value="{436EF144-B4FB-4863-A041-
8F905A62C572}" />
      <parm name="Proxy" value="proxyservername:80" />
    </characteristic>
</characteristic>
</wap-provisioningdoc>
```

Backlight Settings AC and Battery

```
<wap-provisioningdoc>
<characteristic type="DeviceInformation">
   <parm name="BacklightACTimeout" value="300" />
</characteristic>
<characteristic type="DeviceInformation">
   <parm name="BacklightBatteryTimeout" value="60" />
</characteristic>
</wap-provisioningdoc>
```

Advanced Intermec SmartSystems Settings: XML Scripting

Intermec SmartSystems-enabled devices use XML to perform all configuration operations. Any item configurable with SmartSystems Intermec Settings can be set and retrieved with the new SmartSystems configuration APIs.

The following is an example of the XML script that enables "Code 39 decoding" in all devices in the Scanners group.

How to get "Code 39" options:

```
<DevInfo Action="Get">
    <Subsystem Name="Data Collection">
      <Group Name="Scanners" Instance="0">
         <Group Name="Symbologies">
    <Group Name="Code 39">
    <Field Name="Enable Code 39"></Field>
      <Group Name="Options">
       <Field Name="Full ASCII Conversion"> </Field>
   <Field Name="Start/Stop transmission"> </Field>
        <Field Name="Start character"> </Field>
          <Field Name="Verify check digit"> </Field>
           <Field Name="Transmit check digit"> </Field>
            <Field Name="Reading range"> </Field>
             <Field Name="Reading tolerance"> </Field>
   <Field Name="Length mode"></Field>
      <Field Name="Length 1"> </Field>
         <Field Name="User defined symbology ID"></Field>
               </Group>
  </Group>
         </Group>
    </Group>
    </Subsystem>
</DevInfo>
```

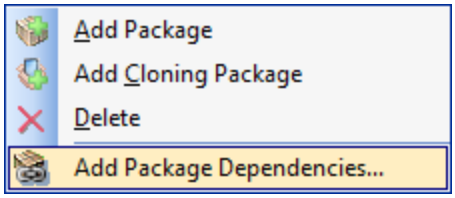
How to set "Code 39" options:

```
<DevInfo Action="Set">
   <Subsystem Name="Data Collection">
      <Group Name="Scanners" Instance="0">
         <Group Name="Symbologies">
            <Group Name="Code 39">
               <Field Name="Enable Code 39">1</Field>
               <Group Name="Options">
   <Field Name="Full ASCII Conversion">0</Field>
      <Field Name="Start/Stop transmission">0</Field>
         <Field Name="Start character">2</Field>
            <Field Name="Verify check digit">0</Field>
               <Field Name="Transmit check digit">0</Field>
                  <Field Name="Reading range">0</Field>
   <Field Name="Reading tolerance">0</Field>
      <Field Name="Length mode">0</Field>
         <Field Name="Length 1">3</Field>
            <Field Name="User defined symbology ID">B1</Field>
                </Group>
  </Group>
         </Group>
    </Group>
    </Subsystem>
</DevInfo>
```

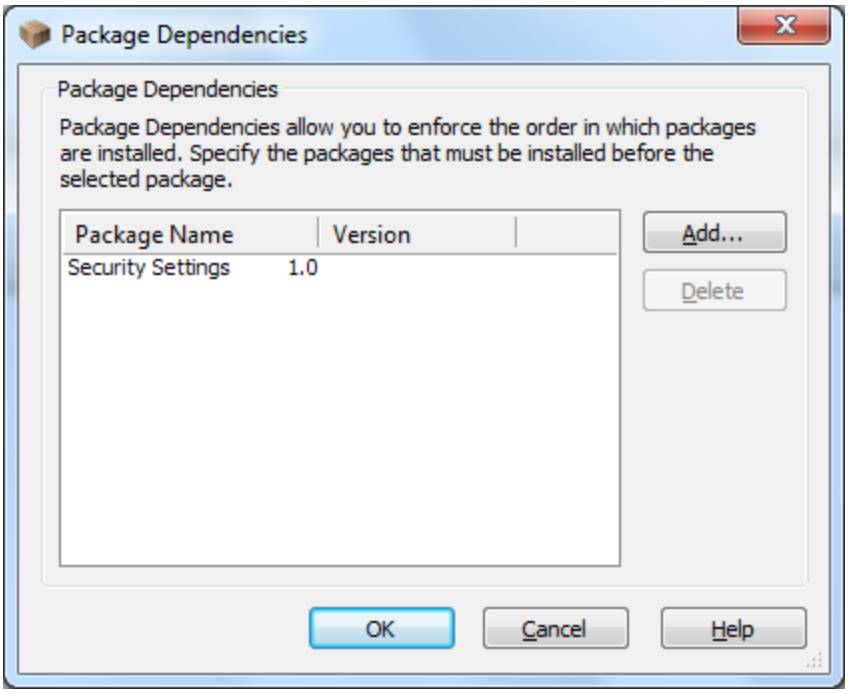
Package Dependencies

Package dependencies provide a mechanism to enforce the order in which packages are installed on a device.

To display the **Package Dependencies** dialog box, right-click on the package and select **Add Package Dependencies** from the pop-up menu. The **Package Dependencies** dialog box lists the configured dependencies.



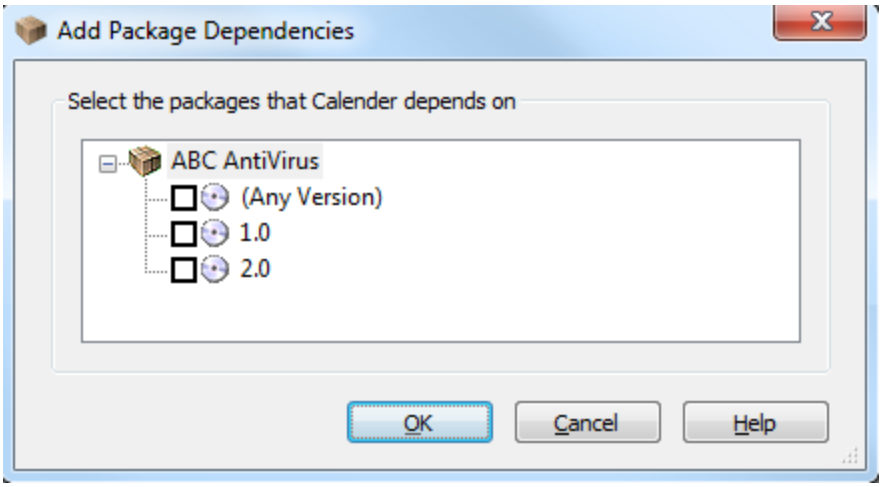
Packages menu



Package Dependencies dialog box

Adding Package Dependencies

To add a package dependency, select the package(s) and version(s) upon which the target package is dependent.



Add Package Dependencies dialog box

EXAMPLE:

Packages A and B need to be installed, but it is mandatory that A is installed before B. Configure a dependency for package B: when editing the package dependencies for package B, select package A.

NOTE:

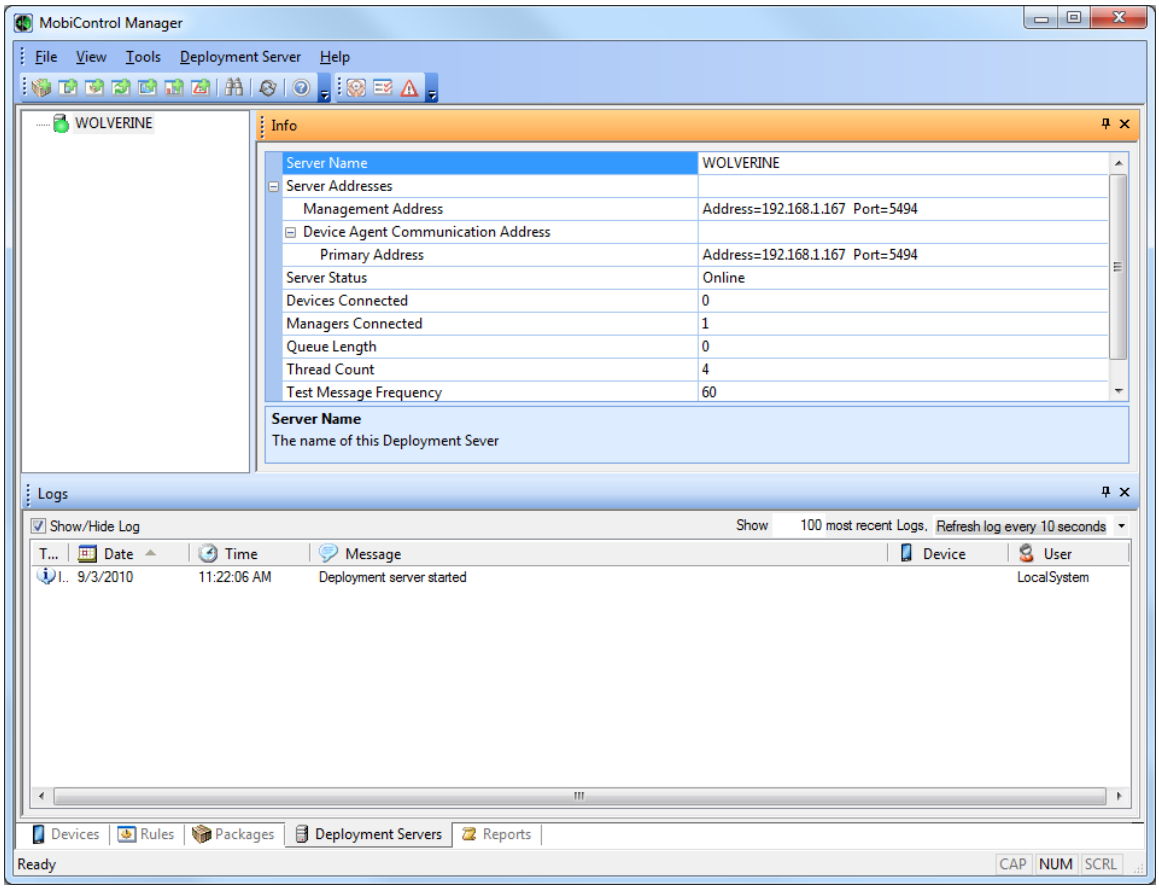
If a package depends on another package that is scheduled to install at a later time, then the Deployment Server will not push the package unless it is also scheduled to install at the same time or later. Please see the "Deployment Rule" topic on page 327 for more information about installation schedules.

Deployment Servers View

The Deployment Servers view (tab) in MobiControl Manager lists all MobiControlDeployment Servers installed, the online devices connected to the servers as well as properties and logs for the servers. Users can remotely configure and manage Deployment Servers using the Deployment Servers view (tab).

To install an additional Deployment Server, execute the setup program on the computer on which you would like to install the Deployment Server, select the custom installation option, and then choose to install the Deployment Server component. You need to purchase a license for each additional server you add to the system.

Please see the "Deployment Server Overview" topic on page 382 for general concepts about MobiControlDeployment Servers.



Deployment Servers view (tab)

Using the Deployment Servers view (tab), users can perform the following Deployment Server management operations:

- **Enable or disable a Deployment Server** by right-clicking on a server and selecting **Enable** or **Disable.** If you disable a Deployment Server, all devices connected to that server will be disconnected. If other servers are available the devices will automatically connect to other available servers.
- **Shut down a Deployment Server** by right-clicking on a server and selecting the **Shutdown Server** option.
- **Delete a server** from the Deployment Servers view (tab) to free up server licenses when moving the Deployment Server to a different server or workstation, by right-clicking on a server and selecting the **Delete Server** option.
- **View activity information for a specific server** by selecting a Deployment Server in the left pane. Make sure that the **Enable/Disable Log** option is enabled (or checked) in the right pane. After viewing the logging information, we recommend that you disable the logging again.
- **View activity information for a specific device** by selecting the device in the left pane. Make sure that the **Enable/Disable Log** option is enabled in the right pane. After viewing the logging information, we recommend that you disable logging again.

NOTE:

Users can set the refresh rate for showing the logging information, but a more frequent refresh rate, e.g. refresh log every second, may slow down system performance.

Please see the "Set Deployment Server Properties" topic on page 383 for detailed information on configuring the Deployment Servers.

Deployment Server Overview

The MobiControl Deployment Server is responsible for interacting with devices and executing deployment and device configuration rules configured via theMobiControl Manager. Deployment Servers also make real-time information about devices available to MobiControl Manager sessions.

MobiControl Deployment Servers provide the following key features:

- **Executing device configuration rules** to automatically configure devices to work with MobiControl.
- **Executing deployment rules** that deploy packages to mobile devices.
- **Providing real-time information** from devices to MobiControl Manager.
- **Fault tolerance** automatically distributes the load among available servers a particular server is not available. All devices connected to an unavailable server will automatically migrate to available servers.
- **Load balancing and scalability** automatically distributes the load among running Deployment Servers when more than one is configured.

Please see the "Deployment Server Configuration" topic on page 386 for more information on managing and configuring MobiControlDeployment Servers.

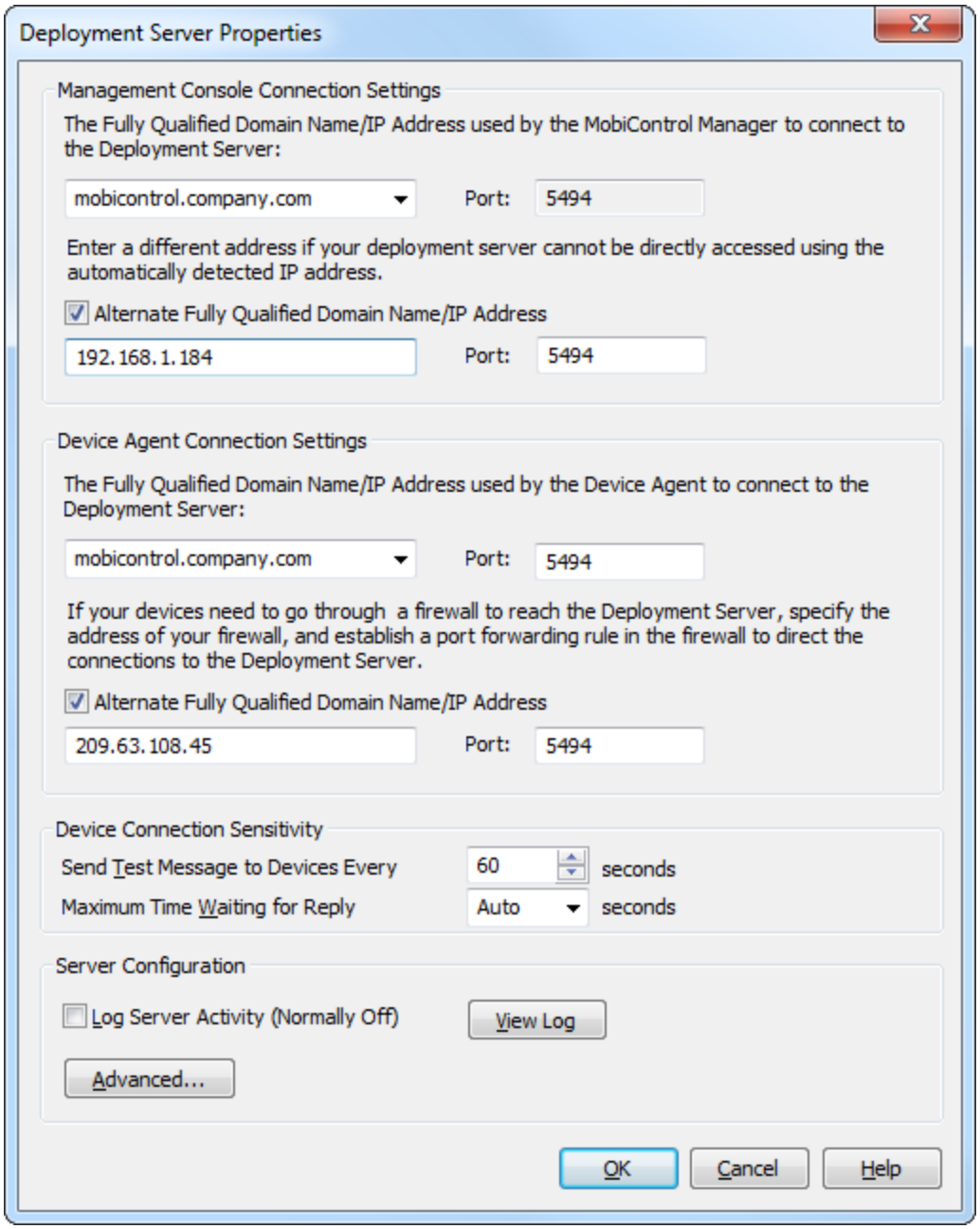
Adding Multiple Deployment Servers to an Installation

Only one Deployment Server is required in an installation of MobiControl, however, you may choose an implementation using multiple Deployment Servers for any of these reasons:

- **Fault tolerance**
- **Scalability**
- **Network optimization:** For network topologies where a large number of mobile devices at different physical locations have a low-bandwidth connection to the central server, system performance can be improved by installing additional Deployment Servers at the remote locations. This results in lower office-to-office network traffic by allowing the remote devices to connect to regional servers instead of the central server.

Setting Deployment Server Properties

To set Deployment Server properties, select the icon for a particular Deployment Server in the Deployment Servers view (tab) and select the **Server Properties** option from the **Deployment Server** menu. The **Deployment Server Properties** dialog box will be displayed.

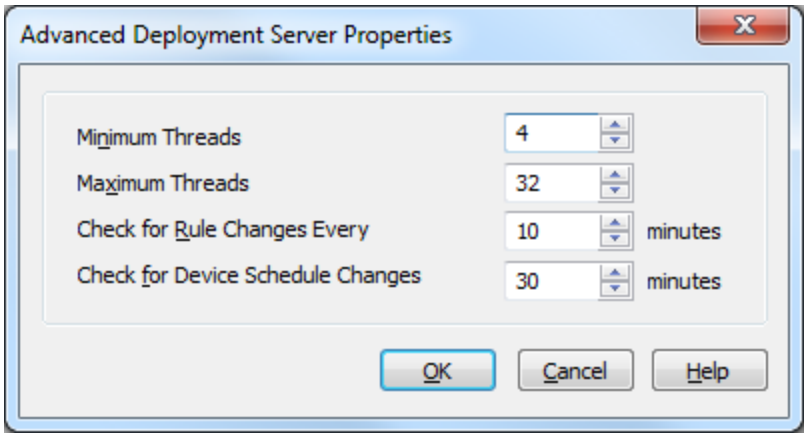


Deployment Server Properties dialog box

Server configuration and device connection sensitivity settings can also be changed through the Deployment Server system tray applet. Please see the "Deployment Server Configuration" topic on page 386. The table below describes each field of the **Deployment Server Properties** dialog box:

Field Name	Description
Management Console Connection Settings	This is the IP address or hostname used by the management console to connect to the Deployment Server to receive real-time updates. The Deployment Server automatically reads the default IP address assigned to the host computer upon which it is running. If you wish to change this IP address, select **Override automatically detected IP address.** You may also specify an alternate server address in situations where the device will need to use a different IP address when connecting to a certain IP network. This option is also useful when you need to move the from one host computer to another.
Device Agent Communication Settings	This is the Fully Qualified Domain Name (i.e. Hostname)/IP address used by devices to connect to the Deployment Server to receive updates and facilitate remote control. By default, this address is the same as the management address. In situations where mobile devices need to go through a firewall or proxy server the devices may need to use external addresses for Deployment Servers that get mapped by the firewall or proxy server to the private network address. **NOTE:** We recommend you to specify a DNS resolvable hostname instead of a static IP address as the DNS resolvable hostname is less likely to change. When MobiControl Device Agent software is generated, the server address for device communication is injected into the generated Device Agents. If you need to change the external IP address, you need to do this before you generate a Device Agent for new devices. For devices that are already connected to the Deployment Server, these settings are refreshed on the devices when they reconnect to the server. You may also specify an alternate server address in situations where the device will need to use a different IP address when connecting to a certain IP network. This option is also useful when you need to move the MobiControl Deployment Server from one host computer to another. When external addresses are configured, MobiControl Device Agents will try to connect to the Deployment Server using one of the addresses. If multiple addresses are configured, the set Deployment Server priorities will be used to determine which Deployment Server an agent should try to connect to. Please see the "Deployment Server Priority" topic on page 167 for information on Deployment Server priority configuration. **Devices connecting through a proxy** If the Device requires proxy access to the Internet in order for the device agents to connect to the Deployment Server you can use the following settings in the Device Agent Connection Field: **www Proxy:** http://<Username>:<Password>@<Proxy Server>:<Proxy Port>/<Deployment Server Address>:<Deployment Server Port> **Socks Firewall/Proxy:** socks://<Username>:<Password>@<Proxy Server>:<Proxy Port>/<Deployment Server Address>:<Deployment Server Port> or socks://<Proxy Server>:<Proxy Port>/<Deployment Server Address>:<Deployment

Field Name	Description
	Server Port>
Send Test Message to Device Every	This setting is used to control how often the Deployment Server is to send test message to device. MobiControl Deployment Servers send test messages (approximately 32 bytes) to devices periodically and then wait for the device to send the message back. If a Deployment Server does not receive a test message back within a specified time, it concludes that the connection is not functioning properly, and closes the connection to the device. For slow connections or situations where you are being charged based on your amount of data you send through the network (e.g. some cellular data plans) we recommend that you set the Deployment Server's **Send Test Message to Devices Every** setting to at least 180 seconds.
Maximum Time Waiting for Reply	This setting is used to control how long the Deployment Server will wait for the reply from the device.
Log Server Activity (Normally Off)	If this box is checked, the Deployment Server will start verbose logging. This may result in slowing down the response time problems, and working with SOTI support staff. Select the **View Log** button to display the debug log for the Deployment Server. This log provides useful information when diagnosing potential problems with technical support.



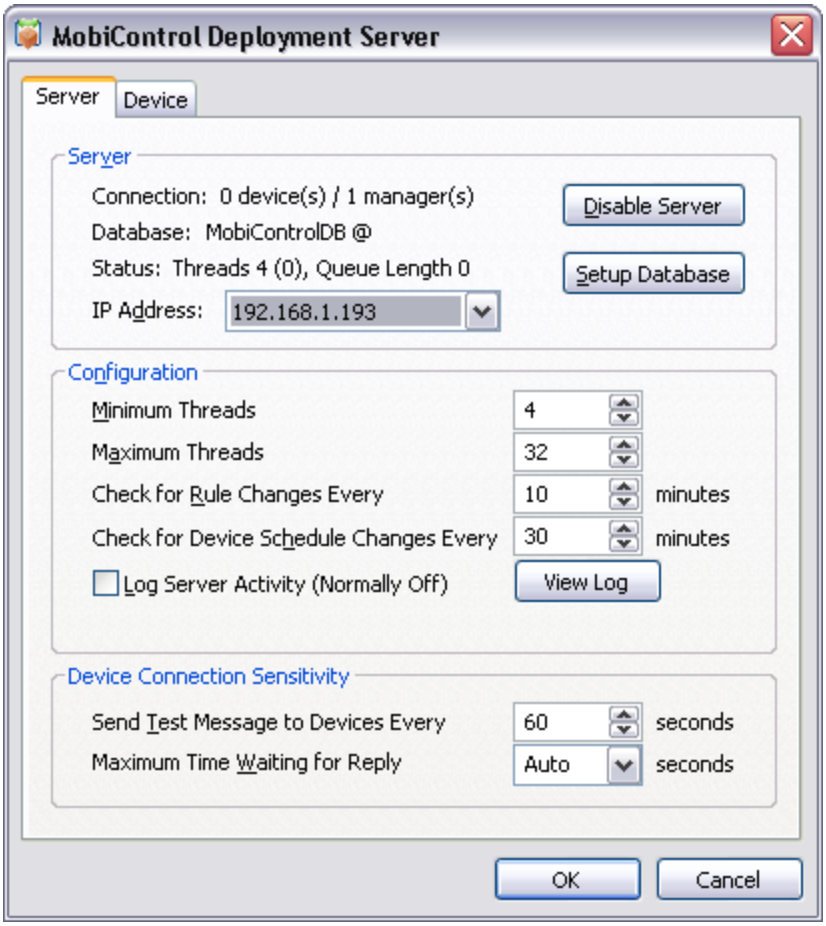
Advanced Properties dialog box:

Field Name	Description
Minimum Threads	Allows the user to set the minimum number of service threads. This value is 2 times the amount of processor cores available on the Deployment Server.
Maximum Threads	Allows the user to set the maximum number of service threads. This value is 16 times the amount of processor cores available on the Deployment Server.
Check for Rule Changes Every	This setting is used to control how often the Deployment Server is to check the database for changes to rules.
Check for Device Schedule Changes Every	This setting is used to control how often the Deployment Server is to check for device schedule changes.

Configuring a Deployment Server

Deployment Servers can be configured using the Deployment Server system tray applet. To access the applet, right-click the **Deployment Server** icon in the system tray, then select **Administration**.

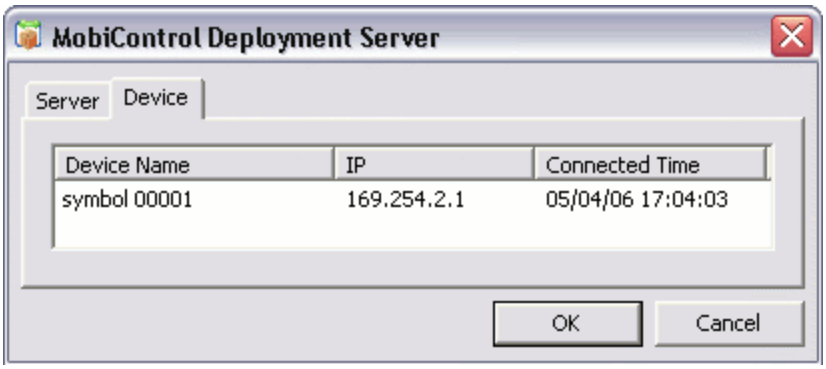
MobiControl Manager also provides a complete set of tools to remotely configure and manage Deployment Servers. Please see the "Deployment Servers View" topic on page 380.



Server tab

Configuration and Device Connection Sensitivity settings can also be changed from the **Deployment Server Properties** dialog box. Please see the "Set Deployment Server Properties" topic on page 383. The following table describes each field of the **Server** tab:

Field Name	Description
Enable/Disable Server	This is a toggle button for enabling and disabling servers. You can enable or disable Deployment Servers by clicking on this button. If you disable a Deployment Server all devices connected to that server will be disconnected. If other servers are available the devices will automatically connect to other available servers.
Setup Database	To change the database settings click on this button. Please see the "Database Configuration" topic on page 463 for more detailed information.
Connection	This field shows the number of devices and the number of MobiControl Managers currently connected to the Deployment Server.
Database	This field shows information about the configured database.
Status	Shows the status of the Deployment Server.
IP Address	This setting is used when more than one network card is installed on the system. It allows the user to select IP address of the Deployment Server.
Minimum Threads	Allows the user to set the minimum number of service threads. This value is 2 times the amount of processor cores available on the Deployment Server.
Maximum Threads	Allows the user to set the maximum number of service threads. This value is 16 times the amount of processor cores available on the Deployment Server.
Check for Rule changes Every	This setting is used to control how often the Deployment Server is to check the database for changes to rules.
Check for Device Schedule Changes Every	This setting is used to control how often the Deployment Server is to check for device schedule changes.
Log Server Activity (Normally Off)	If this box is checked, the Deployment Server will start logging its activities to a file. This may result in slowing down the response time of the Deployment Server. This setting should only be enabled when tracking problems, and working with SOTI support staff.
Send Test Message to Device Every	This setting is used to control how often the Deployment Server is to send test message to device. MobiControlDeployment Servers send test messages (approximately 32 bytes) to devices periodically and then wait for the device to send the message back. If a Deployment Server does not receive a test message back within a specified time, it concludes that the connection is not functioning properly, and closes the connection to the device. For slow connections or situations where you are being charged based on your amount of data you send through the network (e.g. some cellular data plans), we recommend that you set the Deployment Server 'Send Test Message to Devices Every' setting to at least 300 seconds.
Maximum Time Waiting for Reply	This setting is used to control how long the Deployment Server will wait for the reply from the device after sending it a test message or a request.



Device tab

The **Device** tab shows the devices that are currently connected to the Deployment Server. The fields on this tab are described below:

Field Name	Description
Device Name	The name of the device
IP	The IP address of the device
Connected Time	The date and time when the device last connected to the Deployment Server

Adding or Removing a Deployment Server

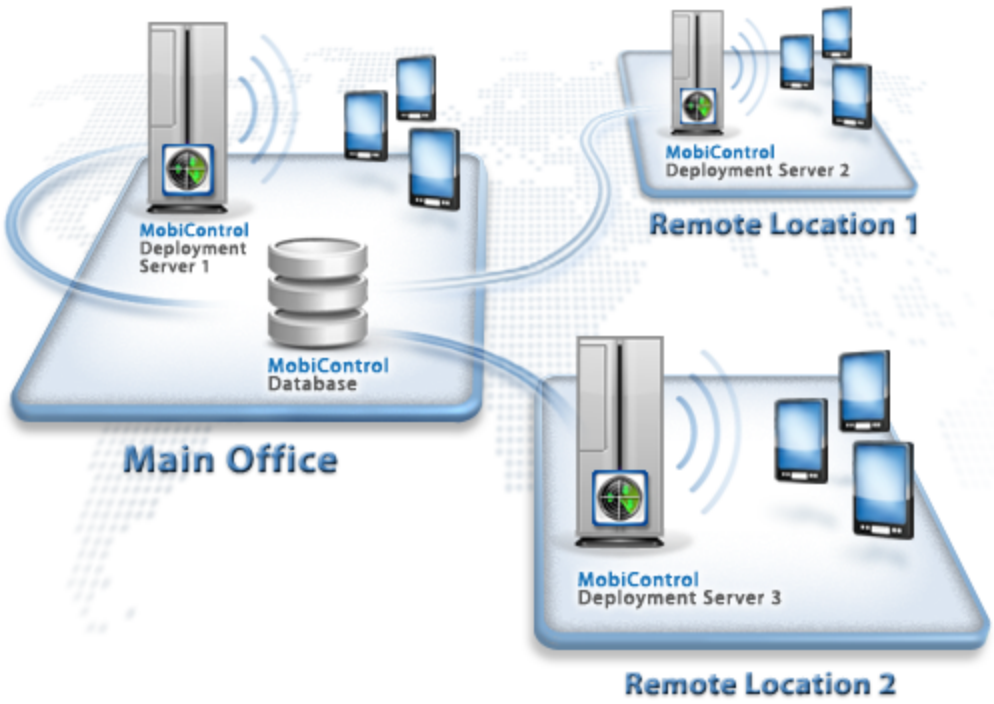


Diagram of a multi-Deployment Server environment

Adding a Deployment Server

To add a Deployment Server, install the MobiControl solution on the workstation or server you want to install the Deployment Server on and follow the instructions on the "Installing MobiControl" topic on page 465. You need to select the option for **Custom Installation** during the MobiControl setup and select only the **Deployment Server** component if you want the machine to solely act as a Deployment Server and not a management workstation. Also, you must direct the new Deployment Server to the same existing MobiControl database that the primary installation is using.

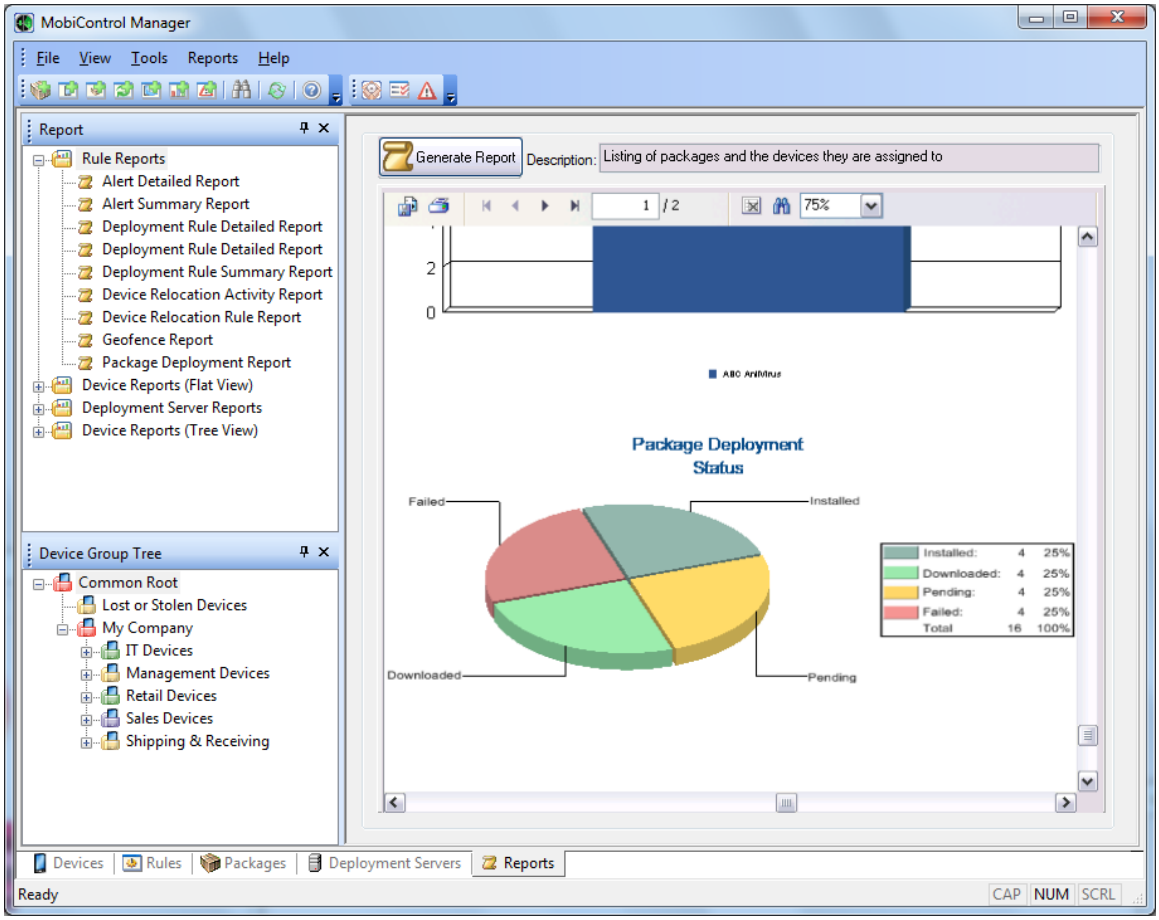
After completing the above, the Deployment Server will automatically be acknowledged by all the other Deployment Servers and be visible in the MobiControl Manager. However, by default, new servers are set to priority one for all devices. (Please see the "Deployment Server Priority" topic on page 167 for more details.) If you wish it to be a lower priority to certain device groups, you must change it using the MobiControl Manager.

Removing a Deployment Server

In the Deployment Servers view (tab) in MobiControl Manager, shut down the server. After the server has been shut down, select **Delete** in the drop-down menu. However, if the server restarts for any reason, it will be added back, so the deleted server should be uninstalled as soon as possible after its deletion for permanent removal.

Reports View

MobiControl includes an advanced reporting engine—Crystal Reports—that gives detailed information about all aspects of system operation. The product includes a set of canned reports that provide information about key areas of system operation. Reports can also be customized as well as new reports can be created and added to the system as needed.



MobiControl Manager Reports view (tab)

Report Types

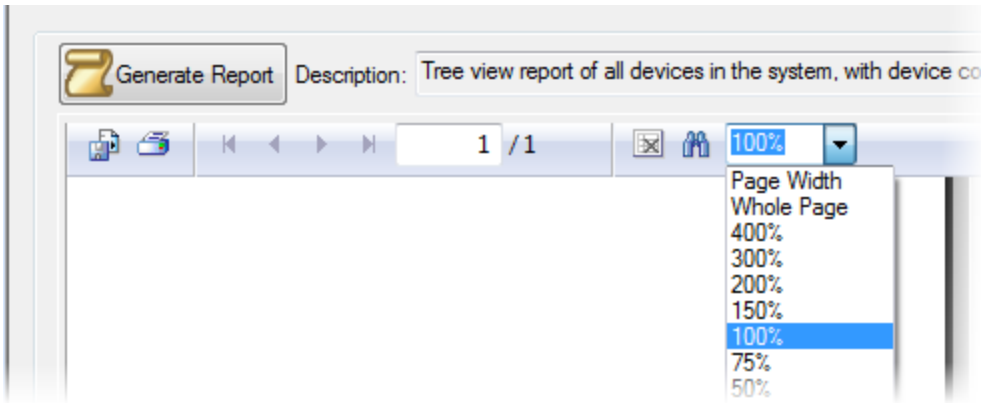
The following reports are included with MobiControl:

- A **deployment server activity report** is a detailed report for deployment server activity over a specified time period.
- A **deployment rule report** is a detailed report of deployment rules and all devices.
- A **Battery and Storage Report** is a detailed report of the battery and storage of the selected devices.
- A **Cellular Signal Strength Data Report** is a detailed report of the cellular signal strength of the selected devices.
- A **deployment rule summary report** is about deployment rule exceptions, showing how many devices have executed the rule successfully, are pending, or have encountered an error.
- A **Deployment Server activity report** is a detailed report of Deployment Server activity over a specified time period.
- A **device activity report** provides information about the device activity during a specific time period.
- A **device custom data report** provides information about devices with the custom data values of selected custom data fields.
- A **device note report** provides information about the notes for your devices.
- A **device package report** provides information about packages installed on your device.
- A **device program report** provides information about all the programs installed on your devices.
- A **device relocation rule report** provides information about all the relocation rules for your devices.
- An **out of contact devices report** provides information about devices that have not connected to the system since the specified date.
- A **package deployment report** provides information about package deployment.
- A **Location Collected Data Report** is a detailed report of the location data collected for the devices.
- A **Connectivity Information Report** is a detailed report regarding device's connectivity.
- A **Device Tree Report** provides information about the device tree structure.
- A **Device Tree with Virtual Groups Report** provides information about the device tree structure along with the virtual groups.
- A **Log Information Report** provides information about the device logs.
- A **Phone Number Report** provides information about the phone number of devices.
- A **Alert Summary Report** provides summary of the alerts.
- A **deployment rule report** is a detailed report of deployment rules and all devices.
- A **Geofence Report** provides detailed report based on the Geofence.
- A **Uninstalled Mandatory Applications Report** provides information about the mandatory application not installed on the devices.

Generating a Report

1. In MobiControl Manager, select the Reports view (tab).
2. Select a report in the left pane of the Reports view (tab).
3. Click the **Generate Report** button.

4. For some reports, a window will appear requesting additional parameters (e.g. time period) that may be required.



MobiControl Manager Report toolbar view

Saving a Report

1. Generate a report.
2. On the report screen, click the **Export Report** button. (It is the first icon in the toolbar, beside the **Print Report** button.)
3. Select the desired file type. Available file types are:
    - Adobe PDF (`.pdf`)
    - Crystal Reports (`.rpt`)
    - HTML 3.2/4.0 (`.html`)
    - MS Excel 97-2000 (`.xls`) or Data only (`.xls`)
    - MS Word editable RTF (`.rtf`)
    - ODBC
    - Record-style (columns of values with or without spaces) (`.rec`)
    - Report definition (`.txt`)
    - Rich text format (`.rtf`)
    - Comma-separated values (`.csv`)
    - Tab-separated text (`.ttx`)
    - Text (`.txt`)
    - XML (`.xml`).

4. Select the location to which you want to export the report. The options available are:
    - Application
    - Disk file
    - Exchange folder
    - Lotus Domino
    - Lotus Domino Mail
    - MAPI (Messaging Application Programming Interface)

Printing a Report

1. Generate a report.
2. On the report screen, click the **Print Report** button. (It is the second icon in the toolbar, beside the **Export Report** button.)
3. The print menu will pop up. Select the desired printer and the report will be printed there.

Generating Custom Reports

It is possible to create custom report files on any available statistic you desire. The Deployment Server database is a standard SQL database and can be queried by writing a custom query. Also, it is possible to create additional reports that are built into MobiControl. For more details, please contact us.

Other Tools

These other tools are available through the toolbar:

- The **Stop Loading** button stops the report generation process.
- **Refresh** regenerates the report. If parameters were required to generate the original report (e.g. time period), a window will appear requesting the additional parameters.
- The **Search Text** button searches the body of the report for a specified text string.
- The **View Zoom** field allows the user to select view magnification, page width, and whole page views.

MobiControl Tutorial

This is the last step of the MobiControl Tutorial. We hope you feel comfortable with MobiControl!

Windows Mobile Device Configuration Applet

The mobile device configuration applet allows various device-side settings to be configured directly on the mobile device.

Accessing the Mobile Device Configuration Applet

Windows CE Users

The configuration applet can be accessed on the mobile device, from the Control Panel (Click **Start**, then **Settings**, and then **Control Panel**.), or from the **MobiControl** tray icon. If the tray icon is enabled by the administrator for the device, you can bring up the configuration applet by tapping on the **MobiControl** tray icon and then selecting **Configure** from the pop-up menu.

Windows Mobile 2003, 5.0 and 6.x Users

The configuration applet can be accessed on the mobile device, from the **Settings** panel (Click **Start**, then **Settings**, click the **System** Menu, and then click the **MobiControl** icon.), or from the **MobiControl** tray icon. If the tray icon is enabled by the administrator for the device, you can also bring up the configuration applet by tapping on the **MobiControl** tray icon and then selecting **Configure** from the pop-up menu.

NOTE:

If you have just installed the MobiControl Device Agent onto your mobile device and you do not see the MobiControl Device Agent applet icon in the control panel window, you may need to reboot your mobile device for this icon to become visible.

Windows Mobile Smartphone Users

The configuration applet can be accessed on the mobile device through the **Start** menu, and then clicking the **MobiControl** icon.

Windows 2000/XP/Vista/7 PC

The configuration applet can be accessed on the PC from the **MobiControl** tray icon on the desktop taskbar. If the tray icon is enabled by the administrator for the PC, you can bring up the configuration applet by double-clicking on the **MobiControl** tray icon and then selecting **Configure** from the pop-up menu.

MobiControl Device Agent Configuration Menus

The configuration applet contains several menus: **Main Applet menu, Status menu, Events menu, Options menu, Packages menu, Servers menu, Certificates menu** (applicable to devices that support `.pfx` files). The functions on all of the menus are the same for all versions of Windows (The following screenshots may look different from another device's screen, depending on the operating system version).

Main Applet menu

NOTE:

Windows CE, Pocket PC 2000/2002/2003 and Windows Desktop device applet will be displayed in a tabbed format.

This menu contains general Device Agent information and the agent connection button. From this Main Applet page, you can access the other menu windows by clicking the Menu button on the bottom right corner and then selecting **Configuration**.

Option	Description
Status	Indicates whether or not the device is presently connected to a Deployment Server.
Connect/Disconnect	Select this button to establish or terminate the connection between the device and the Deployment Server. When connected, the device appears "online" in the management console, making it available for remote control.

Status Menu

This menu displays the status of the.

Option	Description
Agent Version	This displays the version of the Device Agent running, in format of (major version).(minor version).(build number).
IP Addresses	These are the IP address(es) the device has been configured, either static IP addresses or DHCP IP addresses.
MAC Address	This is the hardware MAC (Media Access Control) address of the device's network adapter.
Network (SSID)	This field shows the SSID of the wireless network to which the device is connected (if applicable).
Main Battery	This field displays the devices battery status.
Device ID	This field contains the unique identifier of the device in MobiControl system. The Device Agent automatically populates this field.
Device Name	This field shows the current device name used by MobiControl. MobiControl names devices based on the naming convention chosen when the agent was configured using the Device Agent configuration tool.
Remote Control	This field displays the status of the remote control connection.
MobiControl	This field displays the status of the MobiControl server connection.
Last Connect Time	This displays the last time the device was connected to the MobiControl server.

Events Menu

The **Events Menu** displays all the recent events that occurred on the device.

Options Menu

The **Options Menu** displays the information of the Device Name and Device Agent configuration options.

Option	Description
Allow Inbound Connections	Enable the agent to listen and accept inbound TCP/IP remote control connections. When unchecked, you can remote control this device through "Remote Control Device via TCP/IP (SERVER)," but you cannot remote control this device by through "Remote Control Device via TCP/IP (DIRECT)."
Log to file	This option should normally be unchecked. It should only be used when problems occur, the log file produced can then be supplied to our support team.

Packages Menu

The **Packages Menu** displays the information of all the installed packages.

Servers Menu

The **Servers menu** allows all the Deployment Server options to be configured.

Option	Description
Host	The host/IP and port number of the Deployment Server
Priority	The priority of the servers over other servers
Add	Adds an IP address/port and sets the priority of a new Deployment Server
Edit	Allows the modification of an already added Deployment Server
Del	Deletes the selected Deployment Server entry
Test	Tests the connection between the device and the selected Deployment Server

The agent uses the server list to find out and connect to the Deployment Server. It starts from the server which has the highest priority. If failed, then it randomly picks up another server which has the same priority and retries. If all the servers which have the same priority are not available, then the agent tries the servers which have a lower priority, and repeats these steps until a Deployment Server is successfully connected.

Number one is the highest priority, number two is the second highest priority, …, and number 5 is the lowest priority. When making changes to the server list, keep in mind that the priority numbers of the servers should be consecutive.

Certificate Menu (Windows Mobile 5, 6.x and Windows PC devices only)

The **Certificate** Menu allows the user to import a `.pfx` file that contains a certificate and private key that enables it to communicate with the Deployment Server using the SSL protocol.

The user must specify the location of the file to be imported, and then provide the password that was entered when the `.pfx` file was originally exported from MobiControl.

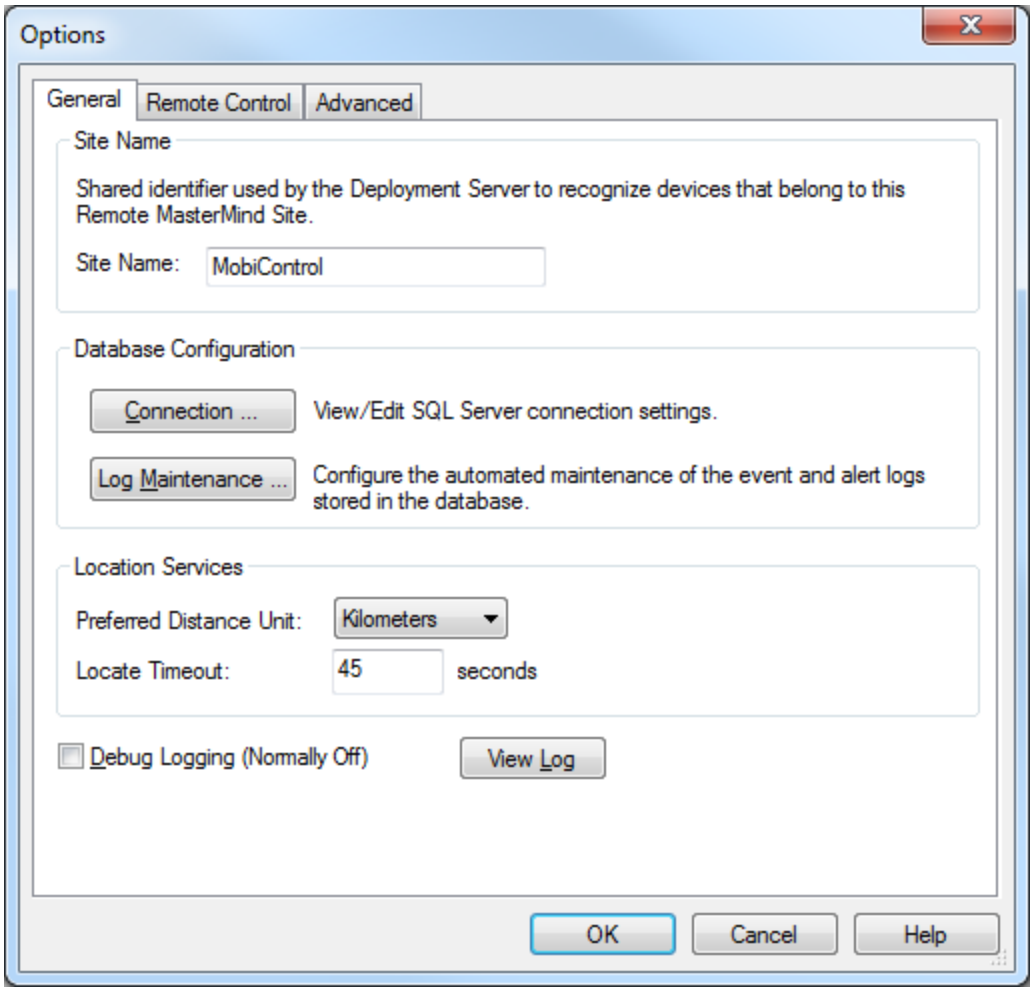
Configuring MobiControl Manager

The **MobiControl Manager Options** dialog box allows you view and configure various MobiControl settings such as the MobiControl site name, MobiControl database connection and remote control settings.

Access this dialog box from the MobiControl Manager by clicking **Tools,** and then clicking **Options.**

General

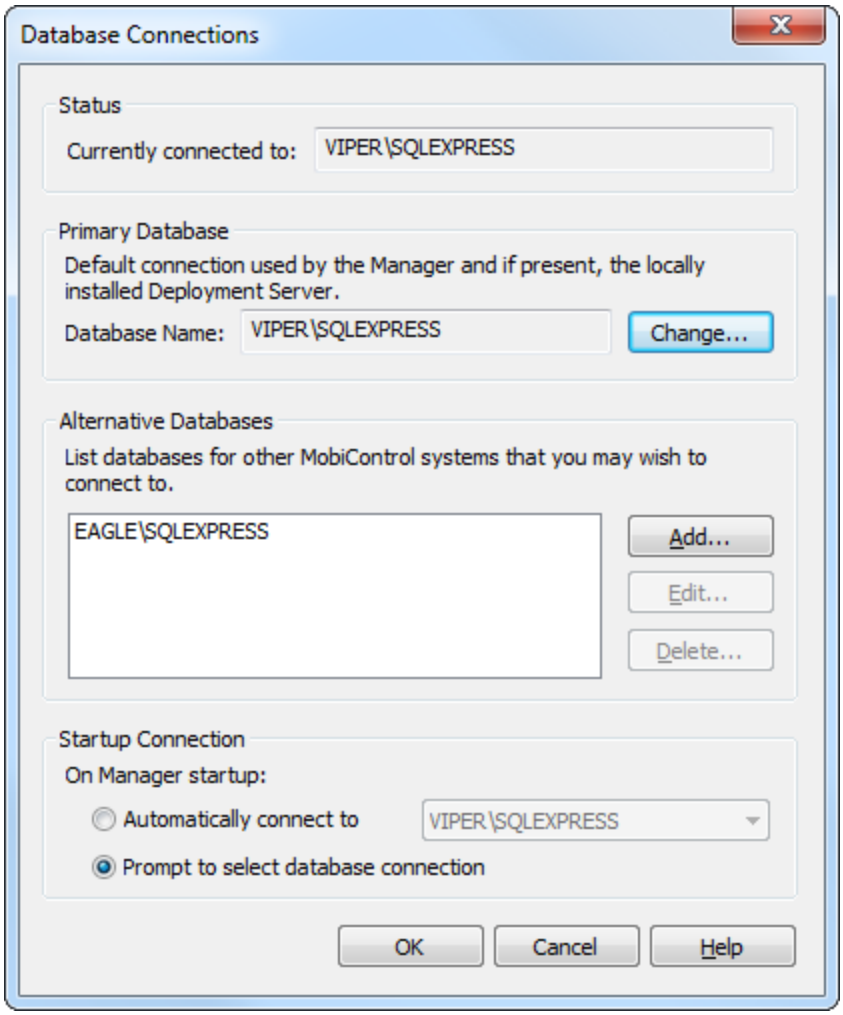
This page allows you to change the MobiControl site name, and the MobiControl database connection.



General options tab

The table below describes the fields in the General Options Page.

Field Name	Description
MobiControl Site Name	In situations where there are multiple MobiControl installations in a single facility, this field can be set to a unique name for each installation. In this way, MobiControl Deployment Servers from one installation will not respond to devices that are being managed by another installation. The site name configured here gets injected into the Device Agent software created by a particular installation. When a MobiControl Device Agent connects to a Deployment Server and the site name supplied by the device does not match, the connection is terminated and then logged. The site name is also used by mobile devices to automatically discover the new IP address of a Deployment Server when the Deployment Server address is changed.
Configure Database Connection	The MobiControl database connection is configured by the installation program but can be modified by clicking on this button. Please see the "Database Configuration" topic on page 463 for more information about configuring the database connection.
Log Maintenance	This tool brings up the options for logs maintenance. Please see the "Log Maintenance Options" topic on page 406.
Location Services	The Preferred Distance Unit allows you to change the unit of speed that is displayed when tracking or locating a device in the Location panel. The Collected Data panel will continue to show speed in knots regardless of this setting. Locate Timeout defines the amount of time, in seconds, that MobiControl should wait for a response from the GPS on the device. The default value is 45 seconds.
Debug Logging (normally off)	If this box is checked, the MobiControl Manager will start logging its activity into the `MCManager.log` file in the program directory. This setting should only be enabled when tracking problems and working with SOTI support staff.



The table below describes the Database Connections Settings.

Field Name	Description
MobiControlStatus	This shows the Database that the Manager is currently connected to.
Primary Database	This shows the default Database that the Manager will connect to. A different Database can be selected by clicking the change button.
Alternative Databases	This allows you to add a new Databases, Edit existing Databases and delete Databases that the Manager will connect to.
Startup Connection	The user can select which Database the Manager will automatically connect to at startup or alternatively have the Manager prompt to select a Database to connect to.

Remote Control Settings Page

You can create multiple connection profiles to connect to devices with different connection options. The installation program automatically adds profiles with typical connection options. You can customize the settings in these profiles, or add or delete profiles as necessary.

To add a new connection profile, click the **New** button. This will cause the **Connection Properties** dialog box to be displayed. (Please see the "Configure Remote Control Connection Profile" topic on page 403 for more information.)

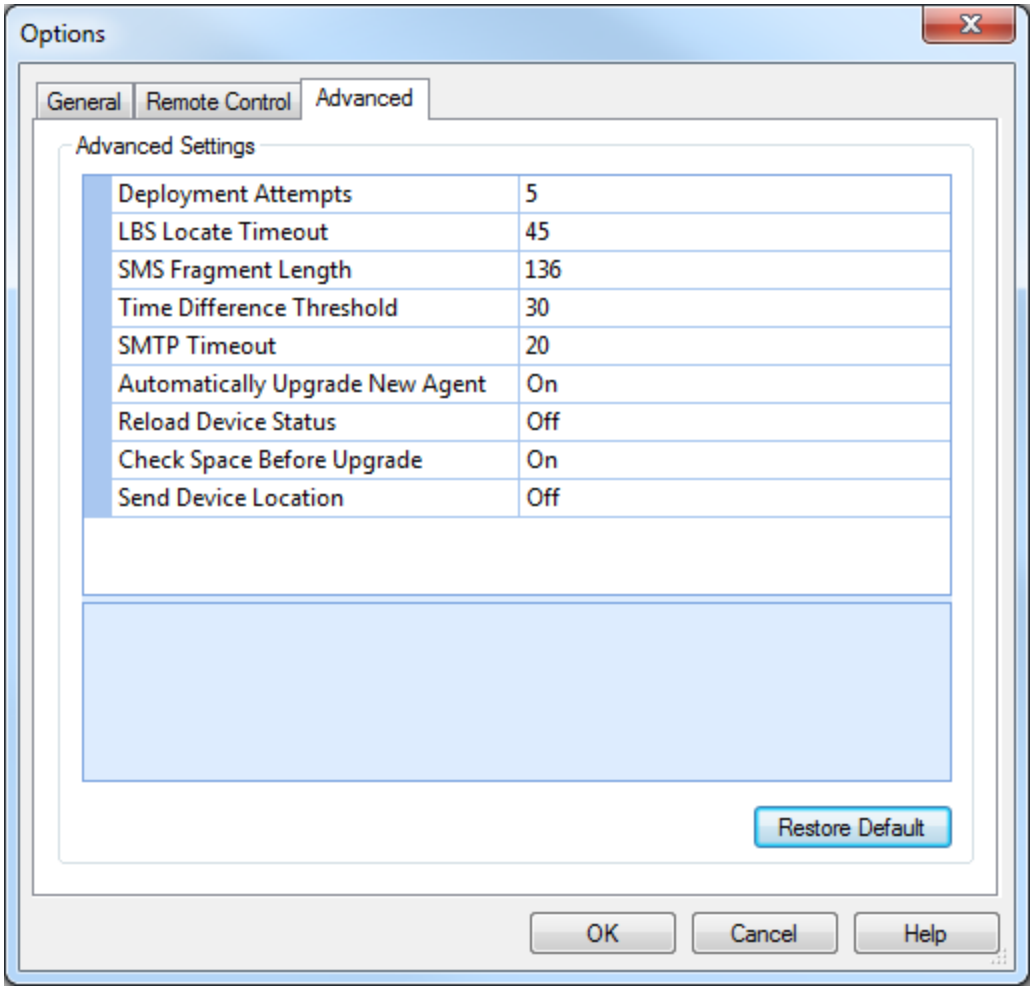
To edit a profile, select the profile you wish to edit from the list and then click the **Edit** button. This will cause the **Connection Properties** dialog box to be displayed. (Please see the "Configure Remote Control Connection Profile" topic on page 403 for more information.)

To delete a profile, select the profile you wish to delete from the list and then click the **Delete** button.

To prompt a device user to accept incoming remote control sessions, check the **Prompt device user to accept remote control session** box. This setting is not enforced on manager users and can easily be switched off. If you wish to enforce this option on manager users, please enable user security and set the appropriate permissions. (Please see the "Manager Console User Security" topic on page 409 for more information.)

Advanced Settings

The Advanced Settings tab provides control and configuration for various undetected settings within the MobiControl management console.



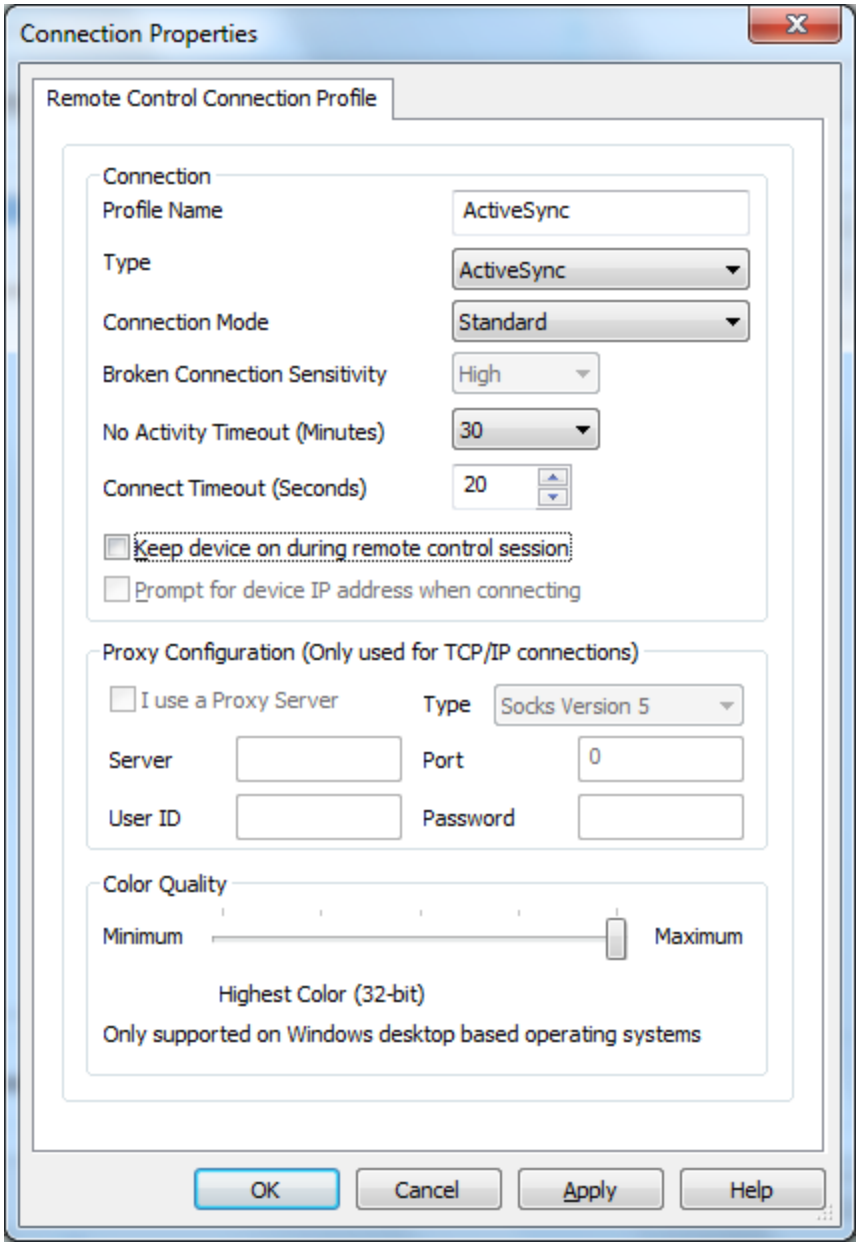
Advanced Options tab

The table below describes the fields in the Advanced Options Page.

Field Name	Description
MobiControl Deployment Attempts	This entry determines the maximum number of attempts to deploy a package.
LBS Locate Timeout	This entry specifies the length of time the manager should give devices to satisfy locate and track requests (in seconds). Note that a device that times out while tracking does not leave tracking mode. This setting is the length of time for which it will turn on the GPS radio. Thus, the setting has no effect on devices tracked with the 'leave GPS radio on continuously' option checked.
SMS Fragment Length	This entry determines the length of the SMS messages sent. The default value for this entry is 136. Some wireless carriers may enforce a shorter SMS character limit. In this case, the SMS fragment length will need to be adjusted to be able to correctly send scripts over SMS.
Time Difference Threshold	This entry determines the threshold value in minutes for the Deployment Server to compare its time with the devices. When a device connects, MobiControl gets its time (UTC) from a snap-shot and compares it with the date/time of the Deployment Server (UTC). If the time difference is found to be more/less than x minutes - where x minutes is specified in this field then a warning LOG message is added to the InstallLog for the specified device.
SMTP Timeout	The timeout value for the SMTP server.
Automatically Upgrade New Agent	This entry determines if the system will upgrade any newly added devices using an old version of the device agent.
Reload Device Status	Setting this entry to 'On' will instruct the Deployment Server to broadcast to all connected Managers to reload device information from the database when devices come online, otherwise devices will be updated using the information delivered by the Deployment Server.
Check Space Before Upgrade	This entry determines if a free space check is necessary before upgrade. The total size needed is calculated by adding all the size of the download files, the free space is taken from the snapshot, if snapshot doesn't contain the info then MobiControl will take it from the database. If it doesn't have enough free space, MobiControl will log 'Insufficient free space on device (Updating Agent)'.
Send Device Location	Setting this entry to 'On' will enable a macro on the device allowing it to collect and store the devices location in the device tree of the management console. The macro **%MCDEVICELOCATION%** can be added to the Lockdown Menu to display this information to the user.

Configuring Remote Control Connection Profiles

The **Remote Control Connection Profile** dialog box is used to edit the specific attributes of a connection and to create new connections. To open this dialog box, click **Tools**, then **Options**, then select the **Remote Control** tab. Select the connection profile you wish to edit or create a new profile by clicking the **New** button.



Connection Properties dialog box

Connection Settings

Here is a list of fields contained within the dialog box shown above with their associated descriptions:

Field Name	Field Description
Profile Name	This field is used to give a connection configuration, a user friendly name. If MobiControl Remote finds that multiple connections have been configured when asked to connect, MobiControl Remote will display the connection names in a list so that you can select the configuration you wish to use.
Type	This field allows the user to configure the type of connection that will be used for remote control sessions. The available connection types are ActiveSync, TCP/IP (Direct), and TCP/IP (Server): • Use the **ActiveSync** option for remote control sessions over ActiveSync connections. The device needs to be docked and connected to the desktop computer via Microsoft ActiveSync. In this case MobiControl will use whatever communication mechanism is being used by ActiveSync to communicate between the computer and the mobile device. ActiveSync connections can be over USB, Serial, USB, Wired/Wireless LAN, Bluetooth or infrared (IR) connections. • A LAN-based wired or wireless **TCP/IP (DIRECT)** connection generally provides the best performance by reducing latency. However, it requires the device to accept the connection without authentication unless SSL Security is enabled. (Please see the "Communication and Connection Security" topic on page 411 for more information.) When set to use TCP/IP, the MobiControl desktop software will open a direct wireless or wired TCP/IP connection to the mobile device (i.e. on TCP port 5494). A LAN-based wired/wireless TCP/IP connection generally provides the best performance. • The **TCP/IP (SERVER)** connection type can be used to establish a remote control session with a mobile devices that does not have a public IP address. When a TCP/IP (Server) remote control session is established, the session is bridged through the MobiControlDeployment Server. (The device connects to the MobiControlDeployment Serveron TCP port 5494 and the desktop MobiControl Remote client connects to the Deployment Serveron TCP port 5494.) Since this connection goes through the Deployment Serverthe performance is generally not as good as a direct TCP/IP connection. For instance, this type of connection needs to be used when the mobile devices are behind a firewall and do not have unique public IP addresses.
Connection Mode	This field is used only for ActiveSync connections. When the connection mode is set to '**Automatic**', MCRemote.exe will first try to establish a TCP/IP connection to the device agent, but if that fails, then MCRemote.exe will instruct the device agent to try and establish a TCP/IP connection to the MCRemote.exe process on the desktop.
Broken Connection Sensitivity	This field is disabled when an ActiveSync connection is being used, and enabled when a TCP/IP connection is being used. If a TCP/IP connection is being used, MobiControl Remote detects broken connections by periodically sending a message to the remote side and then waiting for a response. If the sending side does not receive a response within a specified amount of time it assumes that the connection has been broken and closes the connection. The setting in this field is used to determine how long the sender should wait for a response. For TCP/IP LAN wired/wireless based connections this field can typically be set to **High.** For slower WAN, cellular, serial or modem TCP/IP connections, this field should be set to **Medium** or **Low.**
Connect Timeout (Seconds)	This field allows the user to control the maximum number of seconds to wait for a connection attempt to succeed. You may need to increase the number of seconds that MobiControl Remote will wait for a connection attempt to succeed on slow connections, for fast LAN-type connections, the connection timeout value can be set to a smaller value (e.g. 10 seconds or less) for over slower networks the value may need to be increased

Field Name	Field Description
	(e.g. 25 seconds or more).
Keep device on during remote control session	If checked, the device will be kept on and will not go to suspend mode during remote control session. Keeping the device on will drain the battery more quickly.
Prompt for Device IP Address	If checked, the remote control manager will prompt you for the IP address of the device. It is useful in case you know the IP address of the device and you would like to connect to it while it is offline.

Proxy Configuration Settings

This section allows users who need to go through a local proxy server to get to a mobile device to configure the appropriate proxy server settings. Additionally, this dialog box allows users who are connecting to a remote mobile device over a slow connection such as a modem or cellular connection, to increase the performance of the slow connection by artificially reducing the number of colors used in the remote control session.

MobiControl Remote currently supports Socks4, Socks5, and HTTP tunnelling (i.e. using basic and digest authentication) proxy servers.

To configure MobiControl Remote to connect through a proxy server, follow these steps:

1. Make sure that you select **I use a Proxy Server.** This will enable the other fields that you need to configure.
2. Select the type of proxy server that you are using, currently MobiControl Remote supports: Socks 5, Socks 4, and HTTP Tunnelling.
3. Enter the TCP/IP address and port of your proxy server
4. If the type of proxy server you are using supports authentication, the **User ID** and **Password** fields will be enabled. If you are using authentication, enter the appropriate values into the **User ID** and **Password** fields.

Color Reduction

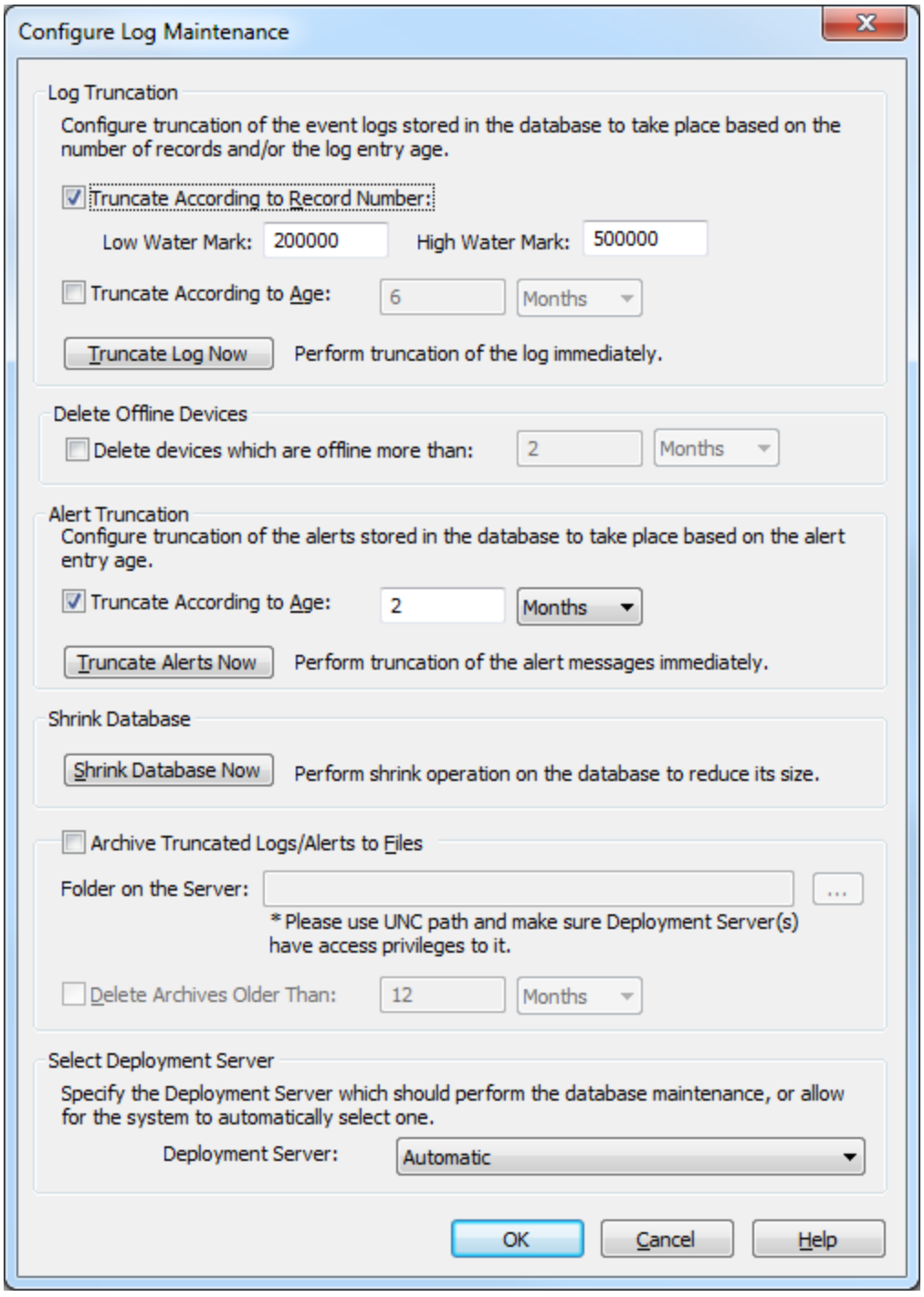
Color reduction can be used to increase performance over slow connections such as cellular, modem or serial connections. The greatest performance increase can be obtained by selecting the setting with minimum color quality, the 2 bit (4-shade grayscale) option. Reducing the number of colors displayed when using a slow connection can increase performance by as much as 75% percent. Although the amount of data transferred will be reduced, CPU usage on the device will increase. Two options with intermediate color quality are 4 bit (16-shade grayscale), and 8 bit (256 color). When connection speed is not an issue, maximum color quality (maximum bit depth) can be selected. This option is the default color quality for the ActiveSync connection profile. For most mobile devices, the normal number of colors displayed is 65535 (16 bit).

Log Maintenance Options

The MobiControl Manager **Log Maintenance Options** dialog box allows the user to view and configure various settings for the event logs generated and stored in the database. Access it from the main Manager console by clicking the **Tools** menu, clicking **Options,** clicking the **General** tab, then clicking the **Log Maintenance** button.

Configuring Log Maintenance

With time, event logs and the database in which they are stored grow in size. If the size of the logs is not limited, they can cause the database to grow substantially and eventually run out of space. In order to avoid such situations, log maintenance is highly recommended. MobiControl comes with options to configure log maintenance to meet the user's requirements. Log Maintenance takes place at midnight. You may see that you are getting access denied errors when creating or editing the log file. In order to avoid access denied errors, you must ensure full permissions are granted to the user creating and updating the log file.



Configure Log Maintenance page

The table below describes the fields in the **Configure Log Maintenance** page:

Field Name	Description
Truncate	The option allows the user to set the record number at which truncation would begin. As

Field Name	Description
According to Record Number	logs are stored in the database, they are stored sequentially in a table and each row in the table has a unique record number. • When the **High Water Mark** is reached, all records up to the low water mark are purged. • The **Low Water Mark** is the limit up to which the records will be truncated.
Truncate According to Age	This option allows the user to control the truncation based on the age of the logs. Once this parameter is set, all logs older than the date specified are deleted from the database.
Truncate Log Now	This option truncates the logs immediately. The truncation is based on the configured water marks and the truncation 'age' threshold.
Delete devices which are offline	This option will delete those devices, which are offline for more than the time specified from the database.
Truncate Alerts Now	This option truncates the alerts immediately according to the truncation 'age' threshold.
Shrink Database Now	This option performs the shrink operation on the database immediately to reduce its size. This option will compress the data in the database using the SQL's standard compression techniques.
Archive Truncated Logs to Files	Users can specify a location on a server or workstation to where the truncated log files will be written. With this option, the user can store the log files outside the MobiControl Database. This can help the user reduce the size of the database.
Delete Archives Older Than	The archived log files, stored at a the location specified in the above field, can be deleted after a set duration. This can prevent the secondary storage location of the logs from running out of space.
Select Deployment Server	This option allows the user to choose which Deployment Server should perform the log maintenance. This option is useful when there is more than one Deployment Server. This way, a Deployment Server with a lower priority can be selected to perform the database log maintenance.

 **NOTE:**

Truncation occurs at Midnight (local time of the Deployment Server), however the Deployment Server truncates records according to the UTC timestamp.

Manager Console User Security

IT administrators in security conscious organizations have roles-based security model(s) implemented to restrict the access to various applications and operations for personnel. The roles often reflect current organizational structures and business groups hierarchy.

When using a powerful, feature-rich mobile device management solution like MobiControl, it may be desirable to limit access to MobiControl's functionality for some individuals or groups of users. For example, for a multi-tier support and help desk team, an organization may want to limit the access of tier-one help desk personnel to the MobiControl Manager while added functionality and features might be available for tier-two personnel.

MobiControl User Access Control

With the introduction of the latest version of MobiControl, you can now use **Integrated User Authentication** with the MobiControl Manager. The new authentication system is very similar to that of Microsoft Active Directory, where a defined Username and Password will be required upon launching the MobiControl Manager, or MobiControl Web Console in-order to manage or support your mobile fleet.

MobiControl Manager Active Directory Security

MobiControl's user security system integrates with the Active Directory and the Windows security system to control access to the MobiControl system and implement existing organizational security structures. The option to allow read-only communication with the LDAP (Lightweight Directory Access Protocol) means that write access to the directory is not required so there is no risk to the directory schema.

NOTE:

You can use both Active Directory users and groups and Basic User Authentication accounts as well.

NOTE 2:

MobiControl console security can only be enabled through the web console. Please see the "Console Security" topic on page 586 for more information.

Communication and Connection Security

For security-conscious organizations that require standards based encryption for protecting data communication, SSL mode can be enabled to secure the communication between the MobiControl Device Agents on the device, the Deployment Servers and the MobiControl Manager consoles have this option enabled by default.

MobiControl's SSL communication mode uses the TLS (Transport Layer Security) v1.2 Cipher Suites of the Secure Channel (SChannel) Microsoft Security Support Provider (SSP), superseding the SSL v 3.0 protocol. These cipher suites are implemented by the Microsoft Enhanced Cryptography Provider that is built into the Windows operating system on top of which the product runs. The encryption meets the requirements specified in the Federal Information Processing Standards Publication (FIPS PUB) for FIPS PUB 140-2 Security Requirements.

The full list of Microsoft cipher suites available with SChannel TLS v1.2 is given below:

TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_RC4_128_MD5
SSL_CK_RC4_128_WITH_MD5
SSL_CK_DES_192_EDE3_CBC_WITH_MD5
TLS_RSA_WITH_NULL_SHA256
TLS_RSA_WITH_NULL_SHA

NOTE:

MobiControl does not support third party certificates (e.g. VeriSign certificates). Support will be added in later versions.

The selection is determined based on the minimum and maximum cipher suite strengths that are defined by the Windows operating system upon which the product runs. The above is the full list of cipher suites that are included with Windows Server 2008.

SSL Configuration for Devices

Right-click on a target device or group in the device tree, click **Configure Devices**, then click **Advanced Settings**. Next, click the **Configure SSL** button and check the box next to **Use SSL Security**. Please see the "Connection Security" topic on page 248 for more information on the SSL options for configuration at the device or group level.

MobiControl Package Studio

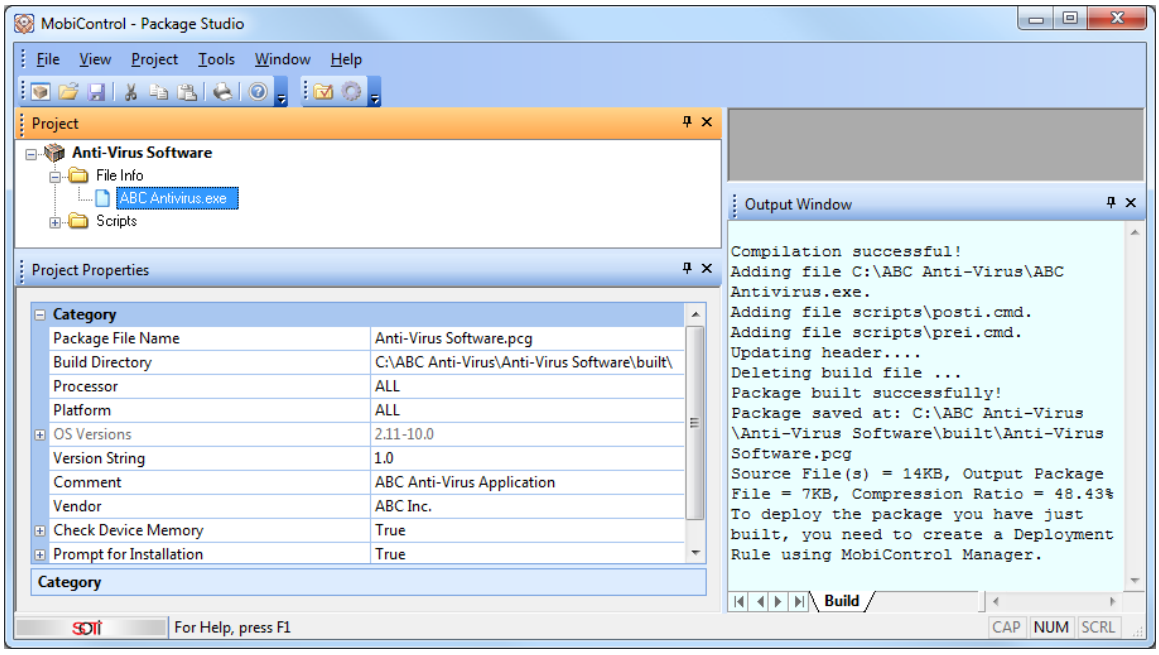
To deploy software or data to mobile devices using MobiControl, you need to package the software or data into a package file. A package is a set of files along with installation instructions that have been compressed into a single file. To create packages, MobiControl has a tool called the Package Studio. Compressed packages allow for faster transmission of software and data over low-speed network connections and also encourage reducing costs for data bandwidth.

You can start Package Studio from the Tools menu in the main MobiControl Manager window, or through the **Start** start menu, **Programs, SOTI, MobiControl,** and then **MobiControl Package Studio.**

In addition to adding regular files into packages, Package Studio also allows users to optionally add scripts to packages. The scripts get automatically executed at pre-defined points in the installation or uninstallation of the package. Using Package Studio, it is also possible to create packages with just scripts (without any software or data files) that execute commands or perform a specific task, and then deploy these packages to devices. Package Studio also includes options to automatically process or execute `.cab`, `.reg` (registry settings), `.exe` (application executables), and other files when they are installed or uninstalled.

Using the **File Properties** dialog boxes for `.cab` files in Package Studio, you can also customize the way `.cab` files are installed on the device. For instance, installing the `.cab` file silently, without prompting the mobile device user for confirmation or the location where the files will be installed.

The blue icon in the left pane shows a file that has been added to the package. The gold icons in the left pane show scripts that have been added to the project. When Package Studio builds projects, it compresses the files in the project as well as the installation rules into a single deployable package file. Package files have the file extension `.pcg`.



MobiControl Package Studio user interface

Creating Packages

To deploy software or data to mobile devices using MobiControl, you need to create a package. A package is a set of files along with installation instructions that have been compressed into a single package file. To create packages, MobiControl includes a tool called Package Studio.

You can start Package Studio from the **Tools** menu in MobiControl or by clicking **Start, Programs, SOTI, MobiControl,** and then **MobiControl Package Studio.**

To create a package using MobiControl Package Studio, follow these steps:

1. Create a package project.

   A package project contains the list of the files to be included in the package, and the file and package installation rules. When a package project is compiled using the Package Studio **Build Package** menu option, a deployable package file is generated. Please see the "Create Package Project" topic on page 415 to learn more about how to create a package project.

2. Add a script (if desired).

   Package Studio allows users to add script to a package to control the installation of the package or to perform advanced operations. Please see the "Add Script" topic on page 423.

3. Add files or delete files (if desired).

   Once you create a project using the Package Studio New Package Wizard, you can add or delete files using Package Studio. To add files using Package Studio, make sure the project is opened, then from the **Project** menu select **Add Files.** To delete a file, select the file in the project tree, and press the **Delete** button. Please see the Please see the "Add Files" topic on page 425, the Add Android APK file page and the "Add Folder" topic on page 426.

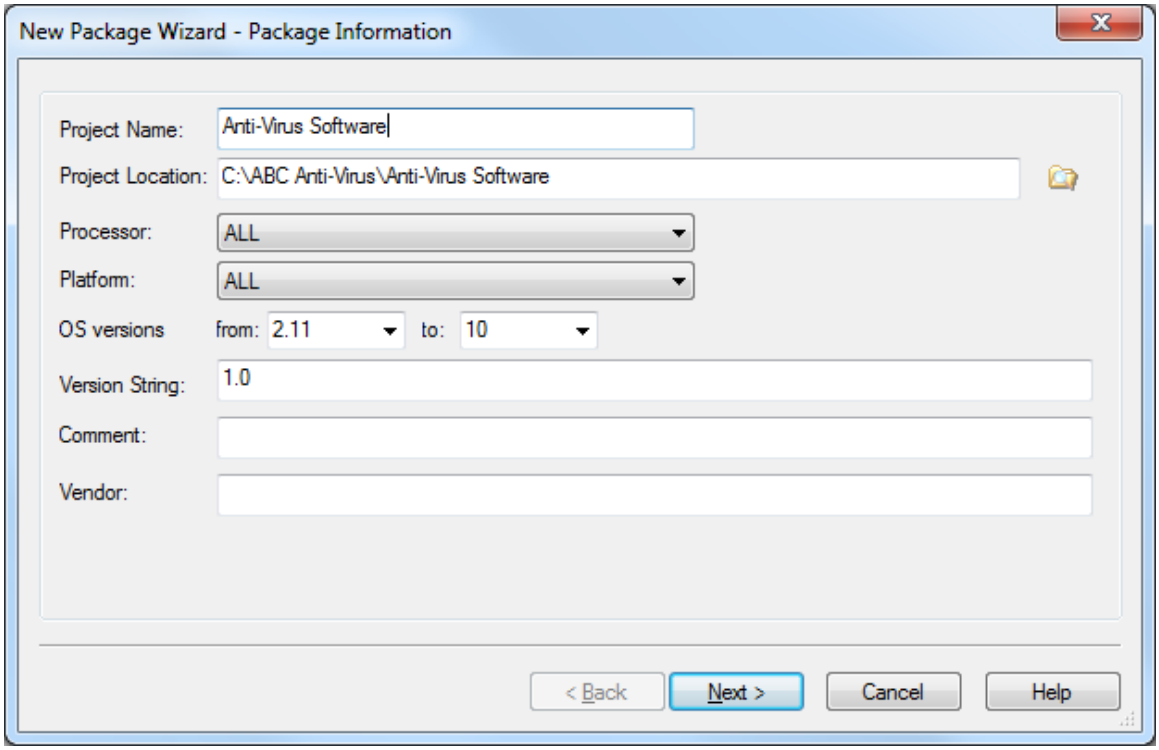
4. Build the project.

   When the project is built, a deployable package file is generated. To build a package project, open the **Project** menu and click **Build Package**. Please see the "Build Project" topic on page 438.

Creating a Package Project

The first step to creating a package is to create a package project. The following steps explain how to use Package Studio to create a package project:

1. From the Package Studio **File** menu, select **Create New Package Project.**

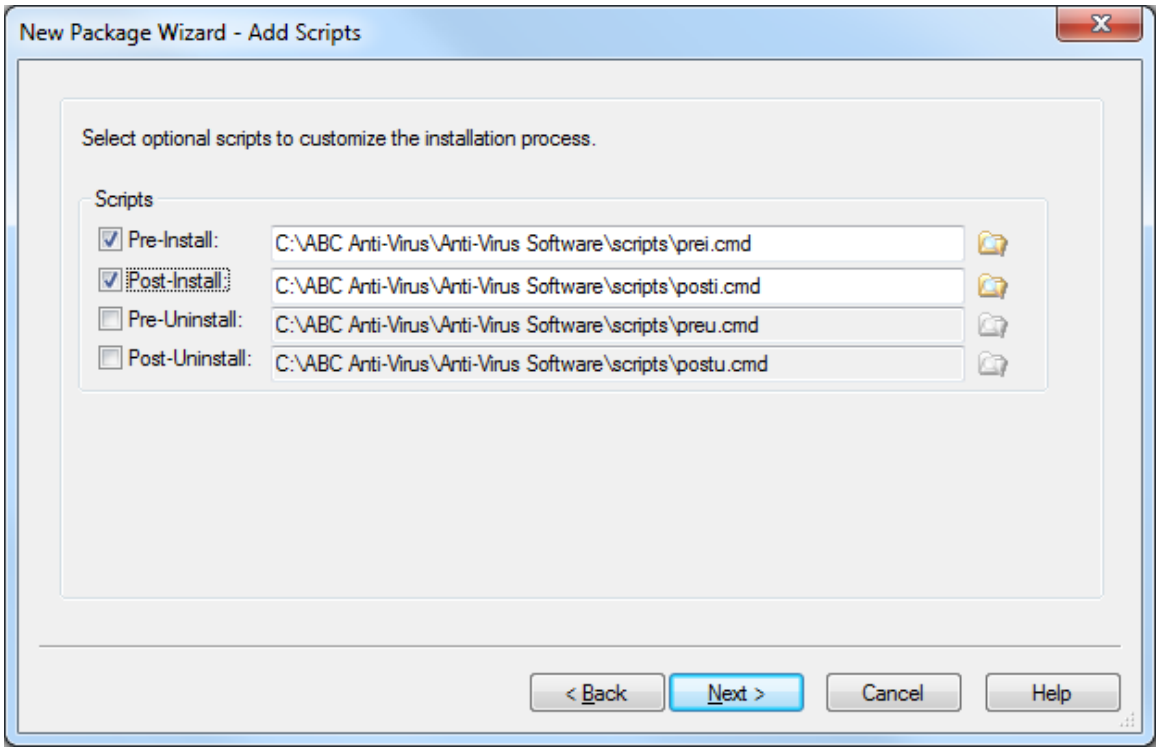


Package Information page

The following table describes the fields in the **Package Information** page of the New Package Wizard:

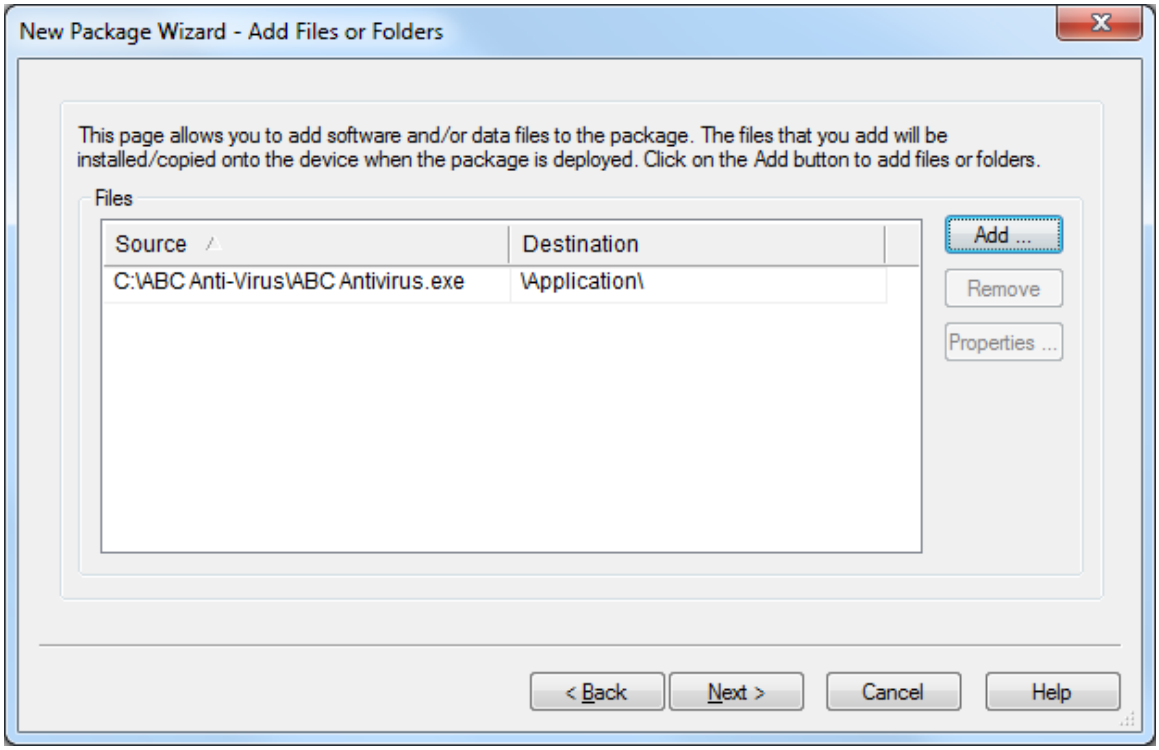
Field Name	Description
Project Name	Enter the name of the project you want to create
Project Location	Select the folder and specify the path where you wish to save your project
Processor	Specify the processor of the mobile device which is compatible with the package. In most cases you do not need to modify the default "ALL" setting.
Platform	Select the mobile device platform. In most cases you do not need to modify the default "ALL" setting.
OS Versions	Enter the range of versions of the mobile device on to which the package can be deployed. In most cases you do not need to modify the default settings.
Version String	The version of the package is to be entered here (e.g. 1.0). The version numbers have to be incremented every time you modify the package, before you add the new modified package to the Packages view (tab)in MobiControl Manager.
Comment	Enter a description for the package. You can optionally leave this field blank.
Vendor	Enter name of the Vendor. You can optionally leave this field blank.

2. **Add optional scripts** through the **Add Scripts** page. You may select appropriate scripts you want to execute during installation or uninstallation of this package. Please see the "Add Script" topic on page 423 for more information.



Add Scripts page

3. **Add files** that are to be installed on the mobile devices through the **Add Files** page.



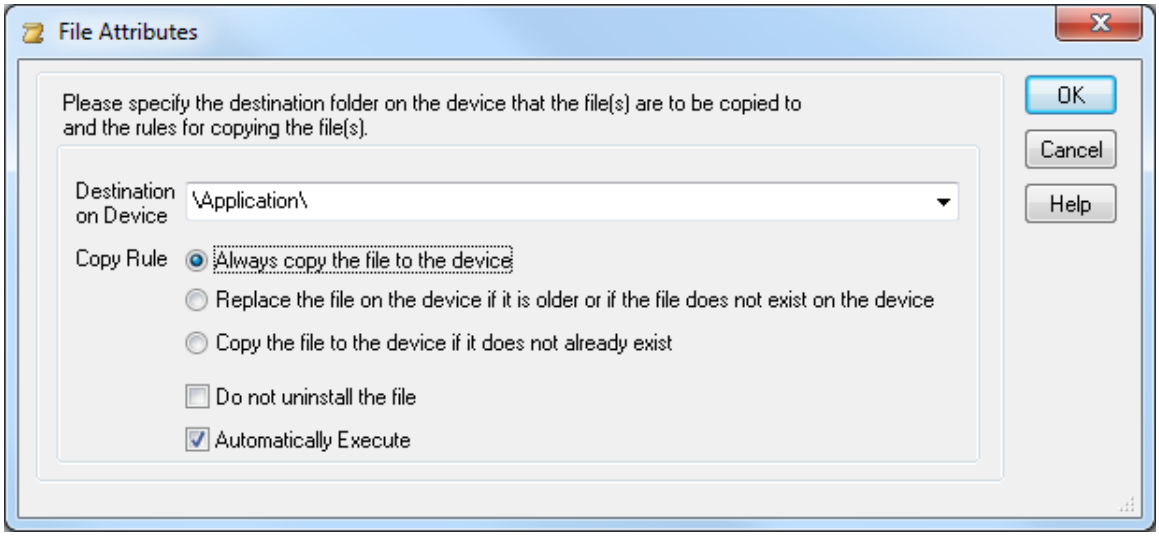
Add Files or Folders page of the New Package Wizard

The following table describes the fields in the **Add Files or Folders** page of the **New Package Wizard.**

Field Name	Description
Source	The full path to the file on the desktop computer.
Destination	The path on the mobile device where the file is to be installed to.

To add a file to the project, click the **Add** button and browse to the file(s) you would like to add to the project. After selecting the files you wish to add, the **File Attributes** dialog box will be displayed.

4. **Specify the location** on the mobile device where the file(s), file copying rules, and installation rules are to be installed.



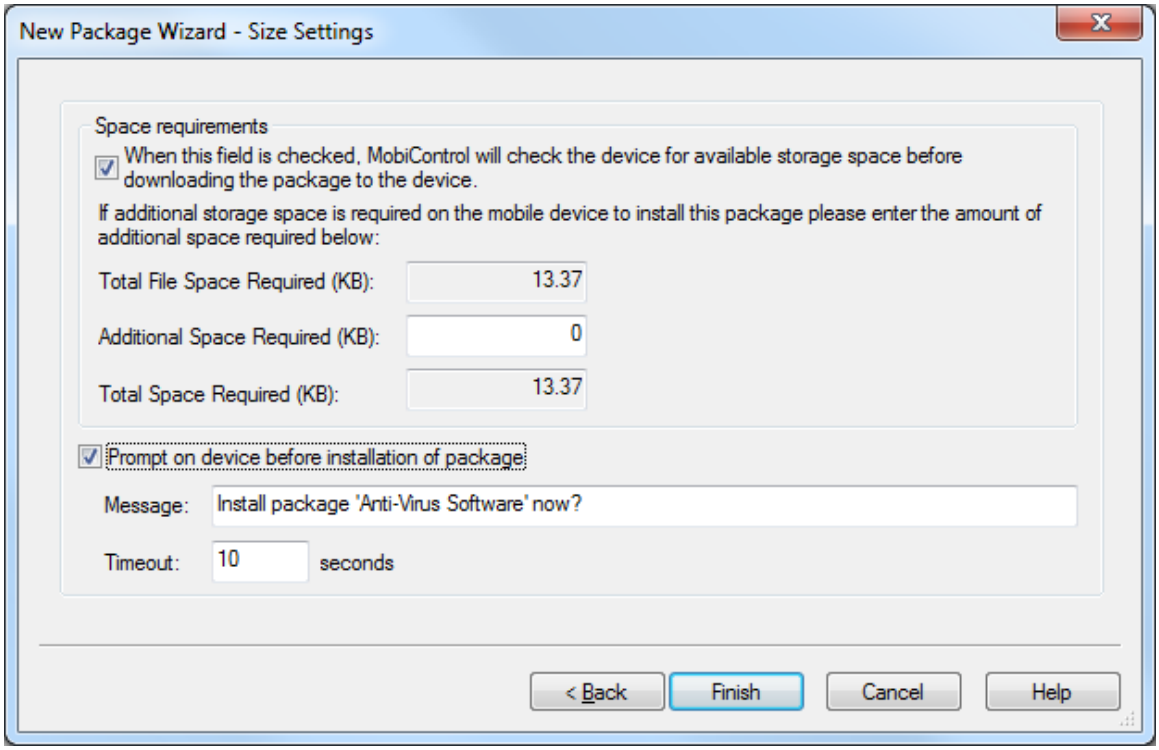
File Attributes dialog box

The following table describes the fields in the above dialog box.

Field Name	Description
Destination On Device	The path on the device to where the file is to be copied
Copy Rule	Specifies the condition to be checked before the file is copied to the device. The options available are: • Always copy the file to the device • Replace the file on the device if it is older than a file with the same name, or if the file does not exist on the device • Copy the file to the device if it does not already exist on the device
Do not uninstall the file	When this option is enabled for a file, that file will not be removed or uninstalled from the device even if the package is uninstalled.
Automatically Execute	Enabling this option results in the file being automatically executed or launched on the device after the package is delivered. This option can be used to automatically install an application distributed as a `.cab` file or to merge the registry settings in a `.reg` file with the device's registry automatically when the package is installed. Please see the "Cabinet File Properties" topic on page 430 for more information on suppressing warning messages for end users when installing `.cab` files and customizing the installation so that the end users are not prompted for locations.

Click **OK.** When you have finished adding files via the **Add File** page, click **Next.**

5. In the **Size Setting** dialog box, specify any additional storage space that may be necessary to install with the package.



Size Settings page

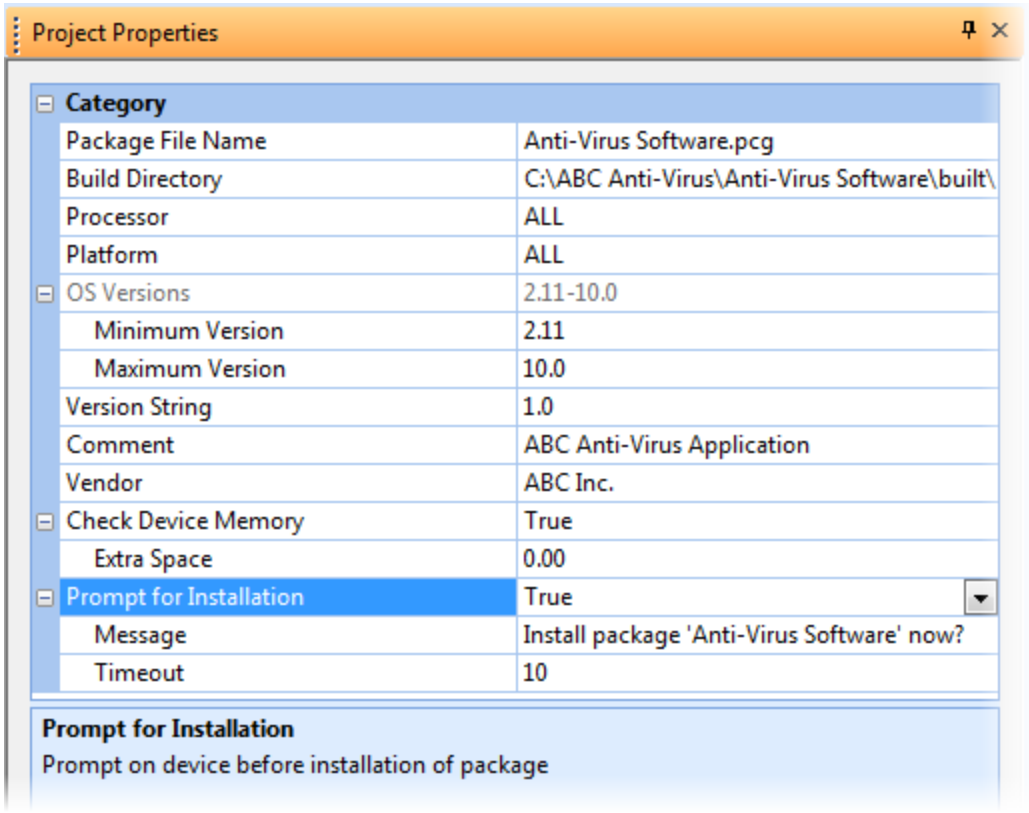
The following table describes the fields in the above dialog box.

Field Name	Description
Additional Space Required (KB)	Specify any additional storage space that may be needed to install the package. When MobiControl tries to install the package it will first check to see if there is enough space on the device to install the package.
Prompt on device before installation of package	If checked, a message box will appear on the device that prompts the user to install the package. If the user clicks **No,** the package will not be installed, the package will attempt to re-install five times by default and it can also be force a re-installed. The package will attempt to install on the Device Schedule Update. The message box is closed automatically after 10 seconds or if the user clicks **Yes** the package will continue installation.

6. Click the **Finish** button to create the project.

Viewing the Package Project Properties

Once you have created a package project, you can view the properties of the project by selecting **Package Properties** from the **Project** menu in Package Studio.



Package Project Properties dialog box

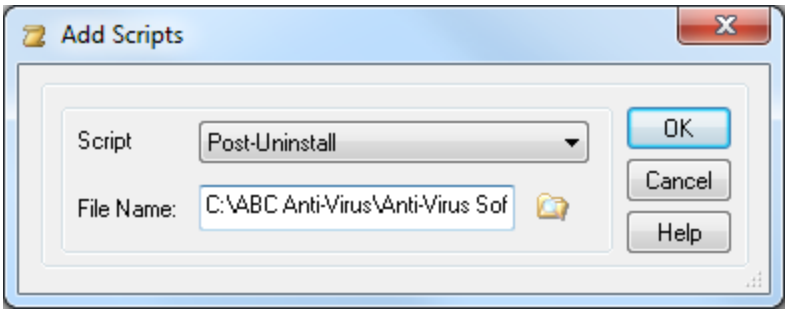
Attribute Name	Description
Package File Name	Name of the package file generated by Package Studio
Build Directory	Path where the package (`.pcg`) file will be saved
Processor	Processor of the mobile device onto which the package can be deployed
Platform	Operating system of the device onto which the package can be deployed
OS Versions	List of the OS versions of the mobile device supported by the package to be deployed
Version String	Version of this package (which must be incremented before rebuilding a package project)
Comment	Remarks or comments regarding the project
Vendor	Name of the vendor who is creating the package
Check Device Memory	When this field is set to "True," MobiControl will check the device for available space before downloading the package to the device
Extra Space	If there is extra space (more than file size required to install the package)
Prompt for installation	When this field is set to "True," the device user will be prompted to install with a pop-up message box.

Adding a Script to a Package Project

MobiControl Package Studio allows users to add custom control scripts to perform advanced operations during the installation or uninstallation of a package. There are four points during installation or un-installation at which custom scripts can be added:

1. A **pre-install script** is executed just before the installation of the package begins.
2. A **post-install script** is executed just after the package is installed.
3. A **pre-uninstall script** is executed just before the package is un-installed.
4. A **post-uninstall script** is executed just after the package is un-installed.

Scripts can be automatically added to a project by the New Package Wizard, or can be added later by selecting the **Add Script** menu option from the **Project** menu.



Add Script dialog box

The following table describes the fields of the **Add Script** dialog box:

Field Name	Description
Script	Select one of the pre-defined script file types
File Name	Select the path and file name of the script file to be executed

EXAMPLE:

Here is a pre-install script file which will execute before installation of a package:

```
cd \
mkdir \MyApp
cd \MpApp
rem Delete all files in case the directory already exists
del *.*
rem Make sure application is not running
kill MyApp.exe
copy "\Flash File Store\*.*" "\Flash File Store\2578\"
```

The commands that can be added to a package script are the same commands that are supported by the MobiControl remote DOS box. Please see the "Script Command Set" topic on page 72 for more information about remote DOS box commands. MobiControl script variables also can be used to creating device-side scripts. Please see the "Script Variables" topic on page 424 for detailed information.

MobiControl Script Variables

The MobiControl scripting engine exposes a number of MobiControl script variables that can be used when creating device-side scripts. These variables provide information such as the device name or the stable storage directory used by MobiControl. You can also create your own variables. Please see the set section of the "Script Command Set" topic on page 72 for more information about the `set` command.

NOTE:

MobiControl script variables are case sensitive.

The script variables are similar to environment variables, but are available only to scripts that are run as part of a package installation or uninstallation. Otherwise, they are used like environment variables. For example, you can use them to compose new variables or as arguments for script commands. Please see the Environment Variables section of the "Script Command Set" topic on page 72 for more information about environment variables.

EXAMPLE:

To copy the file `test.cab` from the current directory to the configured stable storage directory on a device:

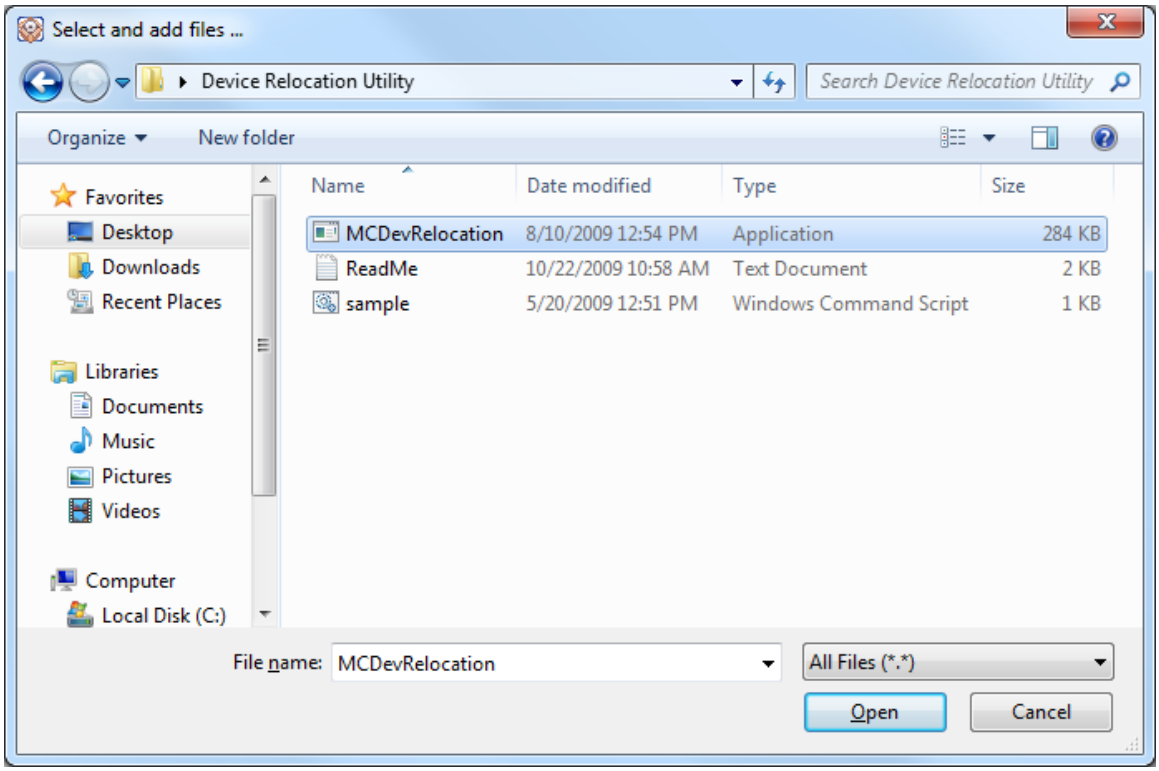
```
copy .\test.cab %MCSTABLESTOREDIR%
```

The following table describes the MobiControl script variables:

Script Variable Name	Description
%MCDEVICENAME%	The configured name of the device
%MCSTABLESTOREDIR%	The path to the stable storage directory that MobiControl will use to back up files that need to persist after a hard reset or battery failure
%MCSITENAME%	There can be multiple MobiControl sites or installations within an organization. This variable holds the name of the MobiControl site to which the device belongs. The default MobiControl site name is "MobiControl."
%MCCABFILE%	The full path to the MobiControlDevice Agent `.cab` file. The MobiControl `.cab` file is typically saved in a stable storage directory on the device so that the agent can be reinstalled after a hard reset or battery failure.
%MCDSLIST%	This variable contains the list of IP addresses for the configured MobiControl Deployment Servers. The Device Agent uses this list to select a Deployment Server to which to connect. If a server has both an internal and an external IP address configured, then only the external address will be in the list. IP addressed are separated by semicolons ";."
%IP%	IP address currently assigned to the device
%MAC%	MAC address of the device's network interface card

Adding Files to a Package Project

To add files to the existing package project, select **Project,** and click **Add Files.** You can also right-click on the project name in the Project panel and select **Add Files** from the context menu. This will bring up the **Select and Add Files** dialog box.



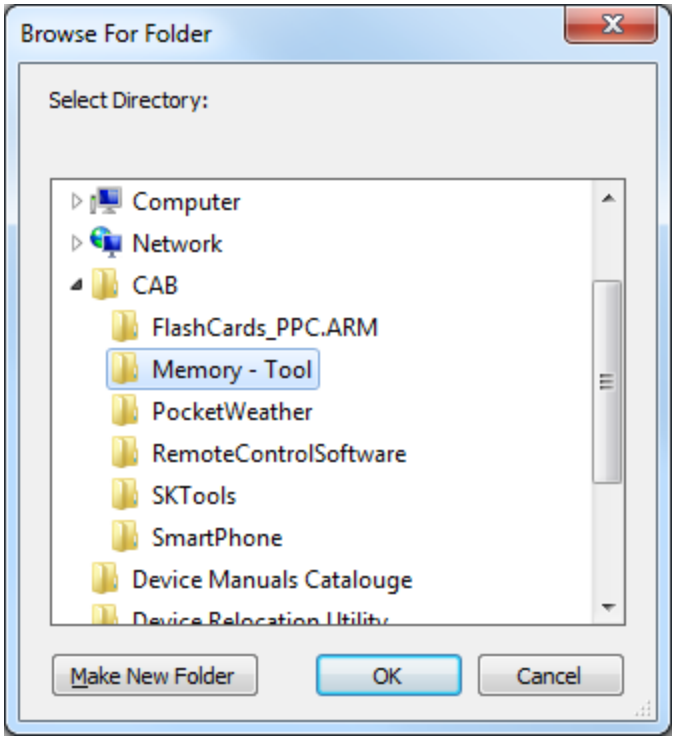
Select and Add Files dialog box

Select one or more files you want to add to the project and click **Open.**

The **File Attributes** dialog box will show up, allowing the user to specify the file's attributes. (Please see the "Create Package Project" topic on page 419.)

Adding a Folder to a Package Project

To add all files from a folder to the existing package project, select **Project**, and click **Add Folder.** You can also right-click on the project name in the Project panel and select **Add Folder** from the context menu. This will bring up the **Browse for Folder** dialog box:



Browse for Folder dialog box

Select the folder you want to add to the project and press **OK.**

The **File Attributes** dialog box will show up, allowing the user to specify the attributes of the files in the folder. (Please see the "Create Package Project" topic on page 419.)

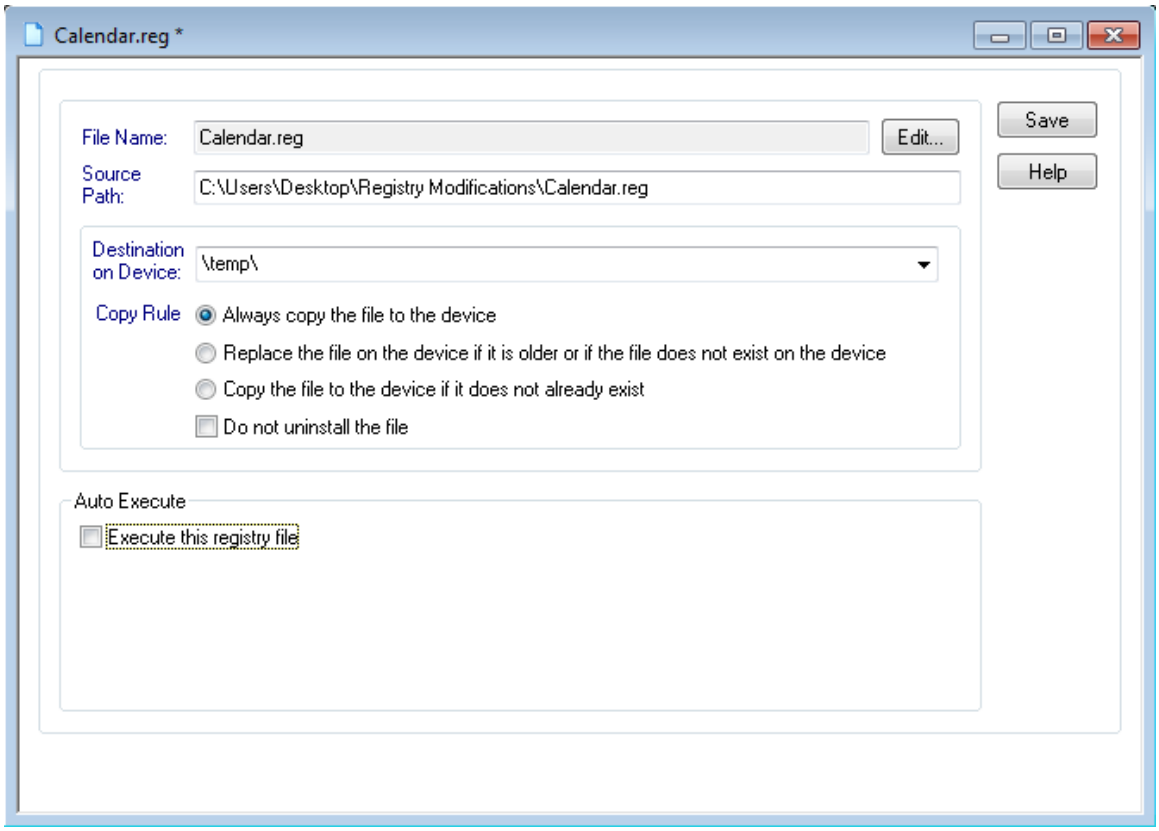
File Properties Overview

There are four different versions of the **File Properties** dialog box that pop up when viewing a file's properties in a Package Studio project. Each version of the **File Properties** dialog box includes options for the different file types that are recognized by the Package Studio.

File Type	Description
`.Reg` files	These are files that modify the Windows registry settings upon execution. Please see the "Package Studio Registry File Properties" topic on page 428 for more information.
`.Cab` files	These files usually contain a software application to be installed on the device in a compressed format. Please see the "Cabinet File Properties" topic on page 430 for more information.
`.Exe` files	These files are executable files. Please see the "Executable File Properties" topic on page 434 for more information.
General files	All files that do not correspond to the above three file types are included in this category. These files may include data files, image files, text files or any other type of file that needs to be delivered or installed on the device. Please see the "Package Studio File Properties" topic on page 436 for more information.

.Reg File Properties

This dialog box allows the user to modify a file's properties, such as its destination folder on the device, and how it is to be processed once it is copied to the device.



Registry File Properties dialog box

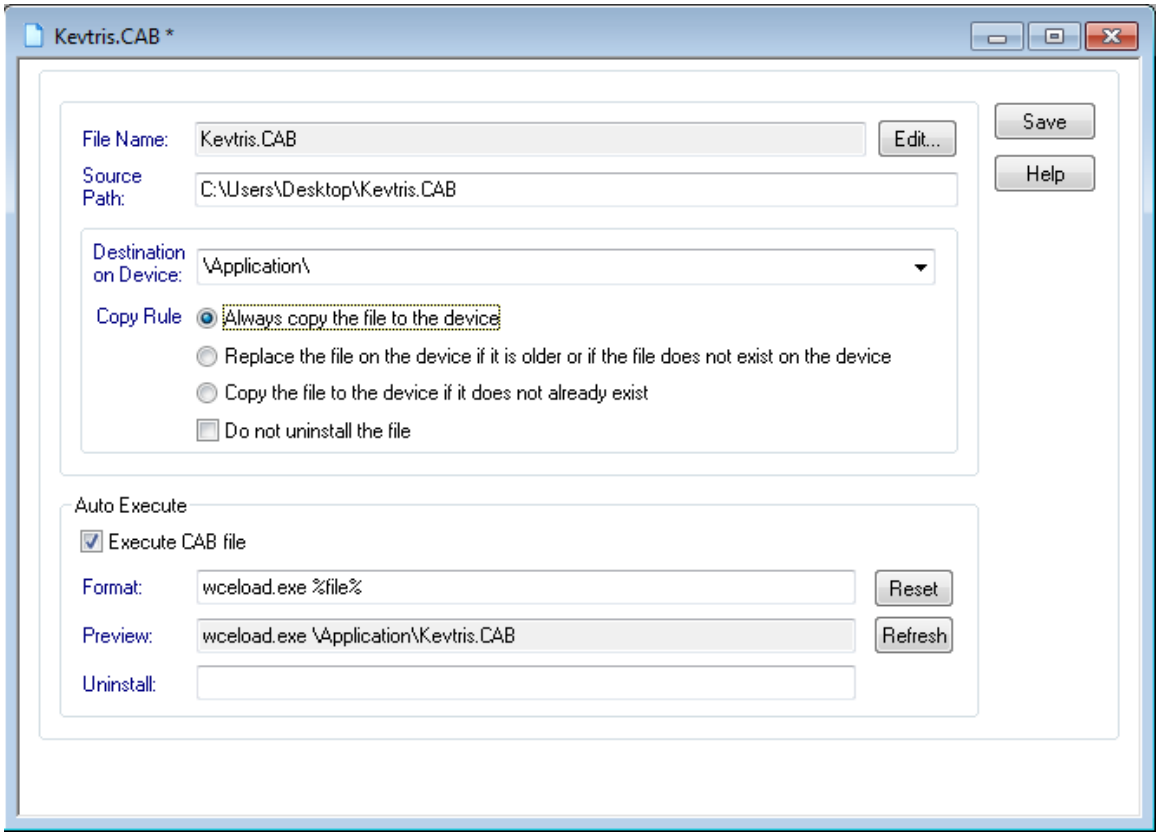
The following table describes the fields of the **Registry File Properties** dialog box:

Field Name	Description
File Name	Read-only field that is used to display the name of the file
Edit	Allows you to edit the contents of the selected file using the associated application for that extension. This option is inaccessible for `.exe` applications.
Full Source Path	Read-only field that is used to display the full source path to the file
Destination on Device	Path on the device to where the file will be copied
Copy Rule	Specifies the condition to be checked before the file is copied to the device. Options are: • Always copy the file to the device

Field Name	Description
	• Replace the file on the device if it is older than a file with the same name, or if the file does not exist on the device • Copy the file to the device if it does not already exist on the device
Execute this registry file	The registry data from the `.reg` file in the package will be merged automatically with the mobile device's registry when the package is installed on the device.

.Cab File Properties

This dialog box allows the user to modify a `.cab` file's properties, such as its destination folder on the device, and how it is to be processed once it is copied to the device. The default command line options can be used to automatically install the `.cab` file on the device or these options can be modified to customize the installation of the `.cab` file.



.Cab File Properties dialog box

The following table describes the fields of the **.Cab File Properties** dialog box:

Field Name	Description
File Name	Read-only field that displays the name of the `.cab` file
Edit	Edit the contents of the `.cab` file using the associated application for that extension.
Source Path	Read-only field that is used to display the full source path to the file
Destination on Device	Path on the device to where the file will be copied
Copy Rule	Specifies the condition to be checked before the file is copied to the device. Options are:

Field Name	Description
	• Always copy the file to the device • Replace the file on the device if it is older than a file with the same name, or if the file does not exist on the device • Copy the file to the device if it does not already exist on the device
Do not uninstall the file	The file will not be uninstalled from the device if the package is uninstalled, for instance, if the deployment rule is deleted.
Execute CAB file	The command line specified in the preview field will be automatically executed after the file is copied to the destination directory.
Format	Allows the user to customize the command line to be executed after the file is copied to the device. The "`%file%`" macro can be used instead the real file name and path.
Preview	A read-only field that displays the command to be executed after the file has been copied to the destination folder. After the format field has been edited, the user needs to click on the **Refresh** button to update the preview field.
Uninstall	The command line to be used to uninstall the `.cab` file during uninstallation of the package if the **Execute cab file** option is checked

Auto-Execute Options and wceload.exe

To install a `.cab` file on the mobile device, the Microsoft utility `wceload.exe` is used. This utility is built into the Microsoft operating system for mobile devices for customizing the installation of `.cab` files on the mobile device.

IMPORTANT:

The following information is only for the convenience of MobiControl customers and does not replace any official documentation available from Microsoft. It is recommended that you consult Microsoft's website for additional documentation and information for developers. For more information on `wceload.exe`, please see the following on Microsoft's site: http://msdn.microsoft.com/en-us/library/bb158700.aspx.

There are a series of command-line options that can be used to control aspects of the `.cab` file installation. These options vary for different operating systems. Some options may not be implemented at all for certain devices.

EXAMPLE:

```
wceload.exe [ /delete <value> | /noui ] [ /confignotify | /nodelete
| /safe | /silent | /verifyconfig] <location of cab file>
```

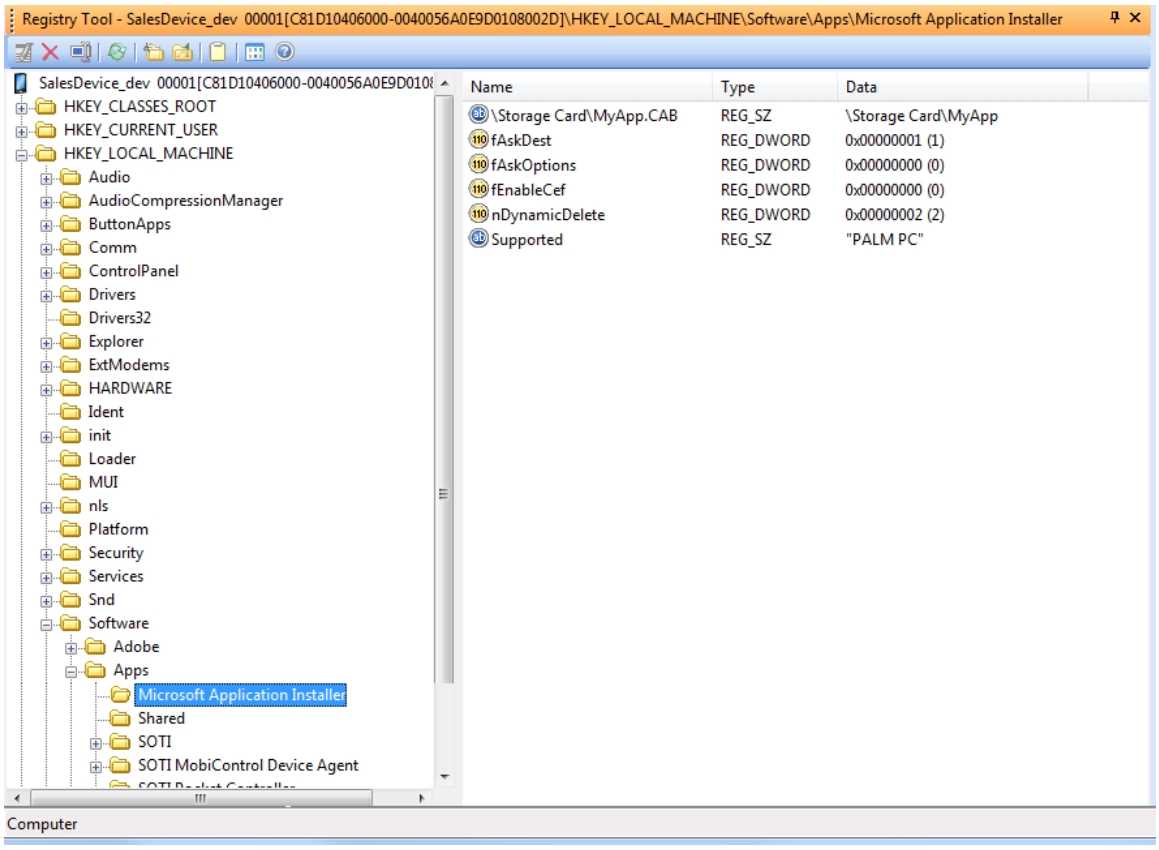
Option	Description
/delete <value>	• If <value> is set to 0, the .cab file is not deleted from the mobile device, after it has been installed. (e.g. wceload.exe /delete 0 MyCab.cab) This is the same as "/nodelete." • If <value> is set to 1, or if "/delete" is not set, then the .cab file will be removed.
/nodelete	Specifies that the .cab file is not removed after installation.
/noui	Specifies that the user will not be prompted for any input during the installation. By default, prompts are answered with **Yes.** However, if the .cab file is unsigned, any security-related prompts will default to **No** for security reasons, and the installation might fail. This is the same as "/silent" for legacy compatibility reasons.
/silent	Suppresses dialog boxes during the installation, and all Yes/No prompts default to **Yes,** unless the .cab file is not signed. However, if the .cab file is unsigned, any security-related prompts will default to **No** for security reasons, and the installation might fail. This is the same as "/noui" for legacy compatibility reasons.
/nouninstall	Uninstall information for the application installed by this cab file is not written to the device. The application entry will not appear in the **Remove Programs** list on the mobile device so the application cannot be removed. This is only available with Windows Mobile 5 and below.
/askdest	The user is prompted to select an installation location on the mobile device to where the application will be installed.
/noaskdest	The user is not prompted to select an installation directory; the default installation directory specified by the cab file is used instead.
/safe	Specifies that the .cab file cannot contain executable files. Also, if the .cab file is unsigned; it can only use restricted permissions, ensuring that it will not be able to write to protected files and registry keys. Only available with Windows Mobile 6 and above.
/verifyconfig	Specifies that the wceload tool must verify whether the file passed in is a .cpf file. If the file is not a .cpf file, the installation fails. Only available with Windows Mobile 6 and above.
/confignotify	Generates a configuration result notification that is placed in the Text Message store on the device. Only available with Windows Mobile 6 and above.

NOTE:

The results for "/noaskdest" may differ on some devices, for instance, Smartphone devices. When specifying this option, wceload.exe might ignore the command line and check for the installation path in the following registry location:
[HKEY_LOCAL_MACHINE\SOFTWARE\Apps\Microsoft Application Installer\Install]
The contents are key/value pairs:
[cab File Path] = [cab Destination Directory]

EXAMPLE:

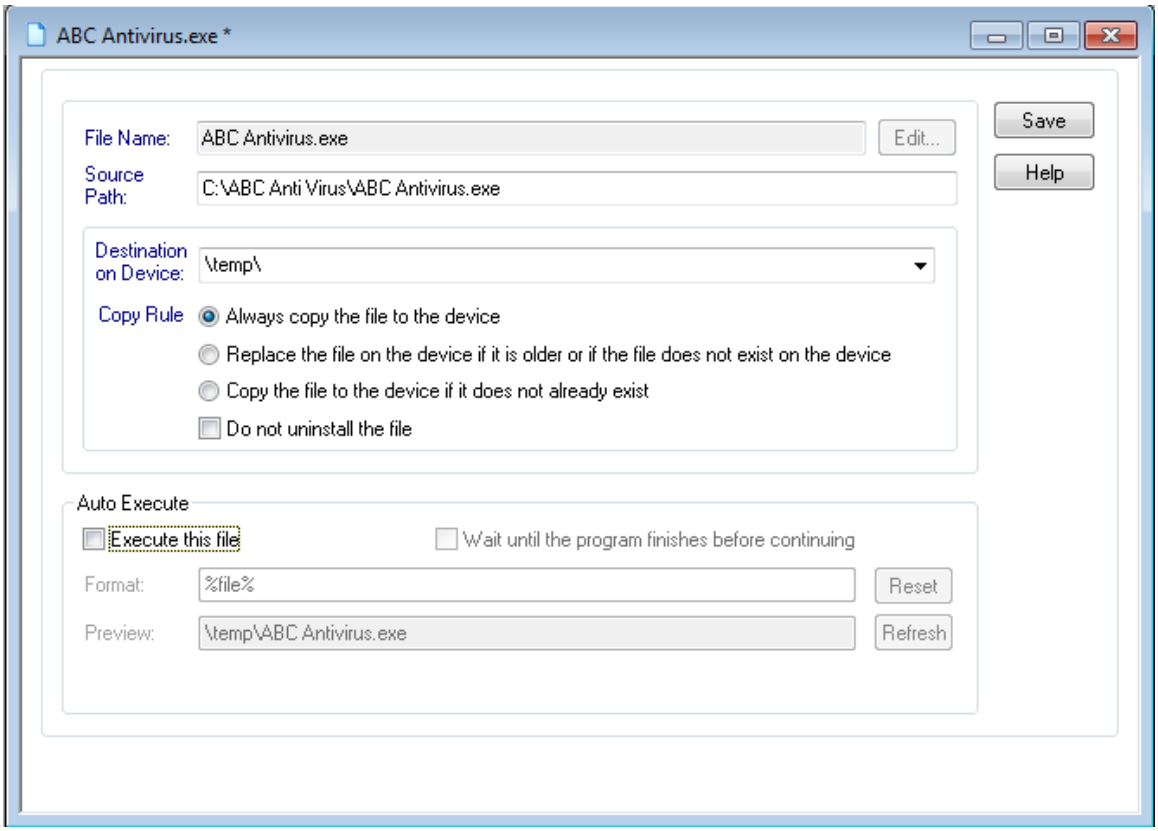
`\Storage Card\MyApp.cab = \Storage Card\Program Files\My App`
will lead `wceload.exe` to try to install the `.cab` specified in the value name to the location specified in the value. In order to suppress any warnings and control the location to which the `.cab` file should be installed, you may need to create the appropriate registry value (possibly using a MobiControl pre-install script) before installing the `.cab` file in the package. See the following image for sample registry content.



Registry entry to install `.cab` file at a custom location

.Exe File Properties

This dialog box allows the user to modify an `.exe` file's properties, such as its destination folder on the device, and how it is to be processed once it is copied to the device.



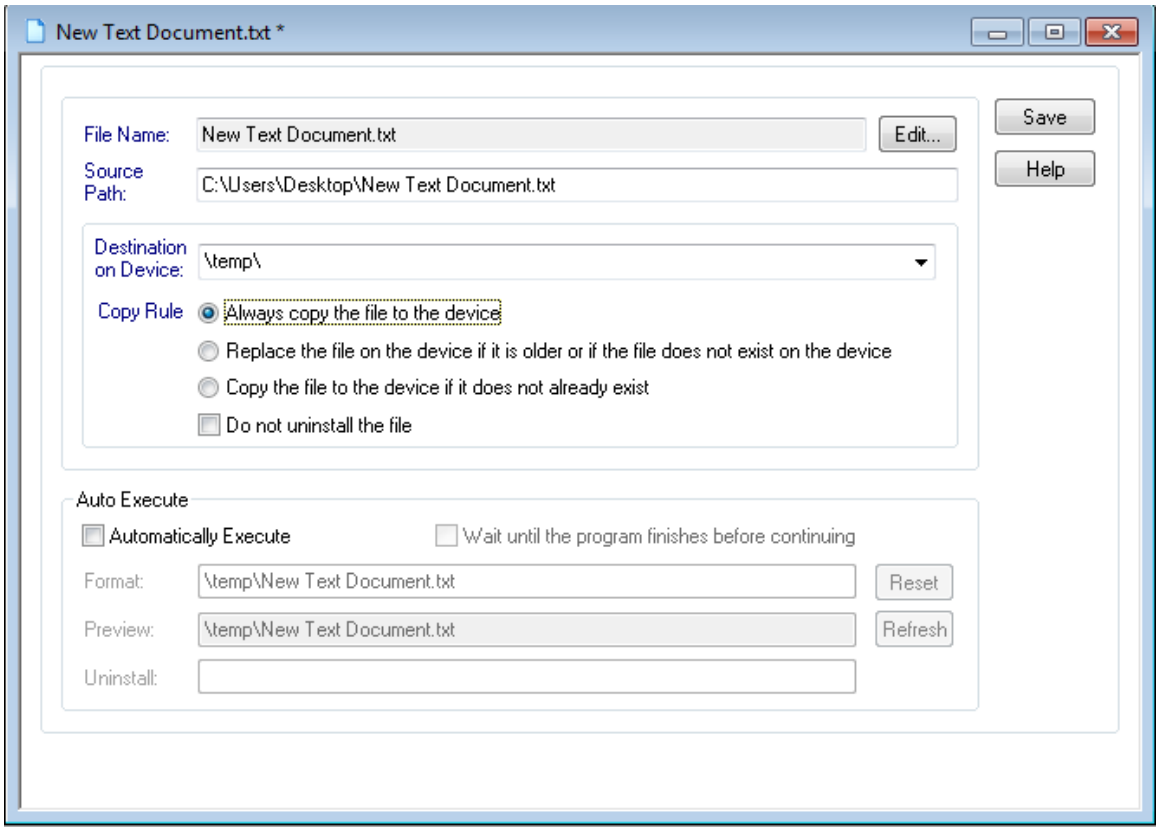
Executable File Properties dialog box

The following table describes the fields of the **Executable File Properties** dialog box:

Field Name	Description
File Name	Read-only field that is used to display the name of the file
Edit	Allows you to edit the contents of the selected file using the associated application for that extension. This option is inaccessible for `.exe` applications.
Full Source Path	Read-only field that is used to display the full source path to the file
Destination on Device	Path on the device to where the file will be copied
Copy Rule	Specifies the condition to be checked before the file is copied to the device. Options are: • Always copy the file to the device • Replace the file on the device if it is older than a file with the same name, or if the file does not exist on the device • Copy the file to the device if it does not already exist on the device
Do not uninstall the file	The file will not be uninstalled from the device if the package is uninstalled, for instance, if the deployment rule is deleted.
Execute this exe file	The command line specified in the preview field will be automatically executed after the file is copied to the destination directory.
Wait until the program finishes before continuing	Installation will wait until the command specified in the preview field finishes executing before continuing with the installation.
Format	Allows the user to customize the command line to be executed after the file is copied to the device. The "`%file%`" macro can be used instead the real file name and path.
Preview	A read-only field that displays the command to be executed after the file has been copied to the destination folder. After the format field has been edited, the user needs to click on the **Refresh** button to update the preview field.

General File Properties

This dialog box allows the user to modify a file's properties such as its destination folder on the device, and how it is to be processed once it is copied to the device.



General File Properties dialog box

The following table describes the fields of the **General File Properties** dialog box:

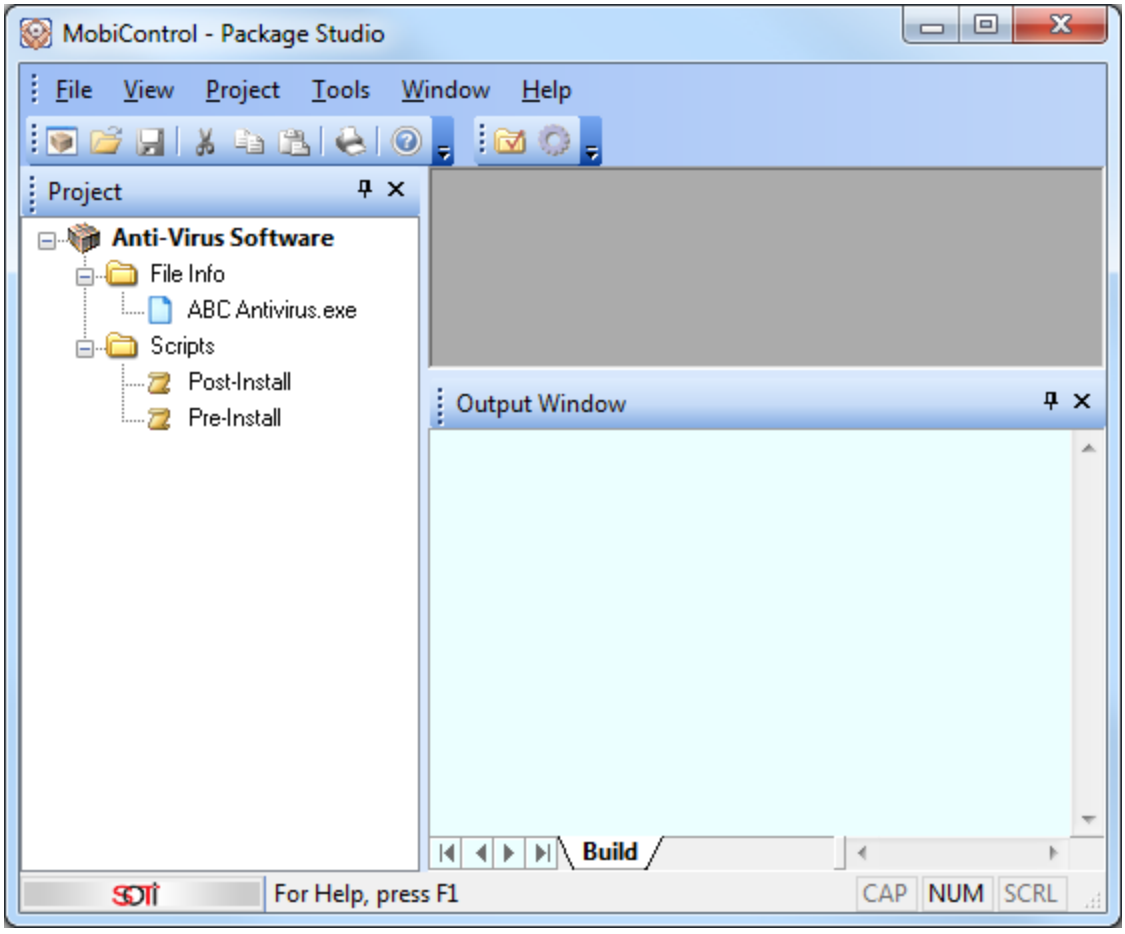
Field Name	Description
File Name	Read-only field that is used to display the name of the file
Edit	Allows you to edit the contents of the selected file using the associated application for that extension. This option is inaccessible for `.exe` applications.
Full Source Path	Read-only field that is used to display the full source path to the file
Destination on Device	Path on the device to where the file will be copied
Copy Rule	Specifies the condition to be checked before the file is copied to the device. Options are: • Always copy the file to the device • Replace the file on the device if it is older than a file with the same name, or if the file does not exist on the device • Copy the file to the device if it does not already exist on the device
Do not uninstall the file	The file will not be uninstalled from the device if the package is uninstalled, for instance, if the deployment rule is deleted.
Automatically Execute	The command line specified in the preview field will be automatically executed after the file is copied to the destination directory.This option can be used to automatically install an application distributed as a `.cab` file, or to open automatically an image file or a document file (like a Pocket Word document or a Pocket Excel spreadsheet) on the device after installing it.
Wait until the program finishes before continuing	Installation will wait until the command specified in the preview field finishes executing before continuing with the installation.
Format	Allows the user to customize the command line to be executed after the file is copied to the device. The "`%file%`" macro can be used instead the real file name and path.
Preview	A read-only field that displays the command to be executed after the file has been copied to the destination folder. After the format field has been edited, the user needs to click on the **Refresh** button to update the preview field.
Uninstall	The command line to be executed before deleting the file during uninstallation of the package if the **Automatically Execute** option is checked.

Building a Package Project

This section of MobiControl Package Studio explains how a package is built once a package project has been created. (Please see the "Create Package Project" topic on page 415.)

1. Open the package project.

   Click **File** and then click **Open Existing Package Project (.mcp) files**. A package project will be opened.



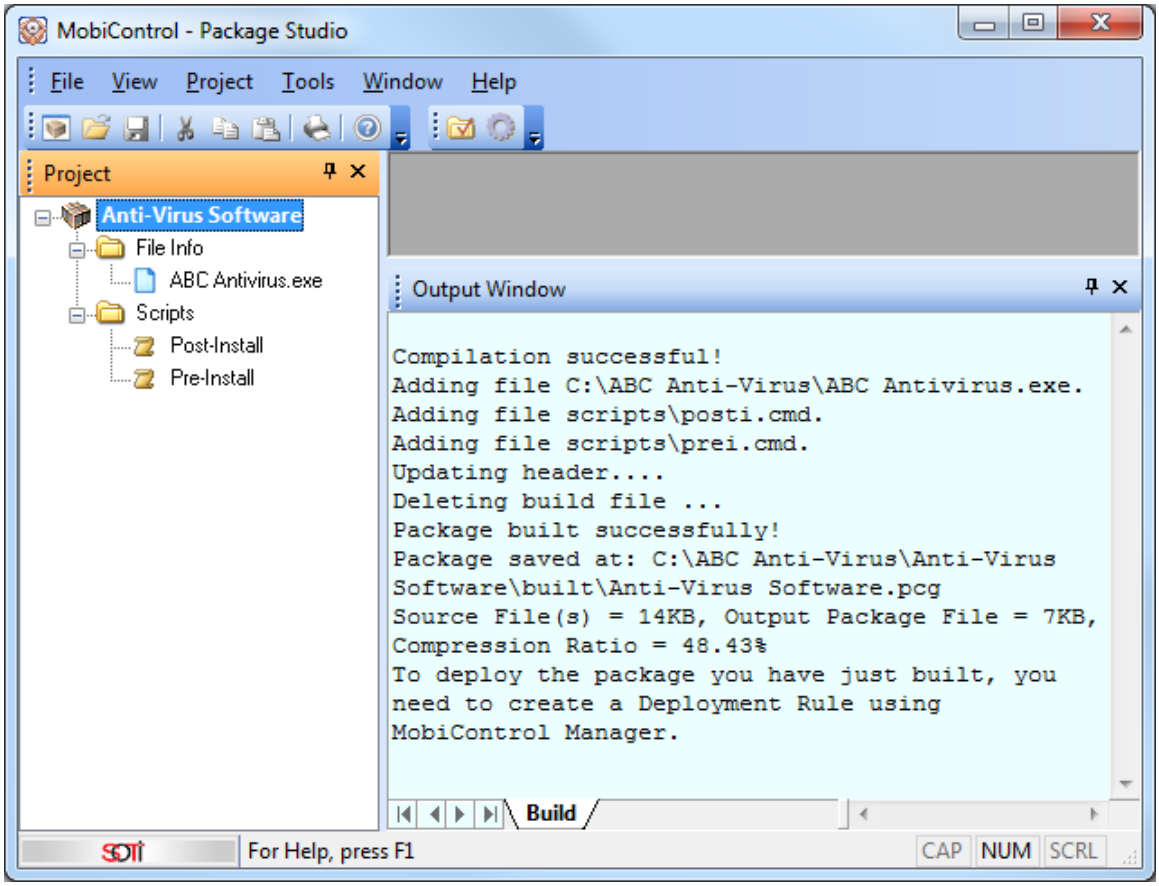
Open package project

2. Build the package project.

   Click **Project** and then click **Build Package.**

3. Check the output.

Check the build status in the Output window.



Build Package Output

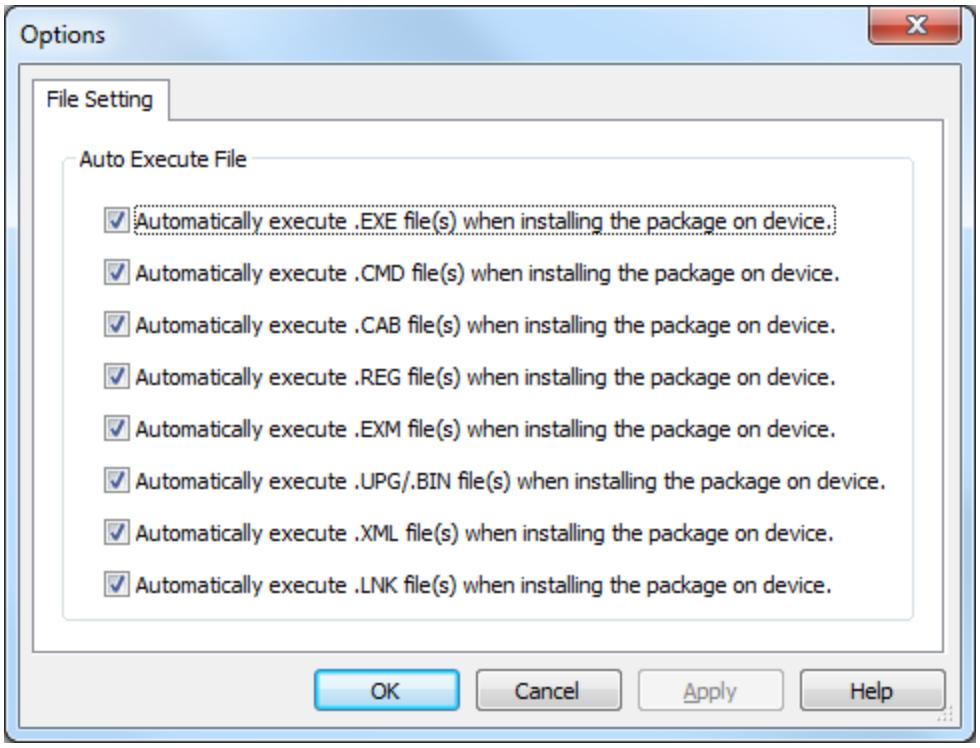
Configuring Package Studio

The **File Setting** tab is accessible through the **Tools** menu and the **Options** menu item from the main Package Studio window.

The auto execute file settings specify the default action taken when an executable file type is delivered to a device in a package. By default, each of the recognized executable file types (`.exe`, `.cmd`, `.cab`, `.reg`, `.exm`, `.upg`/`.bin`) are set to auto-execute when you create a new package using Package Studio. If you do not want any of these file types to be automatically executed for the packages you are creating, uncheck the box.

EXAMPLE:

If the check box next to **`.Cab`** is unchecked, then `.cab` files included in any new packages will not be automatically installed when the package is delivered to the device.



Package Studio File Setting dialog box

Setting up MobiControl

Please explore the following pages related to the setup of MobiControl:

- The "Installing MobiControl" topic on page 465 describes in detail how to install MobiControl for the first time, and how to re-install it.
- The "Activation from the Management Console" topic on page 448 describes what to do after installation: how to obtain and use a registration code and how to upgrade to v 6.0 or later.
- The "Database Configuration" topic on page 463 describes the **Data Link Properties** dialog box that appears during setup.
- The "Upgrading MobiControl" topic on page 553 contains information about how to upgrade an existing installation of MobiControl.
- The "Uninstalling MobiControl" topic on page 562 describes how to uninstall MobiControl Manager, a Deployment Server, a database, or a Device Agent.

MobiControl System Requirements

Architecturally, MobiControl has 4 main components.

These are:

- The Management Service (Web Console)
- The Deployment Service
- The Database
- The Device Agent

NOTE:

The below system requirements are for when the Management Service and Deployment Service are on separate computers.

Management Service Requirements

The Management service hosts the MobiControl Web Console so that we can manage and configure devices.

Operating System

- Windows Vista
- Windows 7
- Windows 8
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012

Processor

- ***10 to 500 devices***: 2 GHz or faster.

- ***500 to 1000 devices***: 2 GHz Dual Core or faster.
- ***1000+***: 2.5 GHz Quad Core or faster.

NOTE:

These are the requirements we recommend. If there is constant data collection and configurations, then we suggest upgrading to higher clock speeds.

Memory (RAM)

- ***10 to 500 devices***: 2 GB of RAM or more.
- ***500 to 1000 devices***: 4 GB of RAM or more.
- ***1000+***: 8 GB of RAM or more.

Memory (Storage)

- MobiControl will use approximately 200 MB of storage space.

Browsers

- Internet Explorer 8 or above
- Google Chrome
- Mozilla Firefox
- Safari

Other

- .NET 4 framework Installed with all critical updates.

Deployment Service Requirements

The Deployment Service accepts incoming connections from all device agents.

Operating System

- Windows Vista
- Windows 7
- Windows 8
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012

Processor

- ***10 to 500 devices***: 2 GHz or faster.
- ***500 to 1000 devices***: 2 GHz Dual Core or faster.
- ***1000+***: 3 GHz Quad Core or faster.

NOTE:

These are the requirements we recommend. If there is constant data collection and configurations, then we suggest upgrading to higher clock speeds.

Memory (RAM)

- ***10 to 500 devices***: 2 GB of RAM or more.
- ***500 to 1000 devices***: 4 GB of RAM or more.
- ***1000+***: 8 GB of RAM or more.

Memory (Storage)

- MobiControl will use approximately 200 MB of storage space.

NOTE:

The below system requirements are for when the Management Service and Deployment Service are on the same computer.

Management and Deployment Service Requirements

When the Management and Deployment Services are installed on the same computer we recommend the following:

Operating System

- Windows Vista
- Windows 7
- Windows 8
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012

Processor

- ***10 to 500 devices***: 2 GHz or faster.
- ***500 to 1000 devices***: 2 GHz Dual Core or faster.
- ***1000+***: 3 GHz Quad Core or faster.

NOTE:

These are the requirements we recommend. If there is constant data collection and configurations, then we suggest upgrading to higher clock speeds.

Memory (RAM)

- ***10 to 500 devices***: 2 GB of RAM or more.

- ***500 to 1000 devices***: 4 GB of RAM or more.
- ***1000+***: 8 GB of RAM or more.

Memory (Storage)

- MobiControl will use approximately 200 MB of storage space.

Browsers

- Internet Explorer 8 or above
- Google Chrome
- Mozilla Firefox
- Safari

Other

- .NET 4 framework Installed with all critical updates.

Database Requirements

MobiControl uses Microsoft SQL as its database server. MobiControl comes bundled with Microsoft SQL Server 2008 Express edition, a lightweight version of SQL Server 2008. Typically, this database is adequate for a device deployment ranging from 10 to 1000 devices. Beyond 1000 devices, use of Microsoft SQL Server 2008 is recommended as it contains numerous salability and performance improvements.

For 10 to 1000 devices we recommend these databases:

- MS SQL Server 2008 Express Edition (Comes bundled with MobiControl)
- MS SQL Server 2012 Express Edition

For 1000 or more devices we recommend these databases:

- MS SQL Server 2008
- MS SQL Server 2012

Operating System

- Windows Vista
- Windows 7
- Windows 8
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012

Processor

- 2 GHz Dual Core or faster.

Memory (RAM)

- 4 GB of RAM or more.

Memory (Storage)

- Approximately 350MB for installation
- ***10 to 500 devices***: 2 GB for database growth.
- ***500 to 1000 devices***: 4 GB for database growth.
- ***1000+***: At least 5 GB for database growth

NOTE:

The size of the database is dependent on the amount of historical log information that you wish to retain and the frequency with which the MobiControl system is being used for package deployment. The disk space recommendations leave plenty of room for growth.

NOTE:

The database and the Deployment servers may be installed on the same host server depending on the number of devices and performance of the host server. For deployments with more than 500 devices, we recommend using a standalone database.

Device Agent System Requirements

iOS Devices

The MobiControl device agent allows the device to synchronize back to the Deployment Server. This includes collecting data and file content management.

Operating System

- iOS 4.3 and above

Devices

- Compatible with all devices capable of running the supported operating system.
- iPod Touch
- iPhone
- iPad

Memory (Storage)

- MobiControl will use approximately 4 MB of space on the device.

Connectivity

- The device agent for iOS devices does not need to be installed to manage device features. Enhanced features are available when the device agent is installed. Please see the "iOS Agent Install Methods" topic on page 949 for more information.

- An APNS certificate is required in order to manage iOS devices. Please see the "Installing the APNS Certificate" topic on page 508 for more information on how to configure the APNS certificate.
- Connectivity is only required when synchronizing a device with the MobiControl system or to perform a review view.

Android Devices

The MobiControl device agent allows the device to communicate back to the Deployment Server. This includes collecting data and remote control.

Operating System

- Android 2.2 and above

NOTE:

Certain devices can be added as Android+ devices. These types of devices should be Android 2.3 or higher.

Devices

- Compatible with all devices capable of running the supported operating system.

NOTE:

To find out if your device is supported for Android+ please contact us.

Memory (Storage)

- MobiControl will use approximately 4 MB of space on the device.

Connectivity

- Connectivity is only required when synchronizing a device with the MobiControl system or to perform remote control.

NOTE:

Only devices which support Android+ can be remote controlled. To find out if your device is supported for Android+ please contact us.

Windows OS Devices

The MobiControl device agent allows the device to communicate back to the Deployment Server. This includes collecting data and remote control.

Operating System

- Windows Mobile (5.0, 6.0, 6.1, 6.5, 6.5.3).
- Pocket PC (2002, 2003).
- CE .NET (4.2, 5.0, 6.0).

- Windows XP (32-bit).
- Windows Vista (32 and 64-bit).
- Windows 7 (32 and 64-bit).
- Windows 8 (32 and 64-bit).

Processor

- Compatible with all processors capable of running the supported operating systems listed above.

Memory (Storage)

- MobiControl will use approximately 4 MB of space on the device.

Connectivity

- Connectivity is only required when synchronizing a device with the MobiControl system or to perform remote control.

Activating MobiControl From the Management Console

Device Licenses

With the introduction of Apple iOS and Google Android devices into the MDM sphere SOTI has risen to the challenge of including features for these devices and increased capability for Windows Desktop OS devices as well. Since these OS's are in their infancy for MDM capabilities SOTI has adjusted the licensing to reflect the level of capability included with each device type. SOTI now offers the following license options:

- Premium Licenses *(Can be used on any device type)*
- OS Specific License
    - Apple iOS
    - Google Android

NOTE:

Registration codes purchased prior to the release of MobiControl v9.0x are considered premium. Unless otherwise indicated at the time of purchase.

Scenario Summary

One of these scenarios will occur during or after the installation of MobiControl:

1. Clean Installation of MobiControl
2. Upgrade to v9.03 or later Required

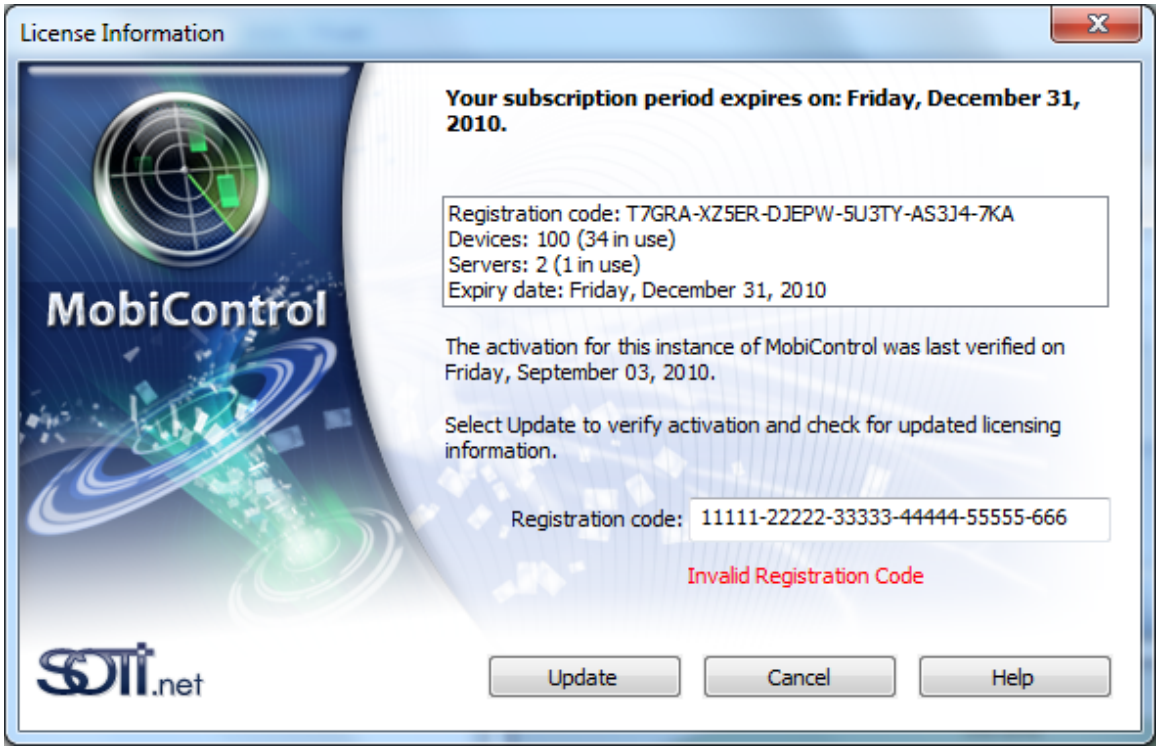
In this section, there is also information available about how to change your registration code:

- Changing your Registration Code

Clean Installation of MobiControl

When MobiControl finishes installing completely, a registration window will open up requesting a registration code. If you don't have a valid registration code or you are upgrading to version 6 or later, you can visit our website to sign up for a 31-day trial registration code or contact us to get a new registration code. If your trial expires, you will be prompted to enter a new registration code.

If you enter an invalid registration code, clicking **Activation** will result in the following error message:



If the activation process has failed, the following will be displayed. Please Contact Us for possible reasons for the failure of your registration code.

If your registration code has already been used to activate another instance of MobiControl then the following message will be displayed. If you require another activation on your registration code please Contact Us.


MobiControl Activation Wizard
MobiControl
MobiControl Activation Failed.
This registration code has already been activated on another computer
Your subscription period expires on: Friday, December 31, 2010.
For support please contact us.
SOTI.net
Close
Help

Upgrade to v9.03 or later Required

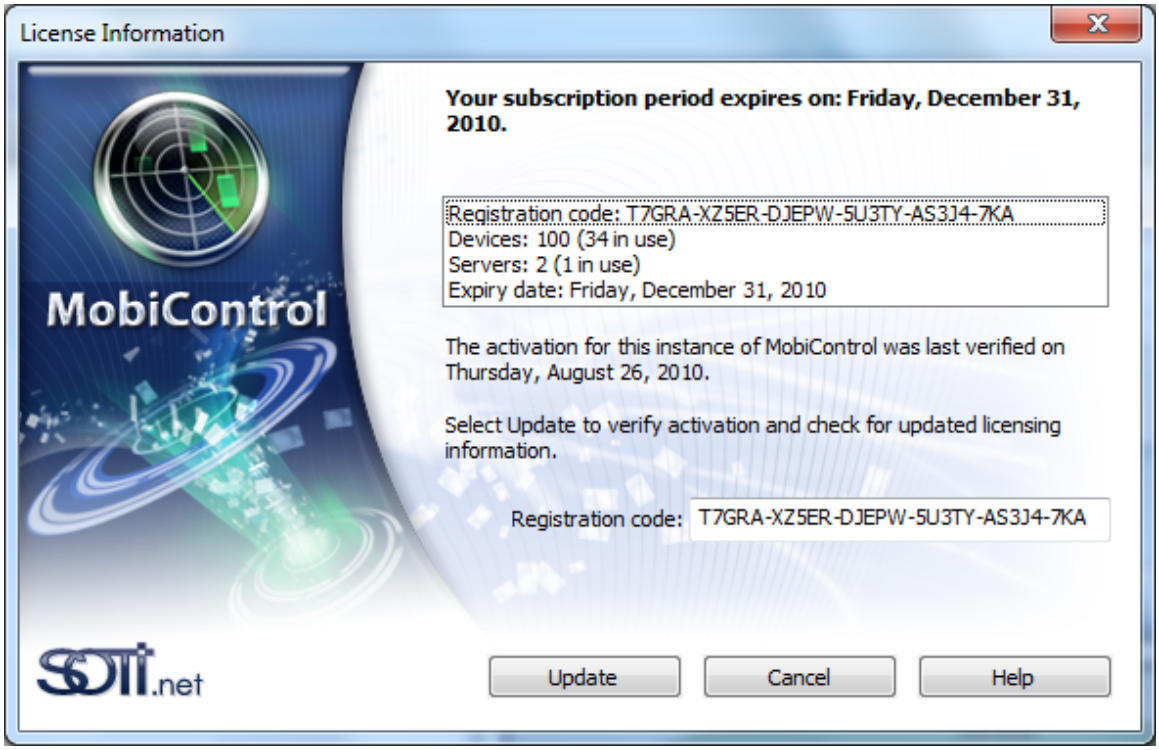
During installation, after selecting the type of install, you may be required to enter a new registration code. This will only appear if you have a registration code that is an older format. To exchange or to obtain your new registration code, you must contact us and provide your existing registration code followed by the company name and the person to whom the product is licensed.

After receiving your new registration code, you will now be able to successfully activate the product.

Changing your Registration Code

In the MobiControl Manager, open the **Help** menu and click **License Information,** and a window will pop up where you can enter a valid registration code.

In v9.03 or later, when you receive a new registration code (for adding devices, or extending service periods) you do not need to update your registration code manually, this update will take place automatically. The deployment server service does a periodic check every day to verify the registration information is correct and up to date.



Manually Registering MobiControl

If there is no Internet connection available, or if the MobiControl Manager is unable communicate with the activation servers you will be prompted to manually activate MobiControl.

Navigate to http://activate.soti.net/MCActivation on a machine that does have access to the Internet and enter the information provided to you by the Manual Activation Wizard. Once you have successfully activated on the Activation website, you will be provided with a License File. Browse to the License file provided by the Activation website and click Activate.

Once you have successfully activated MobiControl you will be able to use all of its features.

Activating MobiControl From the Web Console

Device Licenses

With the introduction of Apple iOS and Google Android devices into the MDM sphere SOTI has risen to the challenge of including features for these devices and increased capability for Windows Desktop OS devices as well. Since these OS's are in their infancy for MDM capabilities SOTI has adjusted the licensing to reflect the level of capability included with each device type. SOTI now offers the following license options:

- Premium Licenses *(Can be used on any device type)*
- OS Specific License
    - Apple iOS
    - Google Android

NOTE:

Registration codes purchased prior to the release of MobiControl v9.0x are considered premium. Unless otherwise indicated at the time of purchase.

Scenario Summary

One of these scenarios will occur during or after the installation of MobiControl:

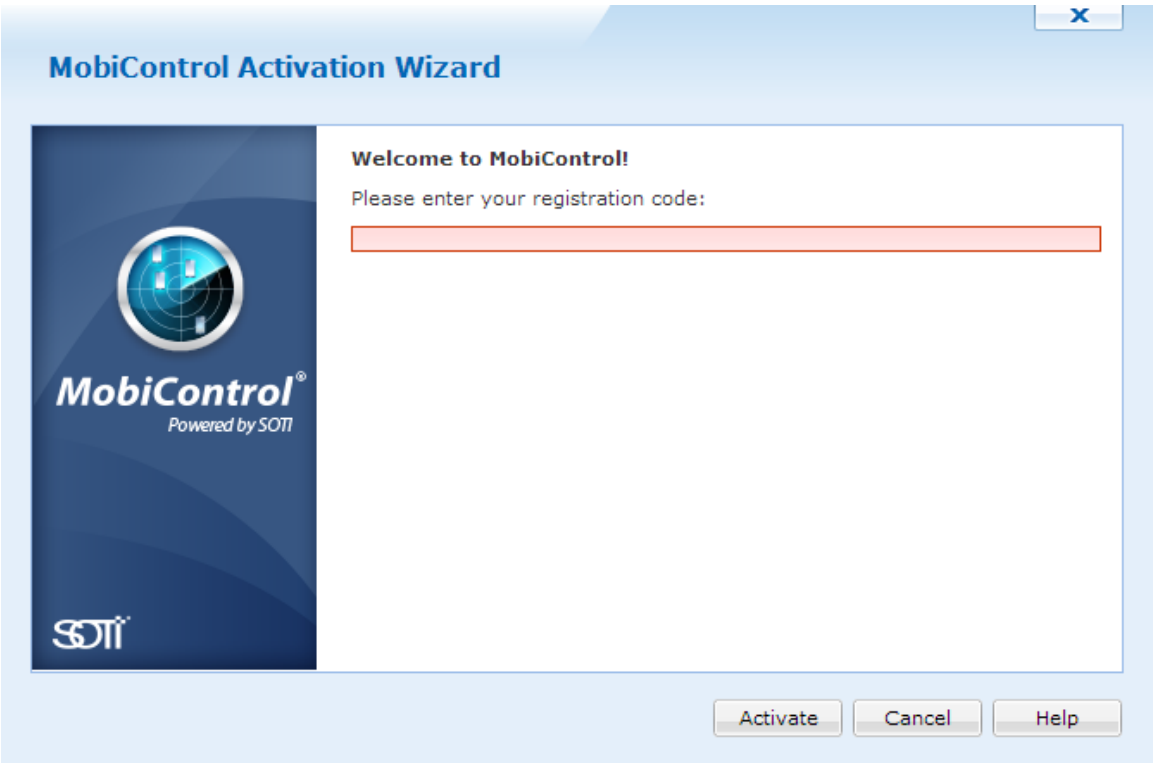
1. Clean Installation of MobiControl
2. Upgrade to v9.03 or later Required

In this section, there is also information available about how to change your registration code:

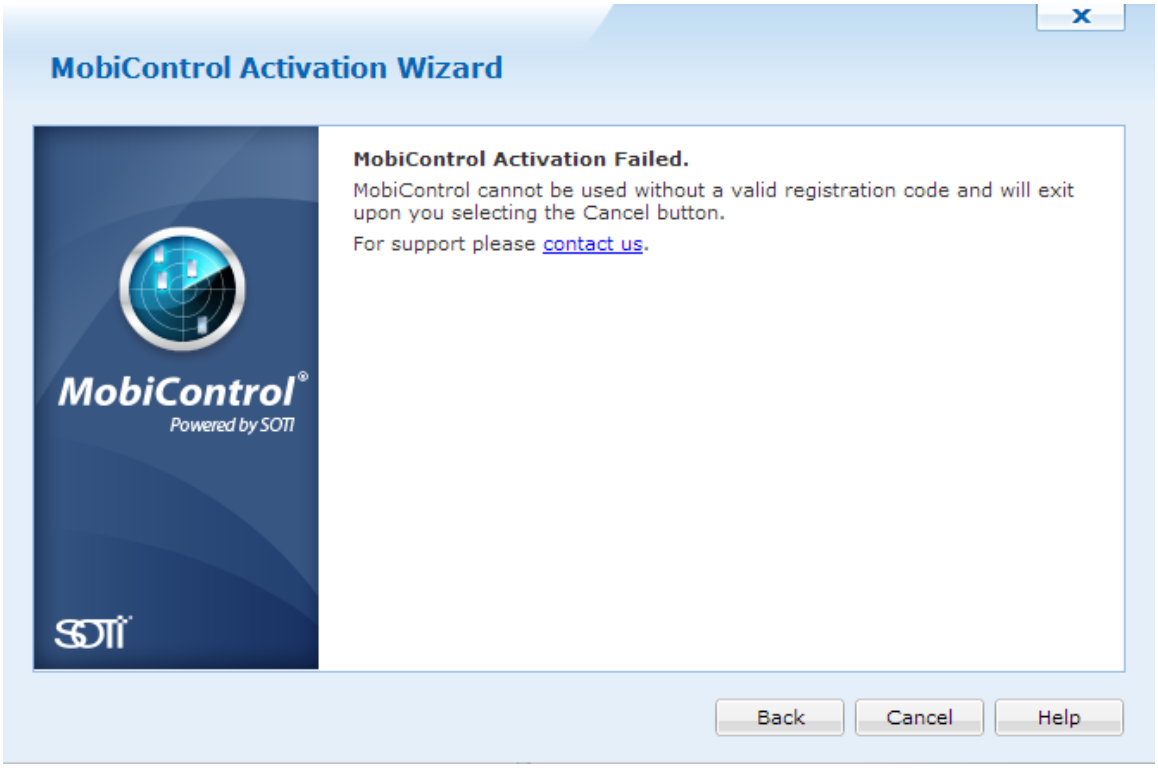
- Changing your Registration Code

Clean Installation of MobiControl

When MobiControl finishes installing completely, a registration window will open up requesting a registration code. If you don't have a valid registration code or you are upgrading to version 6 or later, you can visit our website to sign up for a 31-day trial registration code or contact us to get a new registration code. If your trial expires, you will be prompted to enter a new registration code.



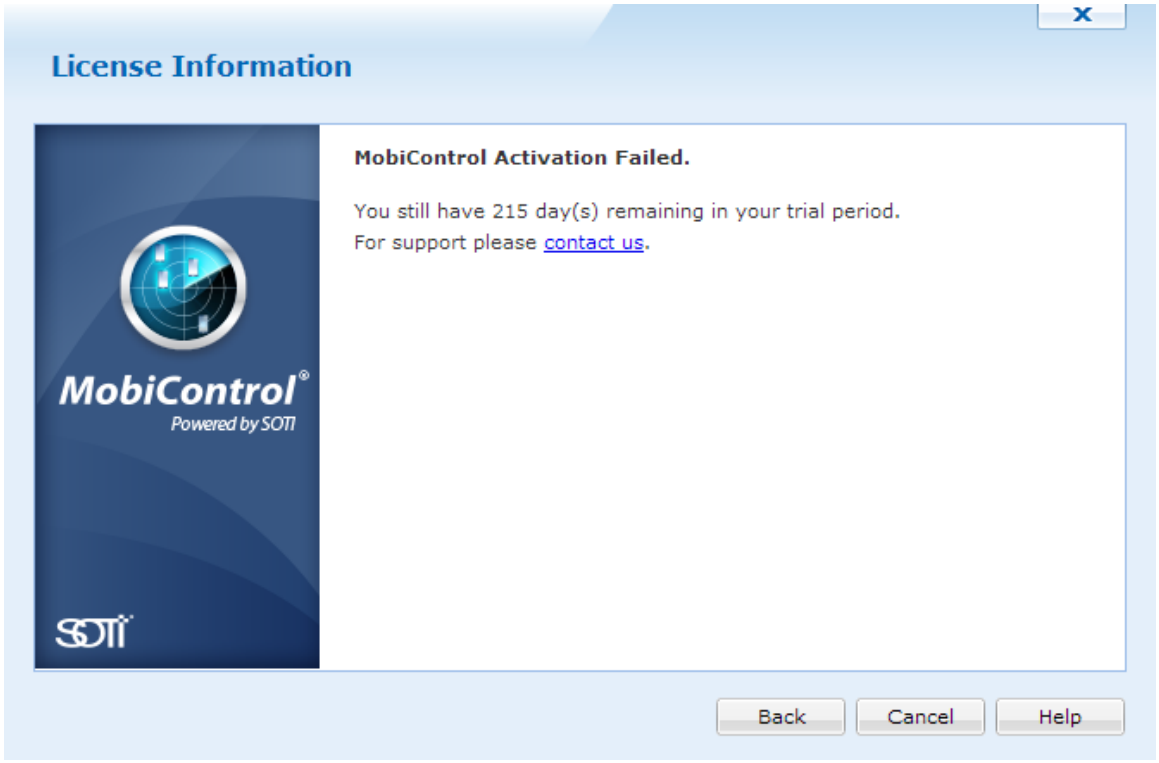
If you enter an invalid registration code, clicking **Activation** will result in the following error message:



s

If your registration code has already been used to activate another instance of MobiControl or the activation failed, then the following message will be displayed. If you require another activation on your registration code please Contact Us.

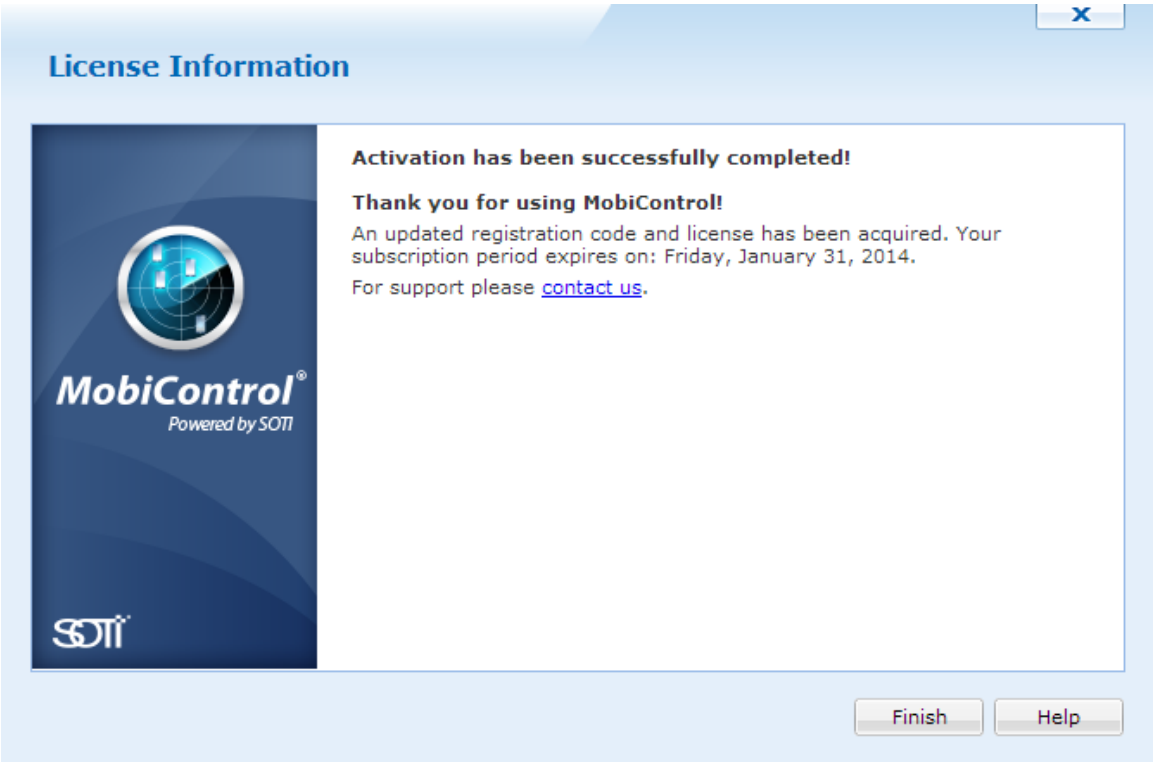
MobiControl will give you a 30 day grace period if activation fails.


License Information
MobiControl
Powered by SOTI
MobiControl Activation Failed.
You still have 215 day(s) remaining in your trial period.
For support please contact us.
Back
Cancel
Help

Upgrade to v9.03 or later Required

During installation, after selecting the type of install, you may be required to enter a new registration code. This will only appear if you have a registration code that is an older format. To exchange or to obtain your new registration code, you must contact us and provide your existing registration code followed by the company name and the person to whom the product is licensed.

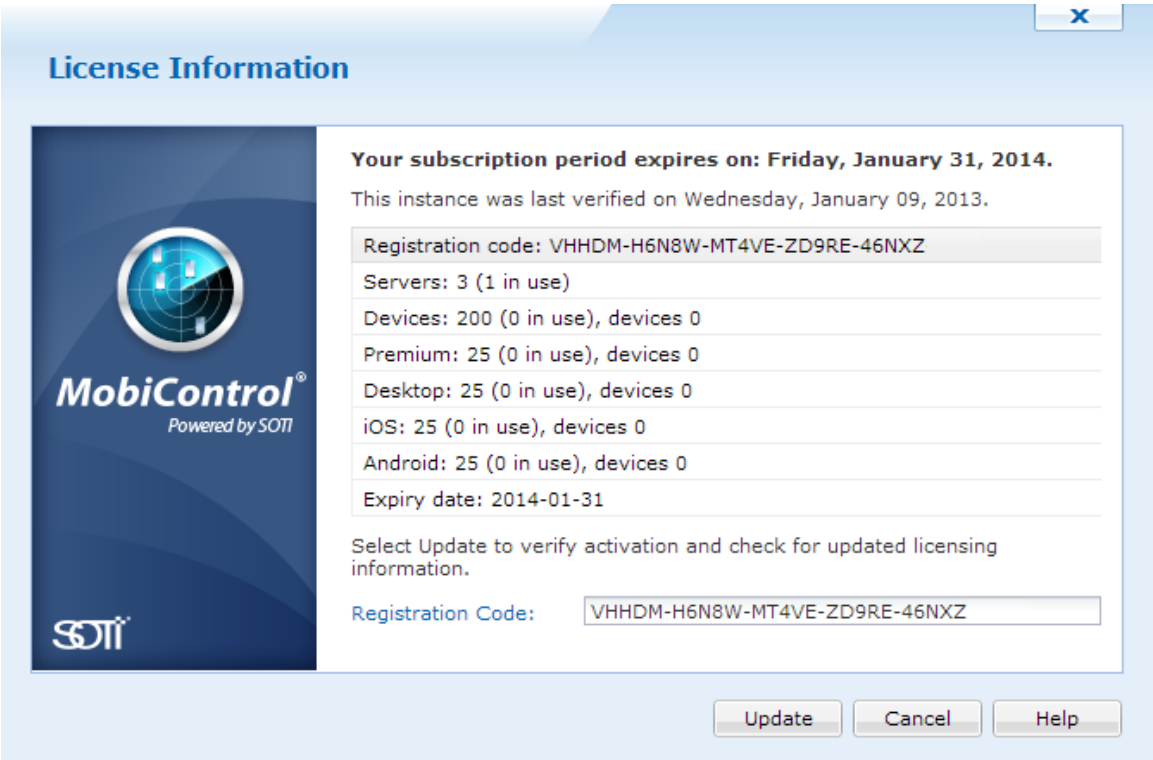
After receiving your new registration code, you will now be able to successfully activate the product.



Changing your Registration Code

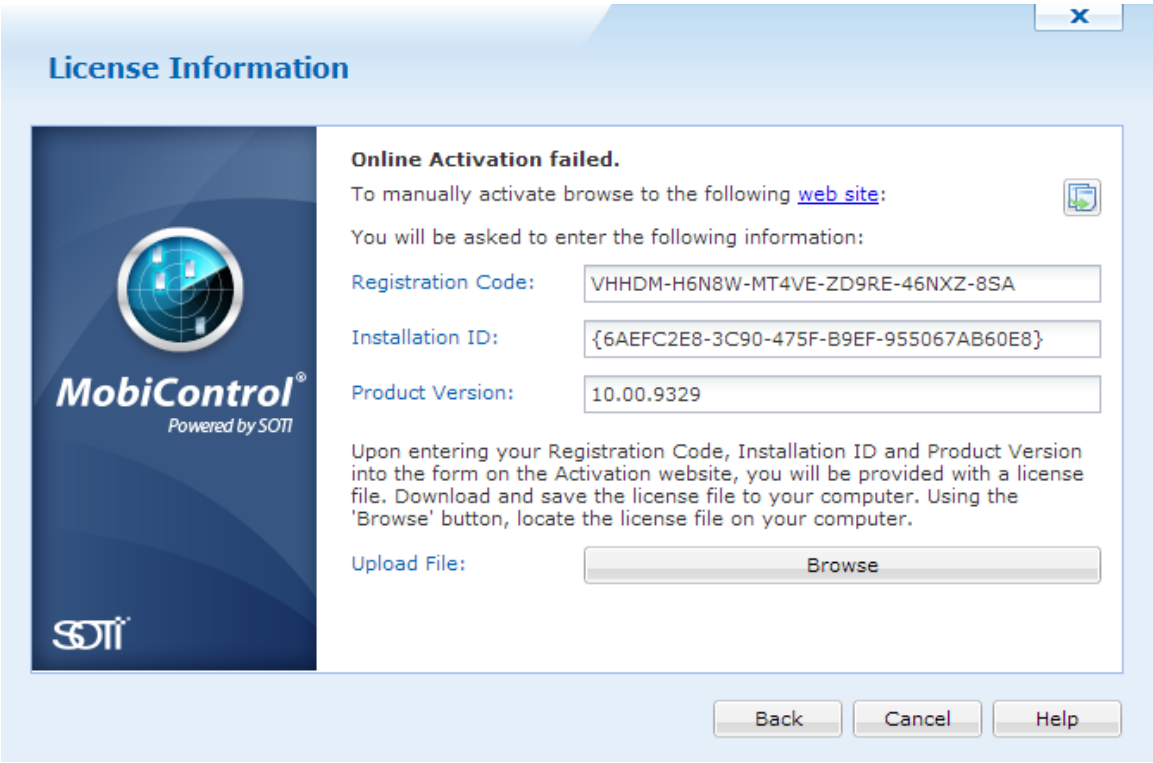
In the MobiControl Manager, open the **Help** menu and click **License Information,** and a window will pop up where you can enter a valid registration code.

In v9.03 or later, when you receive a new registration code (for adding devices, or extending service periods) you do not need to update your registration code manually, this update will take place automatically. The deployment server service does a periodic check every day to verify the registration information is correct and up to date.

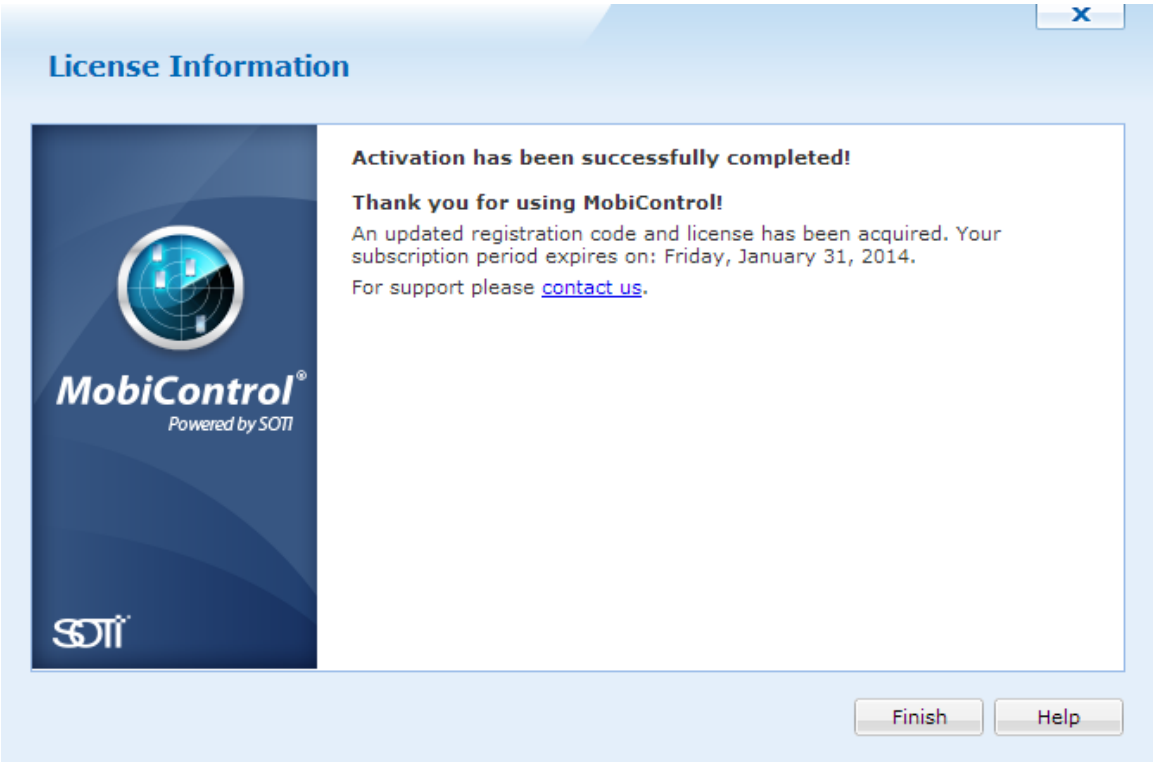


Manually Registering MobiControl

If there is no Internet connection available, or if MobiControl is unable communicate with the activation servers you will be prompted to manually activate MobiControl.



Navigate to http://activate.soti.net/MCActivation on a machine that does have access to the Internet and enter the information provided to you by the Manual Activation Wizard. Once you have successfully activated on the Activation website, you will be provided with a License File. Browse to the License file provided by the Activation website and click Activate.



Once you have successfully activated MobiControl you will be able to use all of its features.

Database

MobiControl uses a database to store configuration information and files that need to be accessed by MobiControl components. MobiControl can store configuration information and files (such as package files that are to be deployed, as well as other files) in an existing database server or can use a free Microsoft SQL Server database (e.g. MSDE) included with MobiControl.

MSDE is the Microsoft SQL Server 2000 database engine, without any UI tools, and with some limitations in the database size (i.e. maximum of 2 GB for data storage) and the number of connections. MSDE is a good, affordable starting database to use with MobiControl. If the number of mobile devices you are managing with MobiControl grows beyond the capabilities of MSDE, you can easily upgrade to a full Microsoft SQL Server database. Our testing results show that MSDE performs well for MobiControl sites that are managing up to 500 devices.

NOTES:

- MSDE is not supported on the Microsoft Vista operating system.
- Microsoft SQL Server 2005 Express Edition requires the installation of Microsoft's .NET Framework v2.0.

Microsoft SQL Server 2005 Express Edition is also a free database engine, however, unlike MSDE, it provides some basic UI tools and does not have as many performance limitations. Our testing results show that Microsoft SQL Server 2005 Express Edition performs well for MobiControl sites that are managing up to 1000 devices.

MobiControl currently supports the following databases:

- Microsoft SQL Server 2005
- Microsoft SQL Server 2005 Express Edition
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 Express Edition (included with MobiControl)
- Microsoft SQL Server 2012
- Microsoft SQL Server 2012 Express Edition

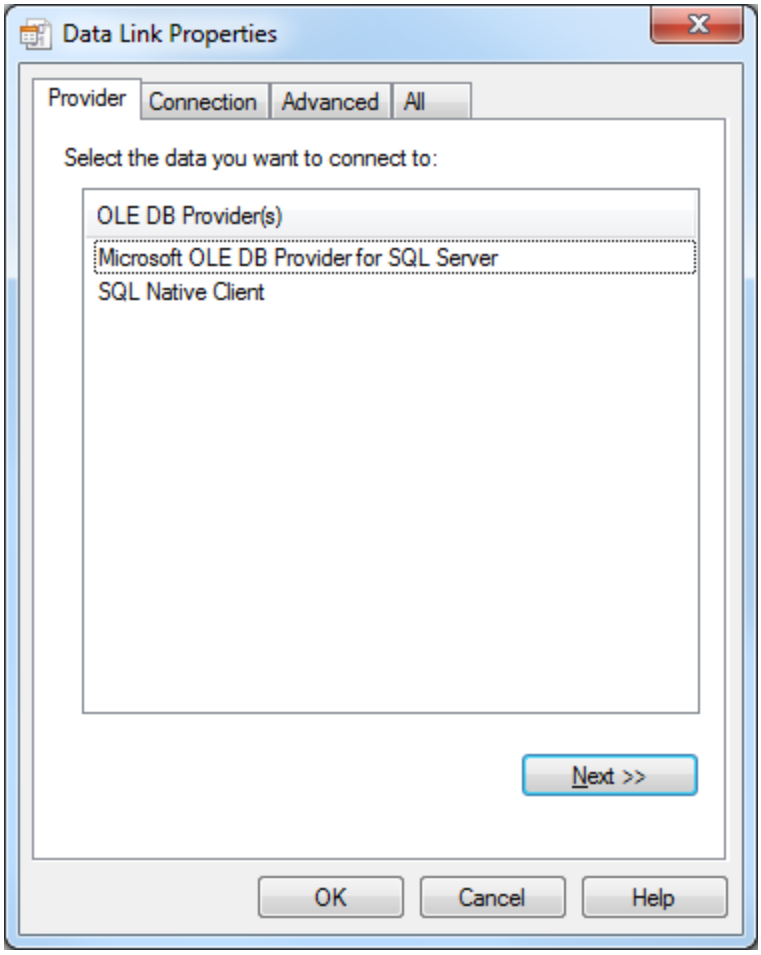
Please see the "Database Configuration" topic on page 463 for detailed information about configuring MobiControl's database connection. Please see the "Log Maintenance Options" topic on page 406 to learn about incorporating automatic log maintenance features to your database.

Database Configuration

The MobiControl installer includes Microsoft SQL Server 2005 Express Edition. The installer also includes an option to connect to an existing database server if there is already one set up on the network.

Configuring MS SQL Server

If this is a first-time installation, or you are changing the database settings, the **Data Link Properties** dialog box will appear during setup. It can also be opened from MobiControl Manager: click **Tools**, and then **Options**.



Provider tab of the Data Link Properties dialog box

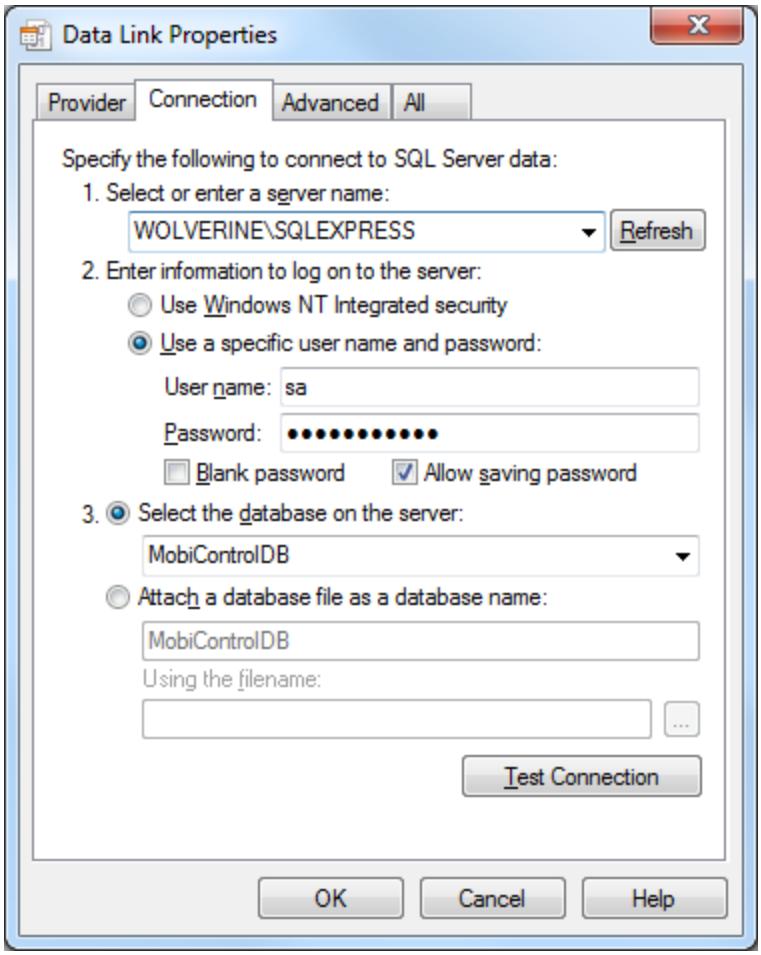
On the **Provider** page, select **Microsoft OLE DB Provider for SQL Server** and then click **Next**.

The **Connection** page will then be displayed. On the **Connection** page, select the database server from the list or enter the server name.

Choose **Use a specific user name and password**, enter the user name and password and make sure that **Allow saving password** is selected.

If you are accessing the **Data Link Properties** dialog box through the setup program and are configuring a MobiControl Database for the first time, leave the **Select the database on the server** field blank, otherwise select **MobiControlDB** from the list.

Click **OK**



Connection tab of the Data Link Properties dialog box

NOTE:

You will need to supply the user name and password credentials for a user that has WRITE access to the database, as the MobiControl setup will create a new database (or upgrade an existing database) before continuing with the installation

Installing MobiControl

First-time Installation

MobiControl uses a database to store configuration information. When installing MobiControl, you can install the database on the same computer on which other MobiControl components are installed, or you can install the database on a separate computer.

MobiControl currently supports the following databases:

- Microsoft SQL Server 2005 (Express, Standard, Workgroup, Developer, Enterprise)
- Microsoft SQL Server 2008 (Express, Standard, Workgroup, Web, Developer, Enterprise)
- Microsoft SQL Server 2012 (Express, Standard, Workgroup, Web, Developer, Enterprise)

Microsoft SQL Server 2008 Express Edition can be downloaded for free with MobiControl.

The MobiControl installation program can configure the MobiControl database on an existing database server or it can install a free database server (included in the setup program) and then configure the database.

NOTE:

Microsoft .NET Framework 4 is required in order to install MobiControl. If it is not installed on your system, it can be downloaded from here.

The MobiControl management service requires access to the Internet to be able to build agents, activate, and locate device. If this cannot be done, please contact us so that we may assist with the set up.

To install MobiControl, select and run the appropriate setup program and follow the instructions. The following is a description of the main screens of the setup program.

1. Accept the license agreement.

   Please read the License Agreement carefully. To install MobiControl, you need to accept the license agreement. If you agree with the License Agreement, please click **Yes,** otherwise click **No.** If you click **Yes,** the Setup Wizard will proceed.


SOTI MobiControl Setup
MobiControl
Powered by SOTI
SOTI
License Agreement
SOTI MOBICONTROL END USER SOFTWARE LICENSE AGREEMENT
PLEASE READ THE FOLLOWING SOFTWARE LICENSE AGREEMENT ("License") CAREFULLY BEFORE USING THE SOFTWARE. BY INSTALLING THE SOFTWARE, YOU ARE AGREEING TO BE LEGALLY BOUND BY THE TERMS AND CONDITIONS OF THIS LICENSE AS WELL AS SOTI'S TERMS OF USE AND PRIVACY POLICY PROVIDED FOR ON THE SOTI WEBSITE. SOTI MAY AT ANY TIME, WITHOUT PRIOR NOTICE TO YOU, REVISE THE TERMS OF USE AND PRIVACY POLICY WHICH SAID REVISIONS WILL BE EFFECTIVE ONCE POSTED ON THE SITE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE DO NOT INSTALL OR USE THE SOFTWARE AND PROMPTLY EXIT THE SETUP SOFTWARE AND RETURN ALL ACCOMPANYING ITEMS (INCLUDING ALL FORMS OF DOCUMENTATION) TO THE ORIGINAL PLACE OF ORIGIN.
This License was last updated on August 25, 2011 and is effective between Licensee and SOTI as of the date of the Licensee accepting this License.
1. DEFINITIONS
"Device" means any computing device/instrument that is supported by the Software.
"Documentation" means all reference materials provided with the Software.
"Licensee" means the end user or the entity, who agrees to the terms and conditions of this license agreement and to whom this License is granted. "You" and "Your" will be understood
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
InstallShield
< Back
Next >
Cancel
Help

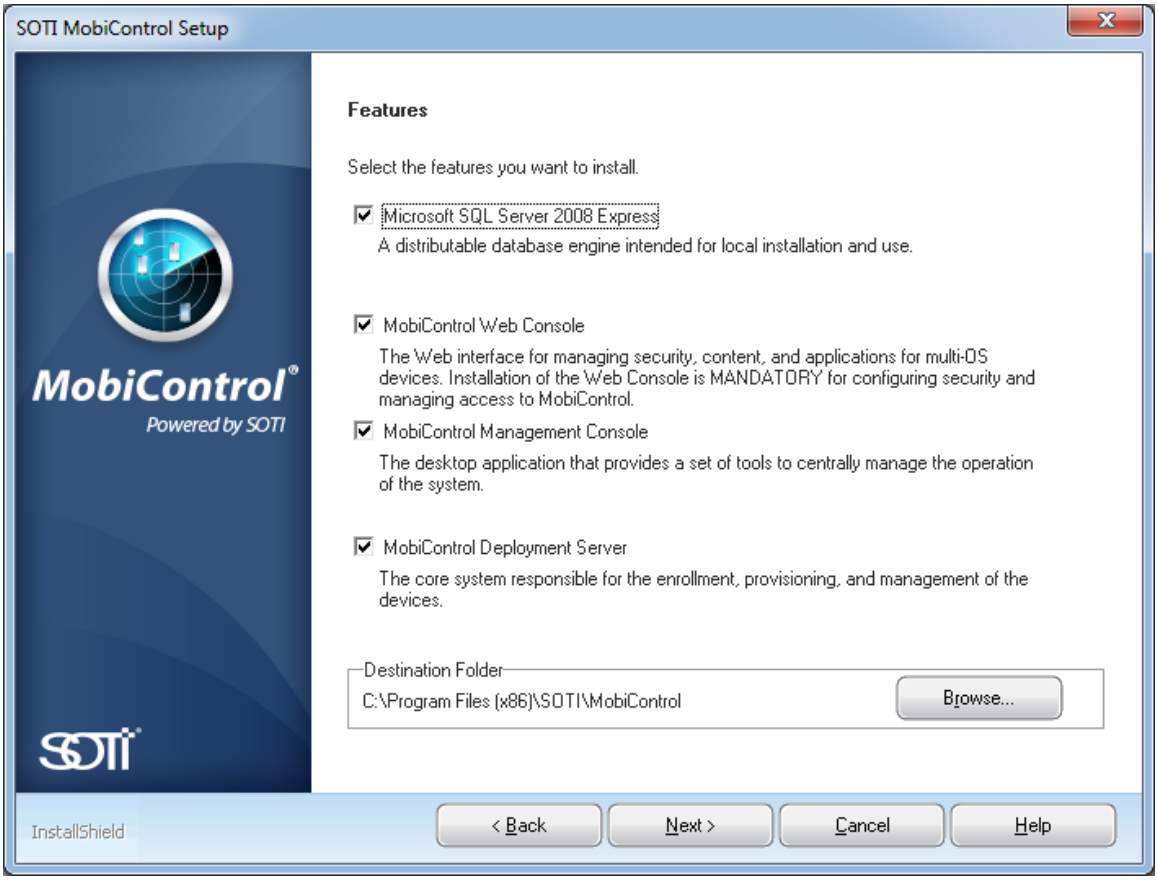
2. Select the MobiControl Features and installation directory.
    - Select Microsoft SQL Server 2008 Express if a SQL Server needs to be installed on the server.
    - Select the **Web Console** option to install the MobiControl Web Console
    - Select the **MobiControl Manager** option to install the MobiControl Manager (MobiControl Manager) and Package Studio. This option is recommended when you are adding an additional Management console to an existing MobiControl installation, for instance, for a new help desk staff member.

      Select the **Deployment Server** option to install the Deployment Server. It is recommended to install the Management Console on any computer on which you are installing the Deployment Server.
    -
    - Selecting the MobiControl Web Console will allow us to manage all Windows Mobile, Windows Desktop, iOS and Android devices.

      NOTE:

      The Web Console is required to manage iOS and Android devices. To manage iOS devices, we would need to create an APNS certificate. Click here to see how to create this certificate.

    You may save MobiControl software in the default folder. If not, click **Browse** and select the folder you wish.

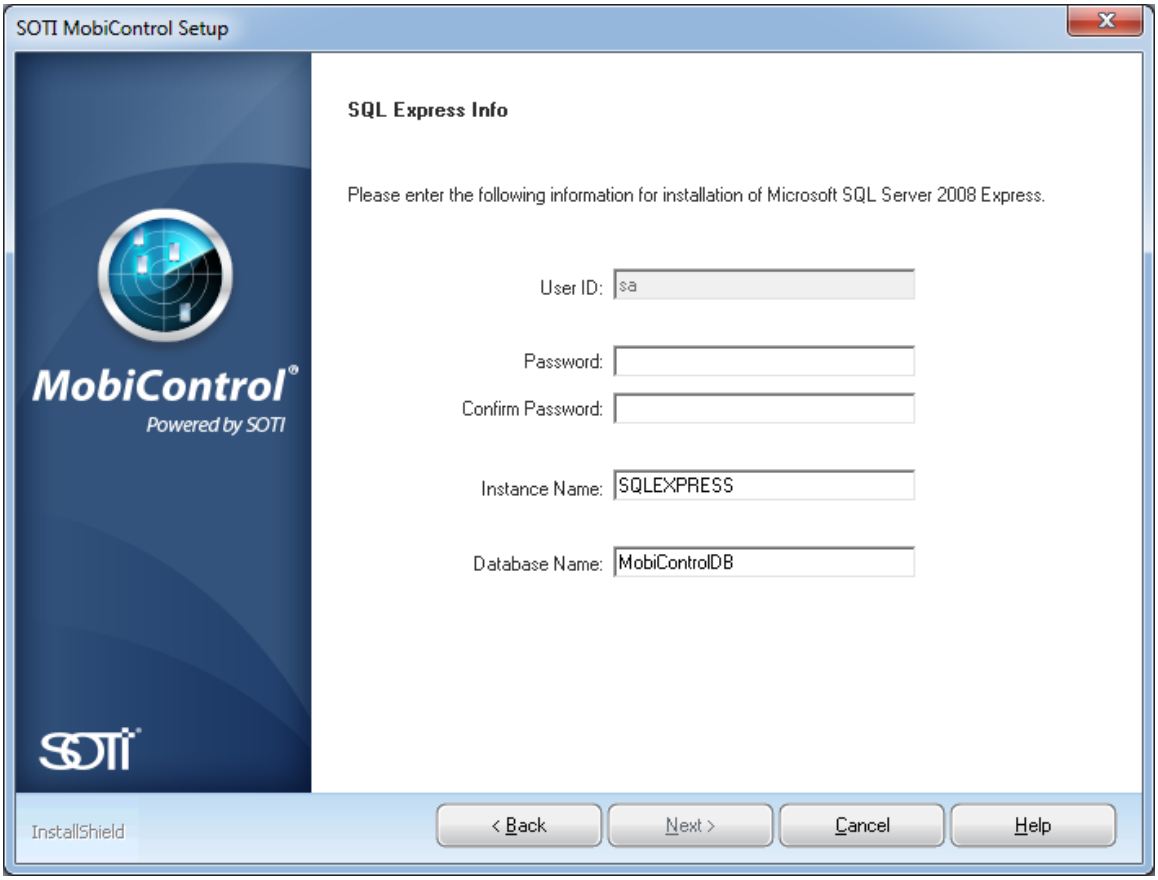


NOTE:

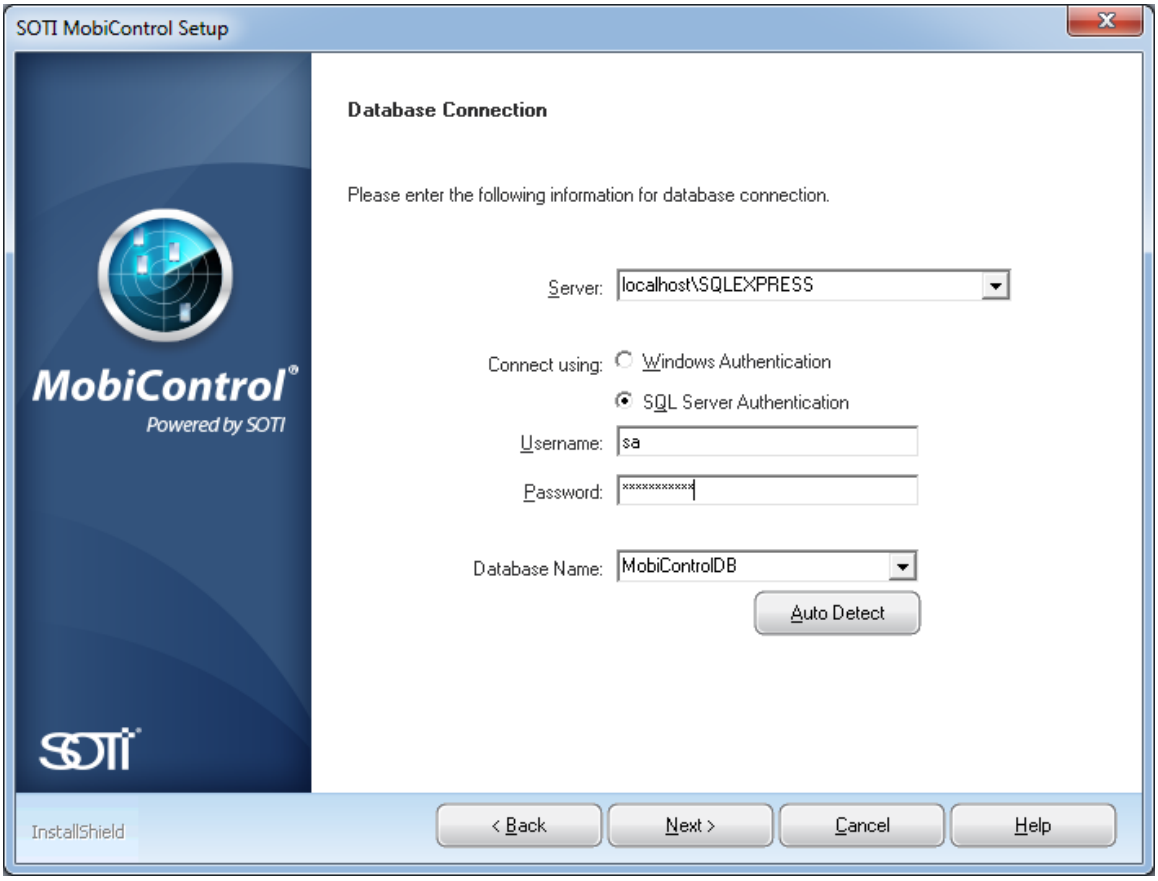
The MobiControl installation will check to see if a Deployment Server already exists before installing a new or an additional Deployment Server. If the maximum number of active Deployment Server licenses has been reached, you will be unable to install a new one and you will be prompted to install only the Manager console. To install an additional Deployment Server, disable an active one first. You may activate only as many Deployment Servers as the number of licenses you own.

3. Setting up the database connection.

   If Microsoft SQL Server 2008 Express has been selected on the previous screen, MobiControl will prompt us to enter a new user name and password for the SQL Server.

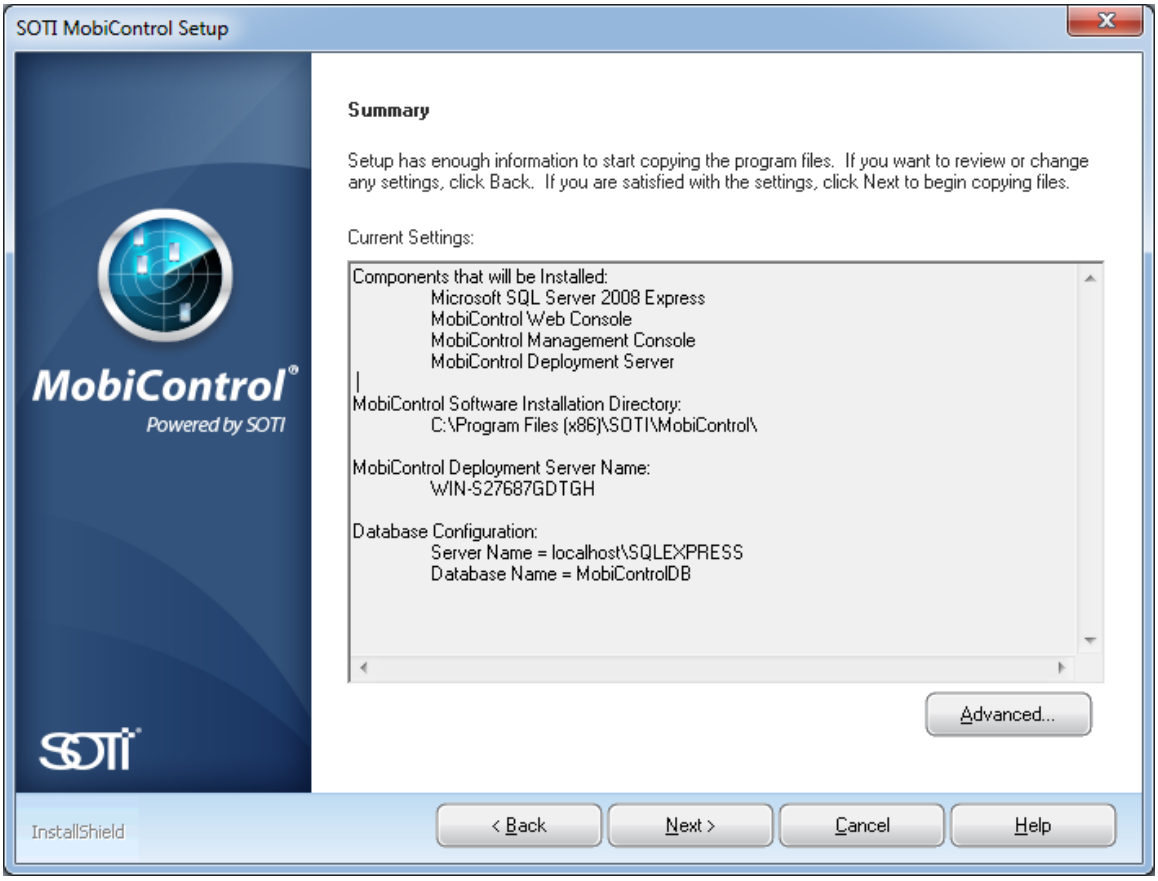


If MobiControl has detected a database, the following screen will appear:


SOTI MobiControl Setup
MobiControl
Powered by SOTI
Database Connection
Please enter the following information for database connection.
Server:
localhost\SQLEXPRESS
Connect using:
Windows Authentication
SQL Server Authentication
Username:
sa
Password:
Database Name:
MobiControlDB
Auto Detect
InstallShield
< Back
Next >
Cancel
Help

4. Confirm installation settings.

   This below screen displays a summary of the selected settings. If you want to change any settings, click **Back,** else click **Next** to confirm the settings and initiate the installation.



5. Advanced Settings.

The Advanced settings page will allow us to change the Site name, Device Management Address, the Web Console instance name, deployment server name, and ports used.

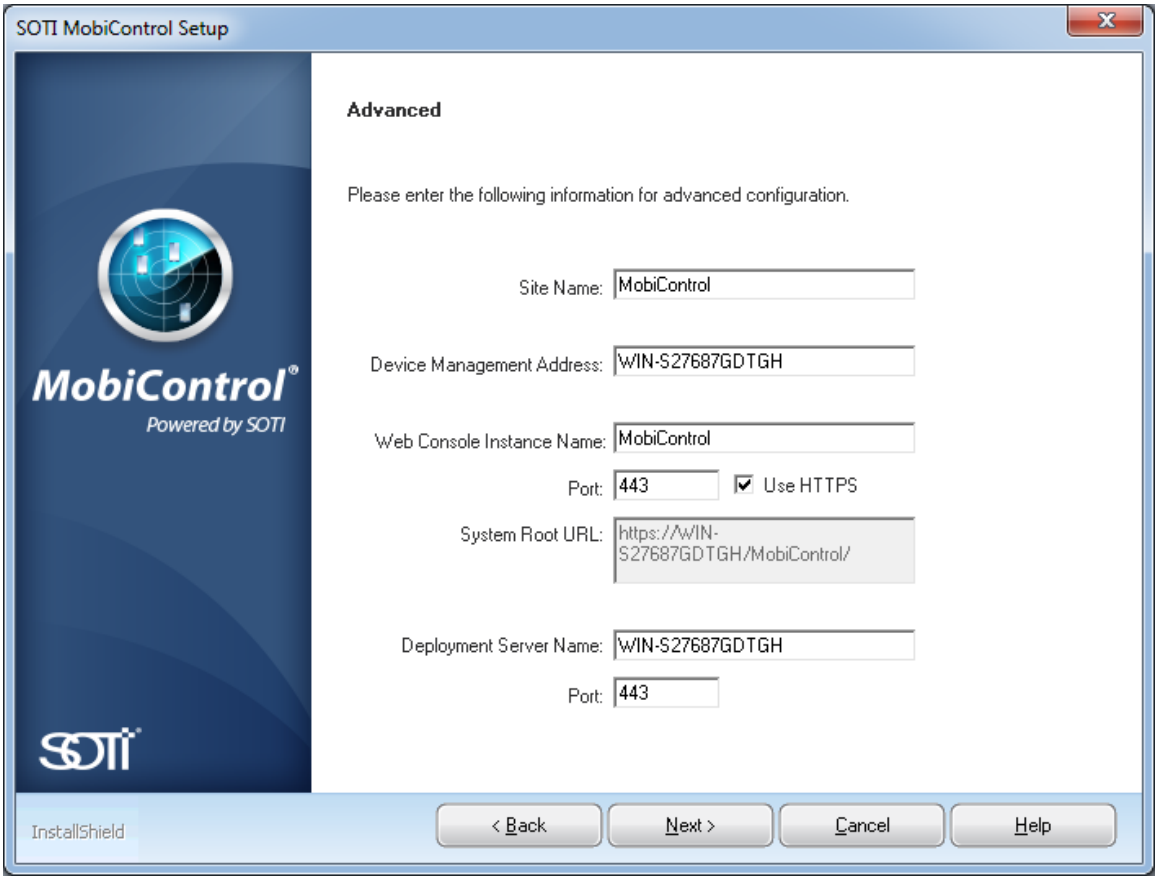
If the Web Console instance name is left blank, the Web Console URL will be the root URL based on the Device Management Address name.

EXAMPLE:

With previous versions of MobiControl the default URL for the Web Console will be *Device Management Address/MobiControl*. If the Web Console Instance name is left blank, then the Web Console URL will just be the *Device Management Address*.

IMPORTANT:

Changing leaving the Web Console Instance name blank will redirect all traffic to MobiControl. If there are other websites being hosted on the deployment server, they will be redirected to MobiControl. Only utilize this if there are no other websites being used.



6. Installation is Complete.

Please see the "MobiControl Tutorial" topic on page 3 once installation is complete.

Re-installing MobiControl

If MobiControl needs to be reinstalled, or repaired, re-run the MobiControl installation file.

IMPORTANT:

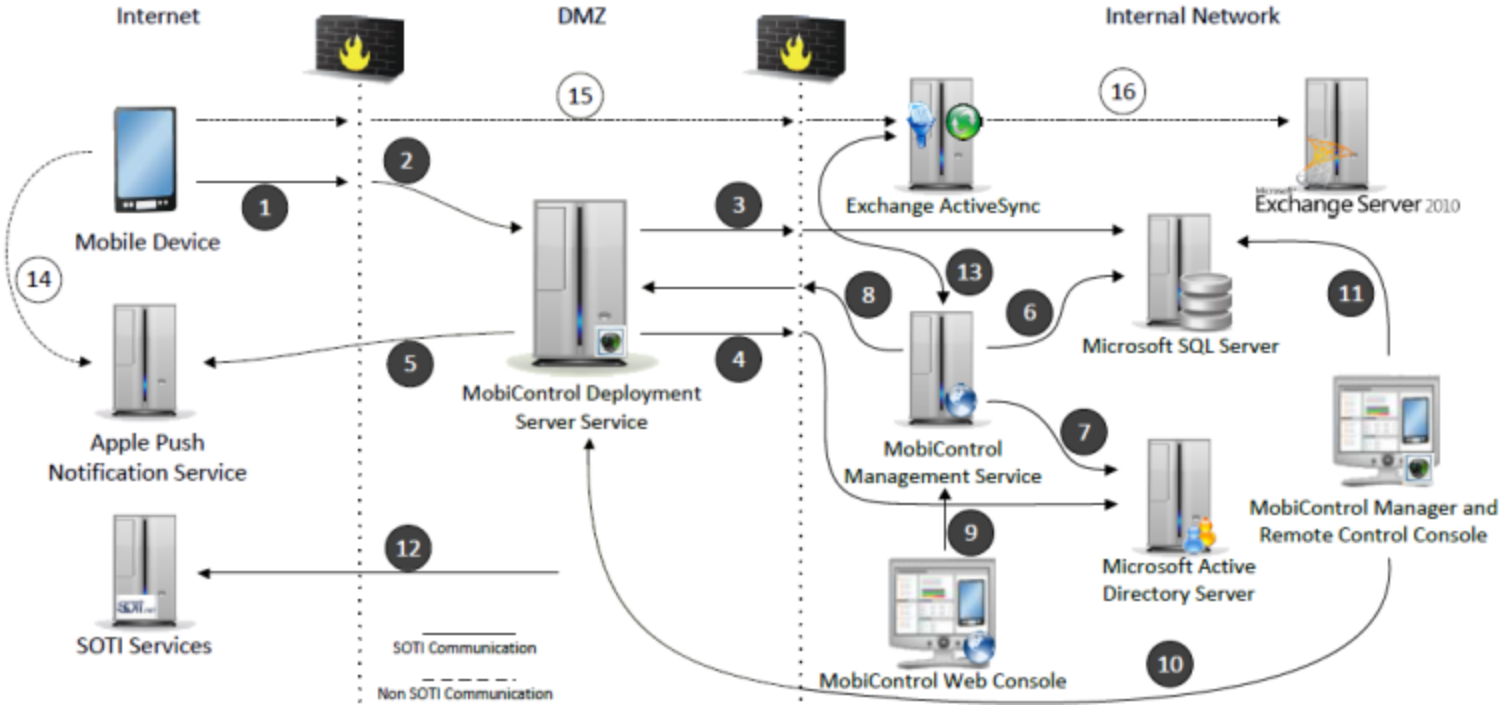
If a feature is unchecked, it will be uninstalled. Please make sure that nothing is unchecked if those features wished to be remained.

NOTE:

If the built-in resource files in the MobiControl database, such as the Device Agent `.cab` installation files, need to be re-written to the database to correct a problem, run the installer executable from the command line with the additional parameter "`-UpdateDB`."

MobiControl network diagram

The diagram below shows all components that MobiControl uses so that devices and consoles are able to connect properly. If any clarification is needed, please do not hesitate to contact us.



#	Network Connection Details	Protocol	Port(s)
1	MobiControl Device Agent connects to MobiControl Server via firewall/gateway	Binary/HTTPS	5494/443
2	Firewall/Gateway port forwards traffic on designated inbound ports to ports on host computer running MobiControl Server	Binary	5494/443
3	MobiControl Server connects to Microsoft SQL Server	Binary	1433
4	MobiControl Server connects to Microsoft Active Directory Server	LDAPS	636
5	MobiControl Server connects to Apple Push Notification Service (APNS) for communication/feedback	Binary	2196/2195
6	MobiControl Web Console connects to Microsoft SQL Server	Binary	1433
7	MobiControl Web Console connects to Microsoft Active Directory Server	LDAP	389
8	MobiControl Management Service connects to MobiControl Server	Binary	5495/5494
9	Web browser connects to MobiControl Management Service	HTTP(S)	443
10	[[[Undefined variable Terms.file_MCMgr]]] and Remote Control Consoles connect to MobiControl Server	Binary	5494
11	MobiControl Manager connects to Microsoft SQL Server	Binary	1433

#	Network Connection Details	Protocol	Port(s)
12	MobiControl Manager, Server and Web Console connect to SOTI Services (Activation, Agent Builder, Enrollment, Location, Messaging, Skins)	HTTP(S) /Binary	443/80
13	Exchange Filter connects to Exchange Filter Service (running with Management Service)	Binary	443
14	Apple iOS devices connect to Apple Push Notification Service (APNS)	Binary	5223
15	Device connects to Exchange ActiveSync Server (EAS) to retrieve email	Binary	443
16	Exchange ActiveSync Server communicates with Exchange Server	Binary	443

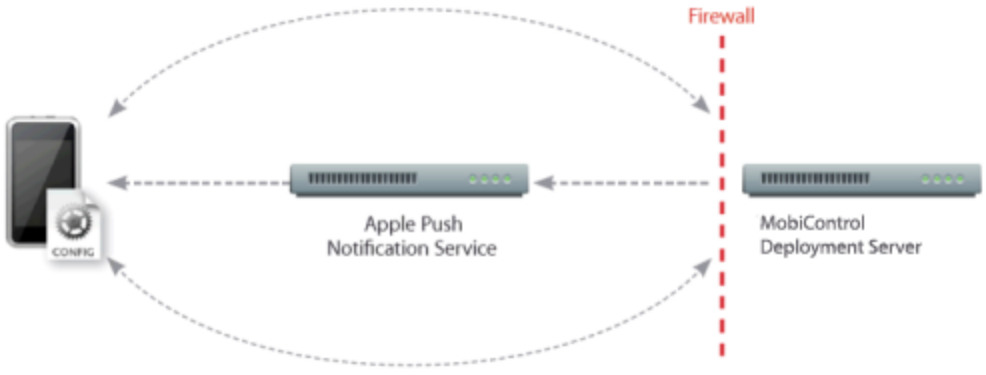
**All communication is TCP based using the protocol outlined above*

APNS Certificate

What is an APNS Certificate?

iOS Devices support Mobile Device Management (MobiControl), providing the ability to manage deployments of iOS Devices across organizations. These Mobile Device Management capabilities are built upon existing iOS Devices technologies like Configuration Profiles, Over-the-Air Enrolment, and the Apple Push Notification Service (APNS). This gives IT departments the ability to securely enrol iOS Devices in an enterprise environment, wirelessly configure and update settings, monitor compliance with corporate policies, and even remotely wipe or lock managed iOS Devices.

Management of iOS Devices takes place via a connection from the Deployment Server to the Apple Push Notification Service. When the Deployment Server wants to communicate with iOS Devices, a silent notification is sent to the device prompting it to check in with the Apple Push Notification Service. The device communicates with the server to see if there are tasks pending and responds with the appropriate actions. These tasks include updating policies, providing requested device or network information, or removing settings and data. The Communication between the Deployment Server and Apple Push Notification Service is secured requiring the use of a Certificate installed on the Deployment Server.



To create an APNS certificate, we should use the iOS APNS Certificate Generator.

Please see the "Installing the APNS Certificate" topic on page 508 for information on the iOS Certificate Generator.

If the iOS APNS Certificate Generator is not functioning correctly, we can go through one of the below steps (depending on your OS) to request a APNS certificate.

Please see the "APNS Certificate Request for Windows Server 2003" topic below if you are running Windows Server 2003.

Please see the "APNS Certificate Request for Windows Vista, Server 2008 or Windows 7" topic on page 491 if you are using Windows Vista, Server 2008 or 7.

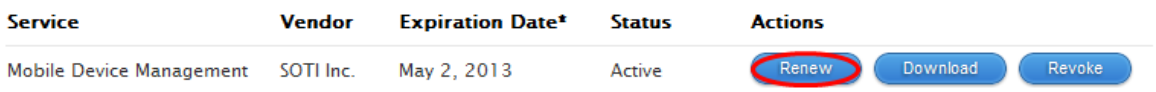
Please see the "APNS Certificate Request for OS X" topic on page 501 if you are running OS X.

After completing the steps outlined above, a valid **Apple Push Notification Service** Certificate will exist in the Windows Certificate Store on the Deployment Server, enabling MobiControl to use the Apple Push Notification Service to communicate with iOS Devices devices.

IMPORTANT:

The certificates that have been downloaded from Apple have a 1 year expiration date. To ensure that devices do not have to be re-enrolled into MobiControlwhen a certificate expires, the certificate has to be renewed.

The process of renewing a certificate is almost the same as creating a new one. The main difference when renewing a certificate is to select **Renew** rather than create a certificate. Once you renewed the certificate, it will need to installed into MobiControl again. Please see the "Installing the APNS Certificate" topic on page 508 for more information on how to install the APNS certificate.



Renewing a APNS certificate

APNS Certificate Request for Windows Server 2003

Windows Server 2003

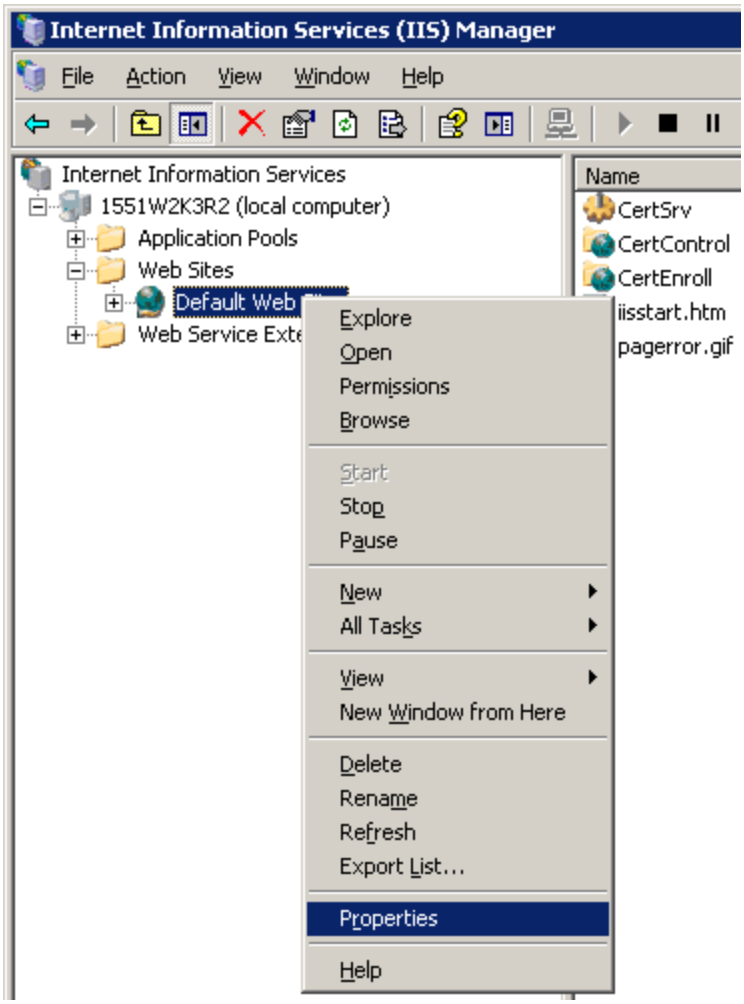
The following instructions are used for creating an APNS certificate request on Windows Server 2003.

NOTE:

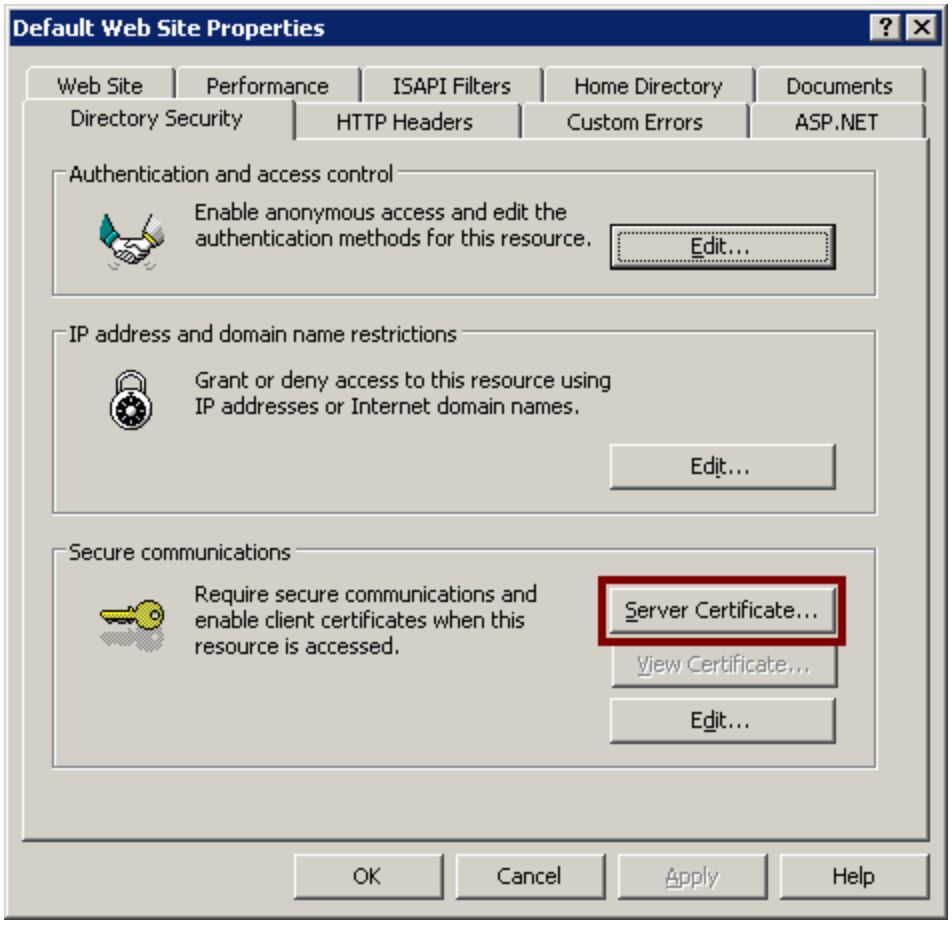
An APNS request can be done from any computer and does not have to be done from a computer with MobiControl installed on it.

1. Create the Certificate Request

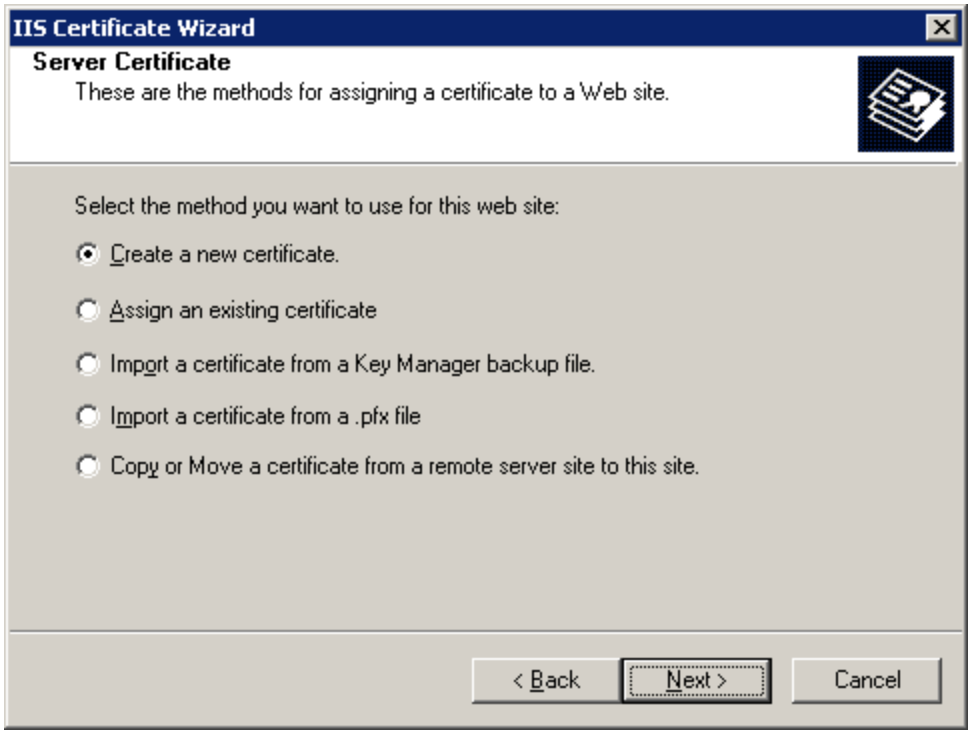
   To create a new APNS Certificate Request, open the *Internet Information Services* Manager (IIS). Once inside the IIS Manager, right click on the **Default Website** and select **Properties**.



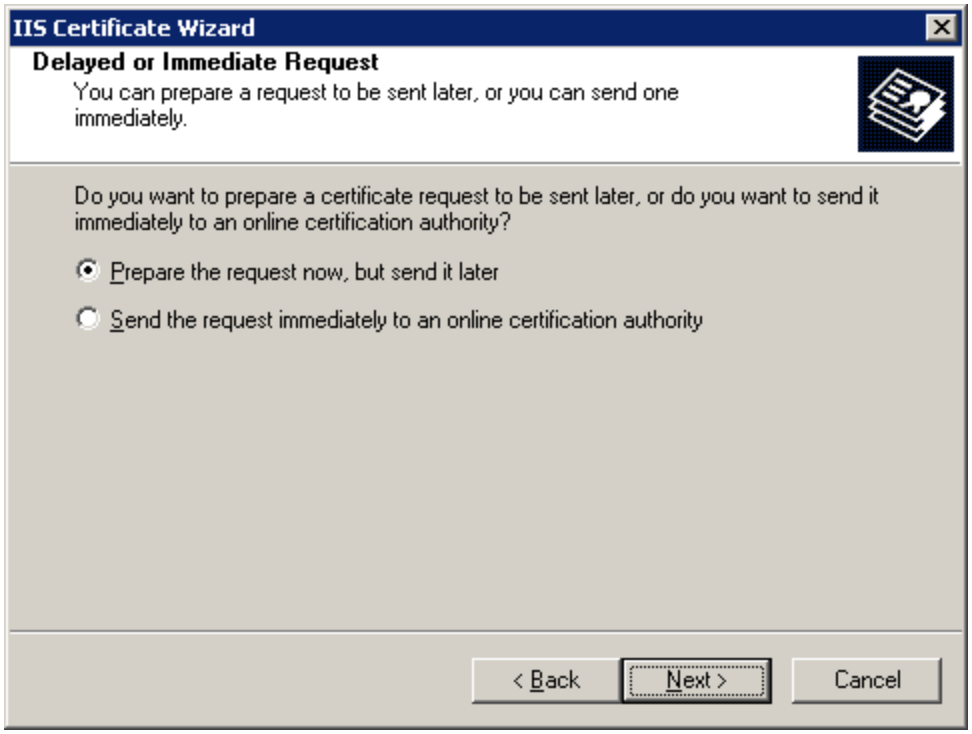
From the **Properties** window click on the **Directory Security** tab and click the **Server Certificate** button.



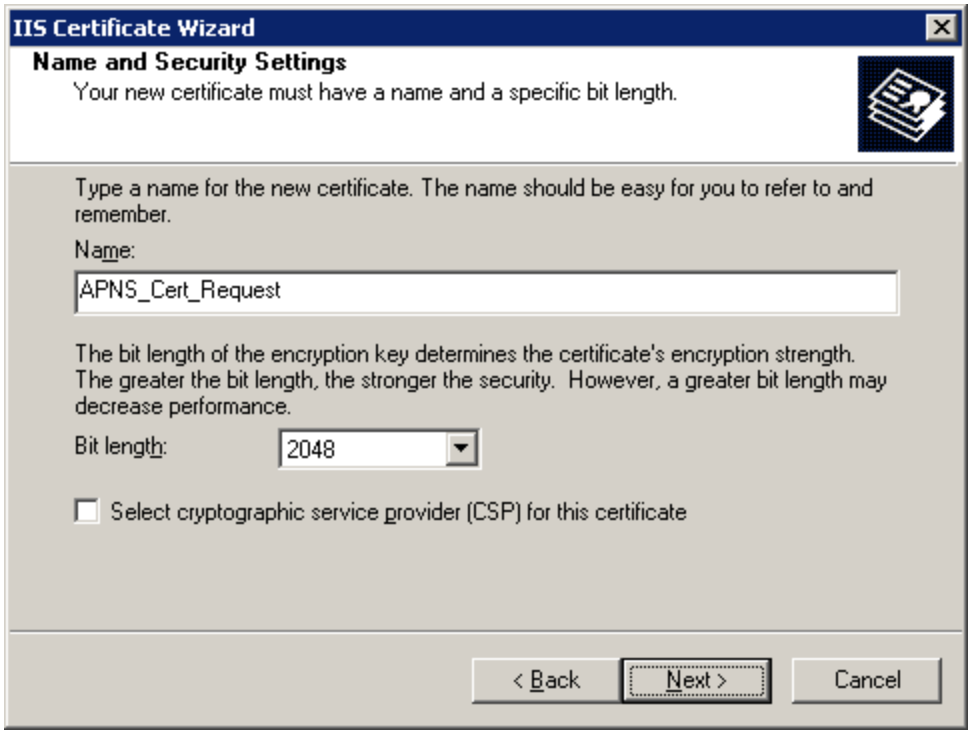
Once the wizard starts click **Next**, select **Create a New Certificate** and click **Next**.



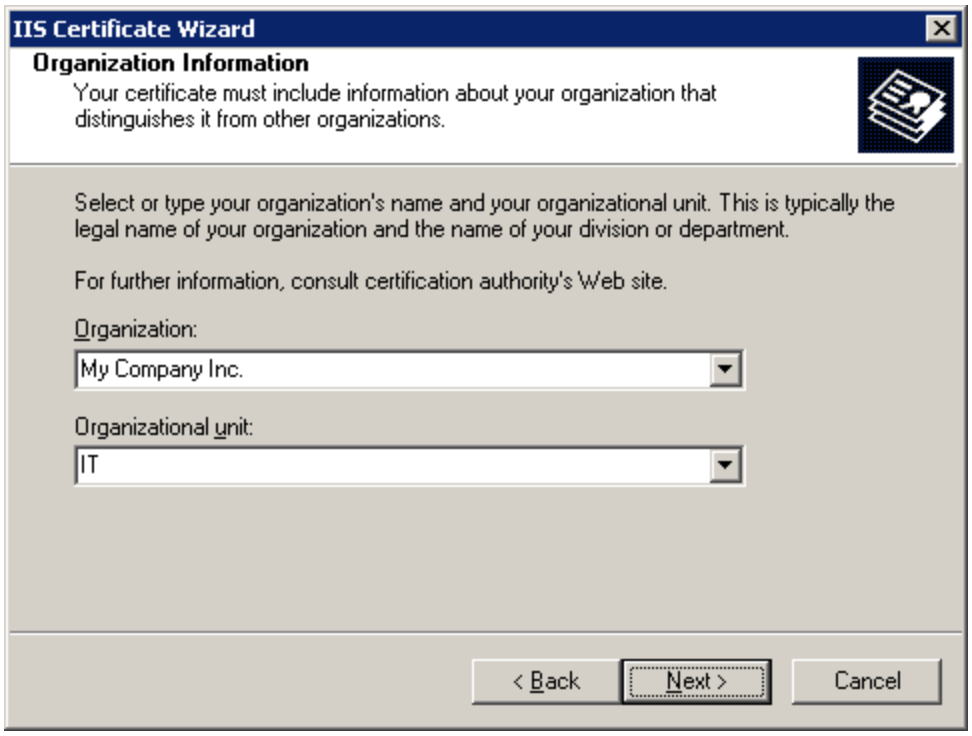
Select **Prepare the request now, but send it later** and click **Next**.



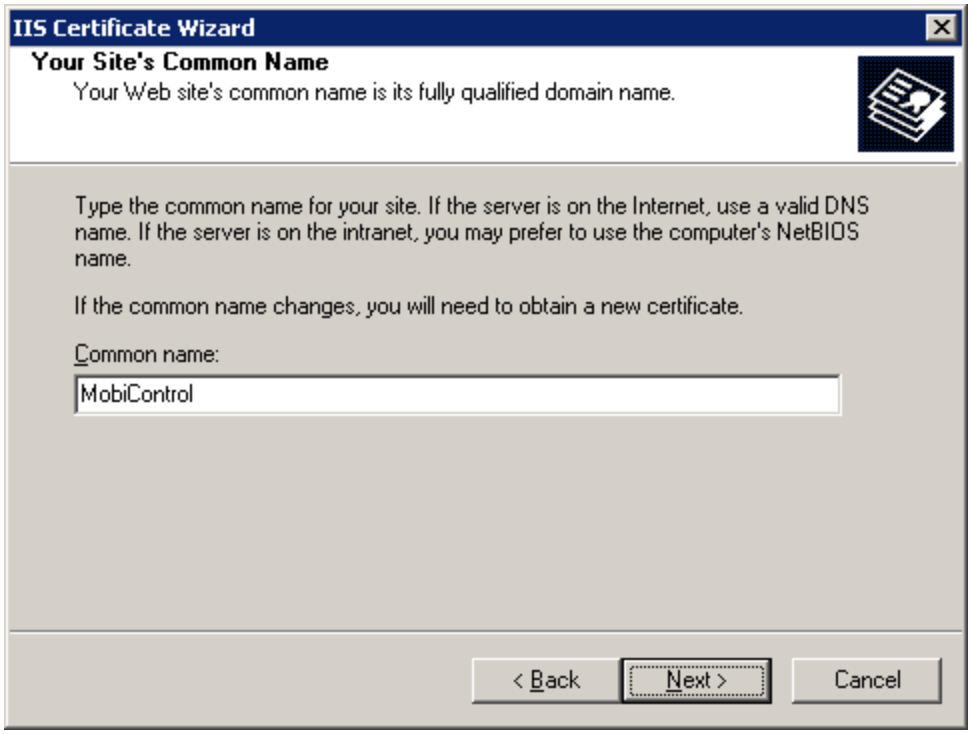
Provide a name for the request and set the Bit Length to **2048** and click **Next**.



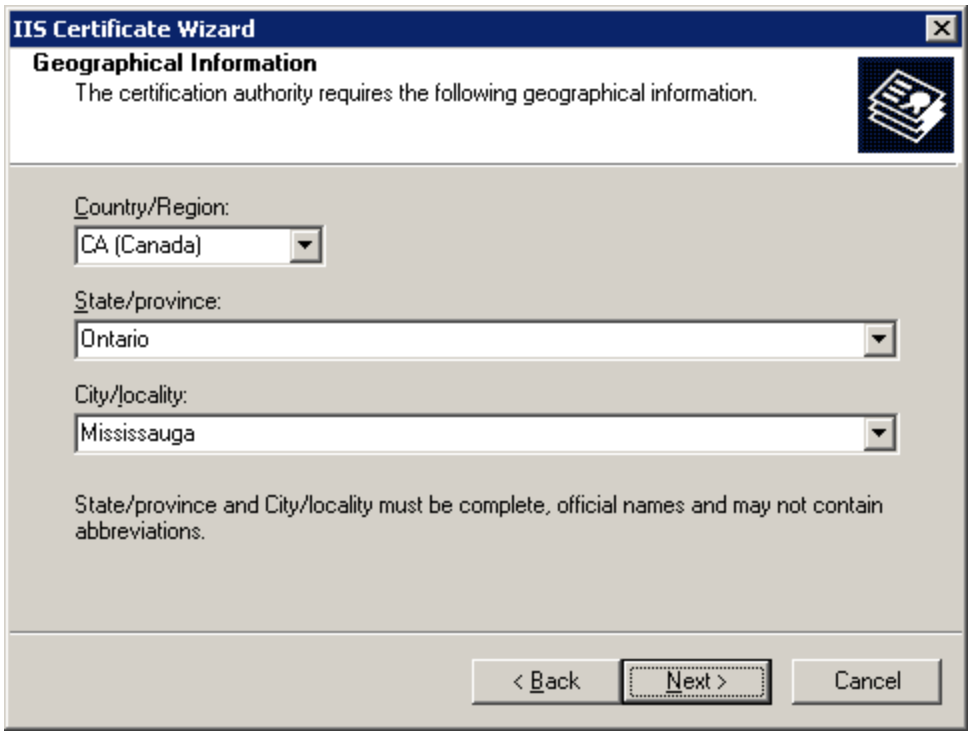
Specify an **Organization** and **Organizational Unit** and click **Next**.



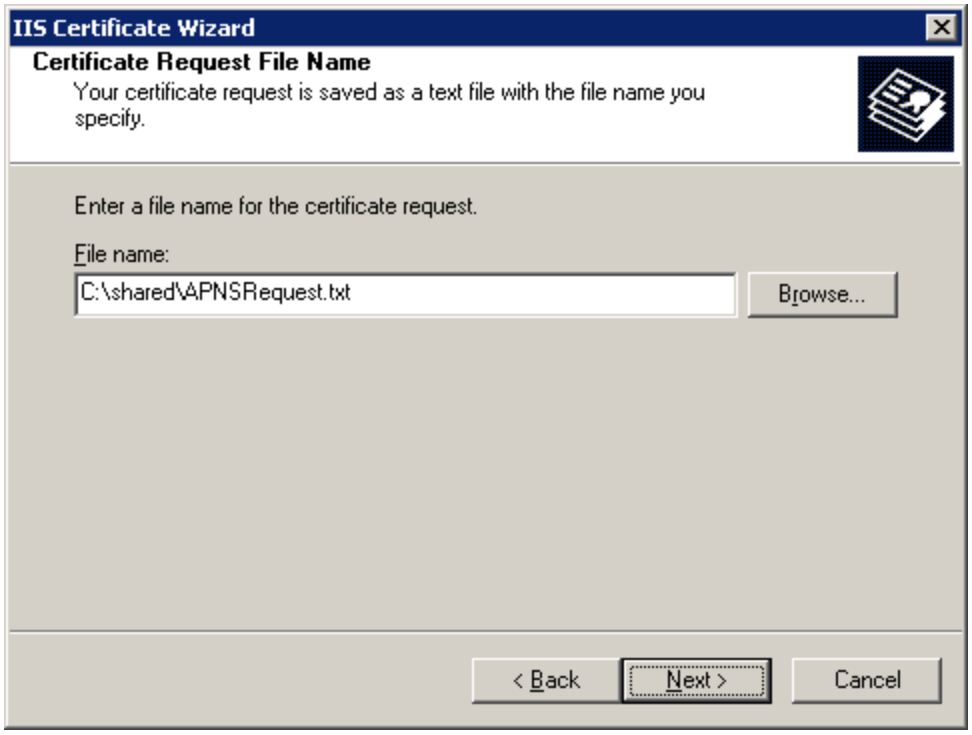
Specify a **Common Name** and click **Next**.



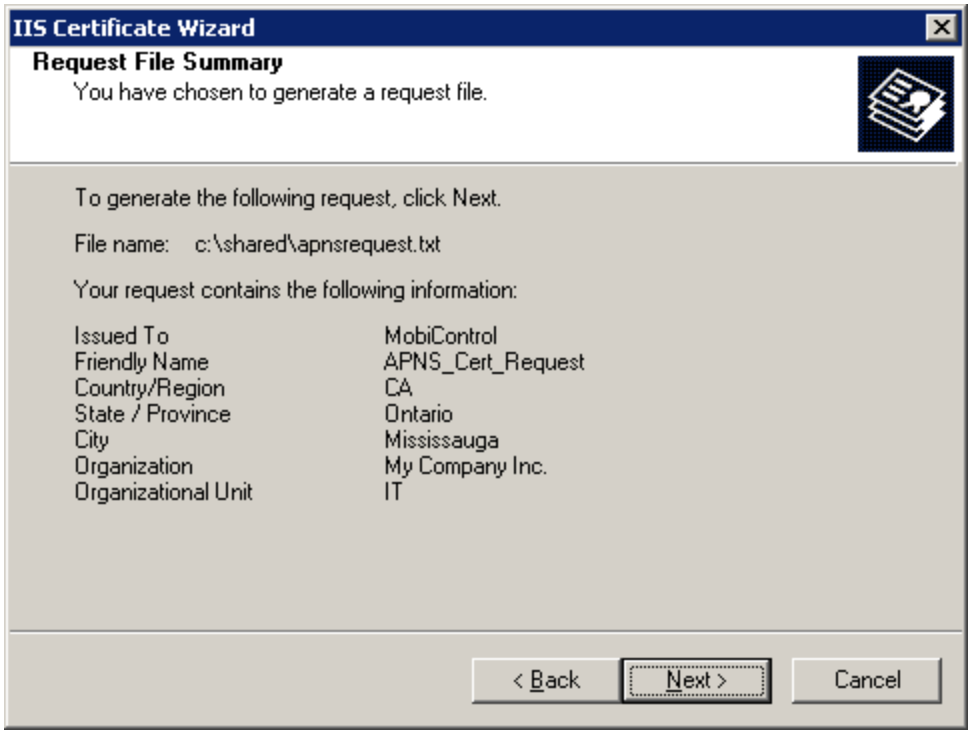
Specify a **Country**, **State/Province** and **City** and click **Next**.



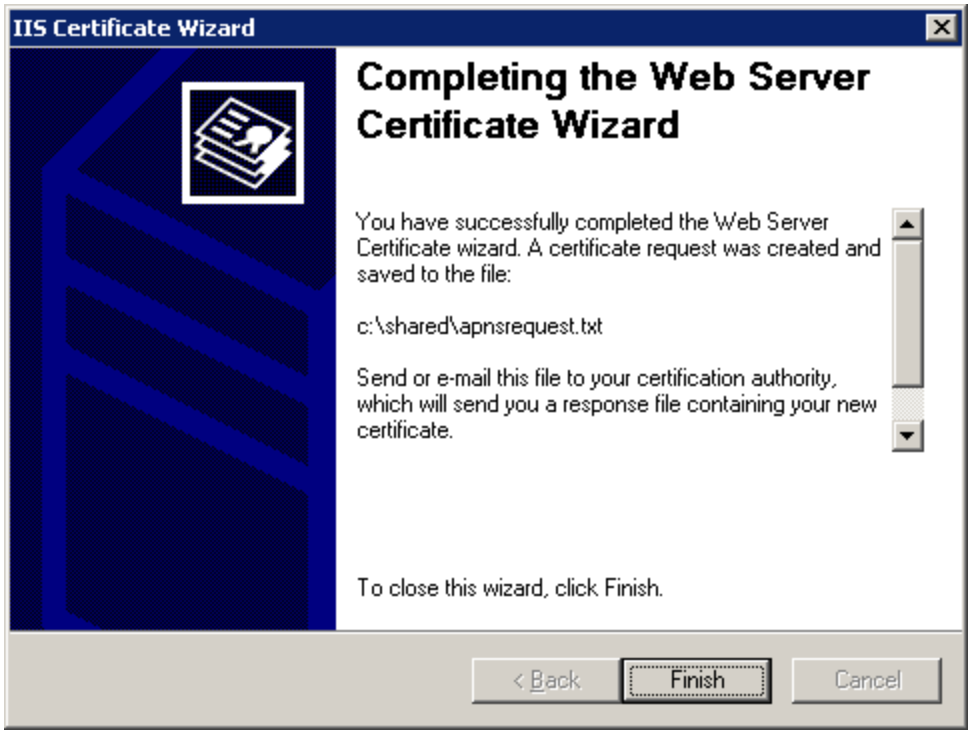
Specify a **File Name** and click **Next**.



Verify the information entered on previous screens and click **Next**.



Click **Finish** to end the wizard.



IMPORTANT:

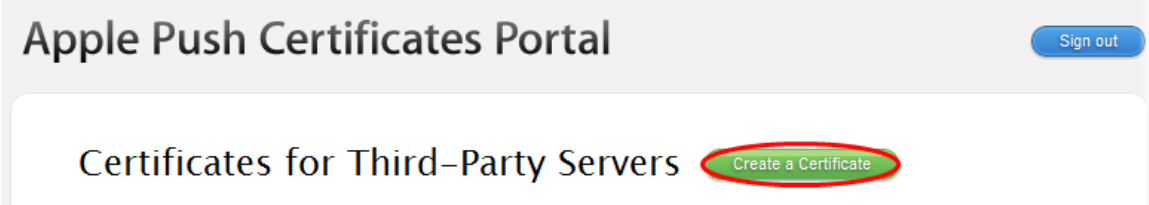
Remember where this .txt has been saved as it will be used later to complete the Certificate Request.

2. Generate the APNS Certificate

To complete the APNS Certificate Request, Click HERE to send us an email containing the Certificate Request generated in the first step. Please make sure to attach the Certificate Request to the email being sent.

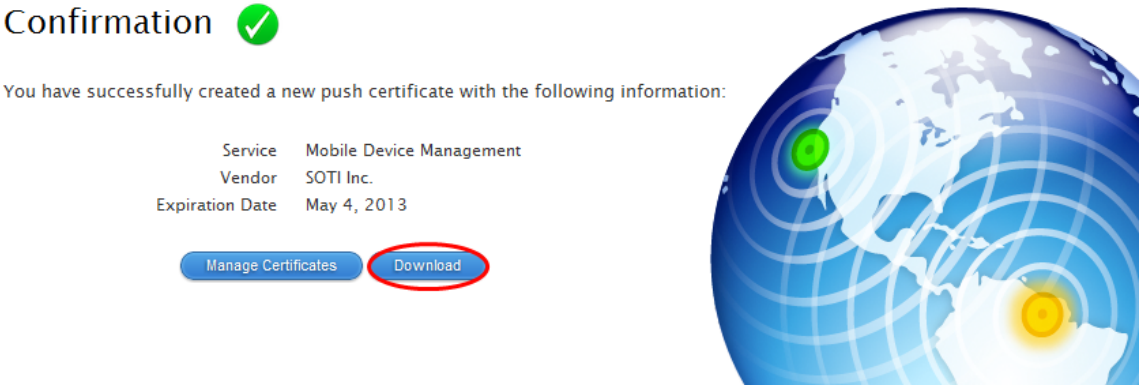
When you receive the Certificate Request back, log into https://identity.apple.com/pushcert with any Apple ID and select Create a Certificate.

IMPORTANT:
The use of Internet Explorer is not recommended. Please use Safari, Firefox or Chrome to complete this step.



Accept the Apple Agreement then browse to the Certificate Request file that you received from SOTI.

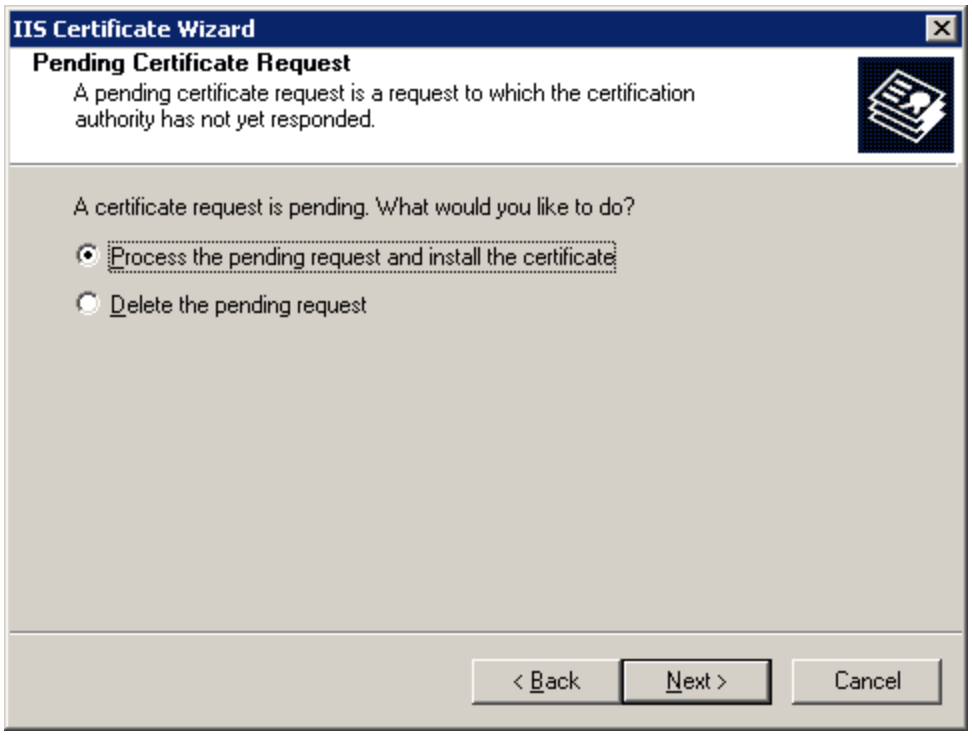
Once you have Uploaded the Signed Certificate Request and completed the process you can download the new Push Certificate.



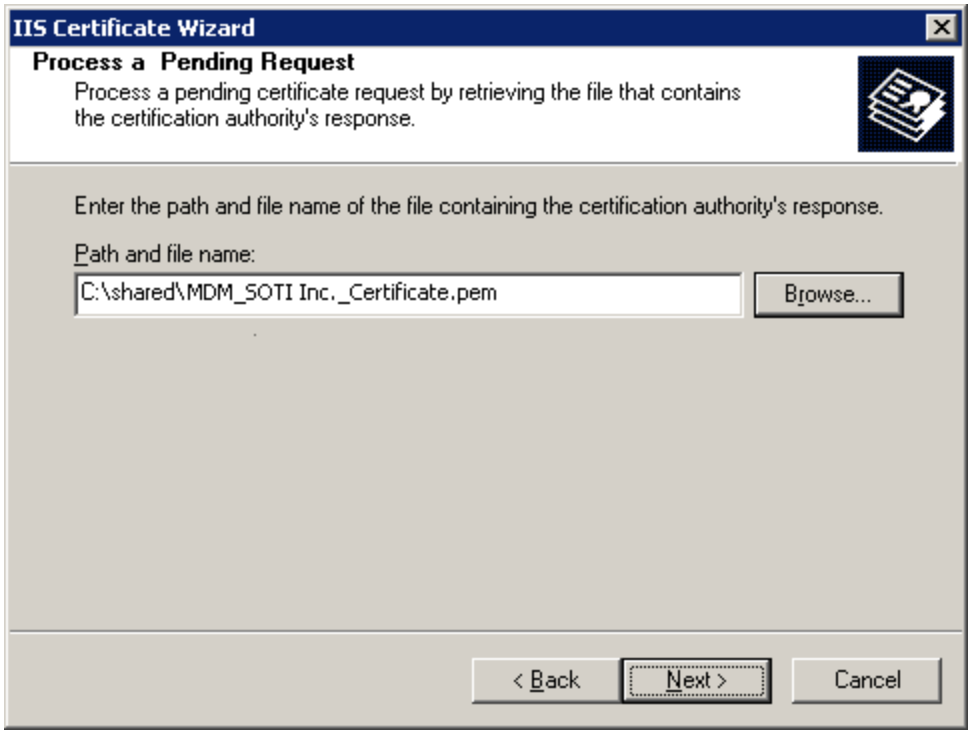
Remember where this file has been saved as it will be used again in the next step.

3. Complete the Certificate Request

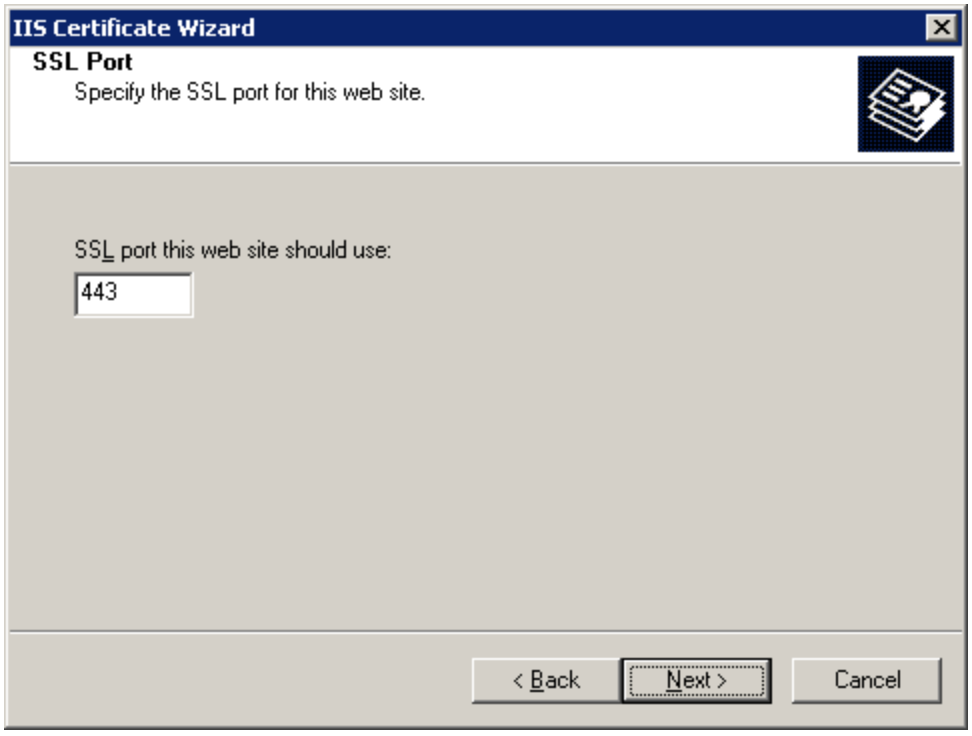
Open the *Internet Information Services* Manager (IIS). Once inside the IIS Manager, right click on the **Default Website** and select **Properties**. From the **Properties** window click on the **Directory Security** tab and click the **Server Certificate** button. Select **Process the pending request and install the certificate** and click **Next**.



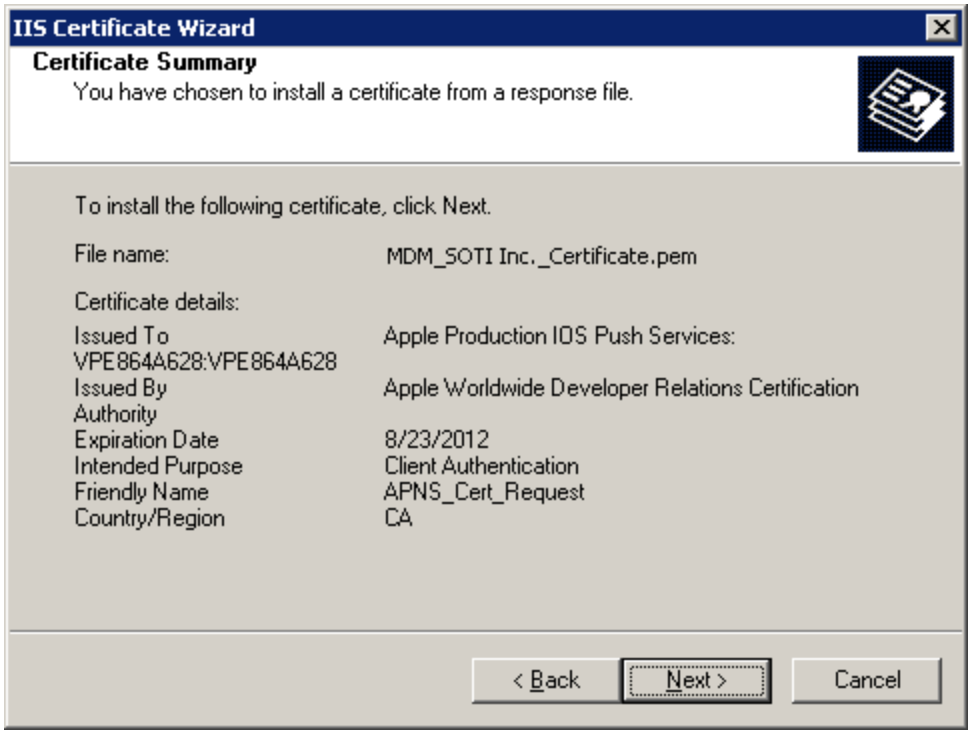
Specify the location of the file downloaded from Apple and click **Next**.



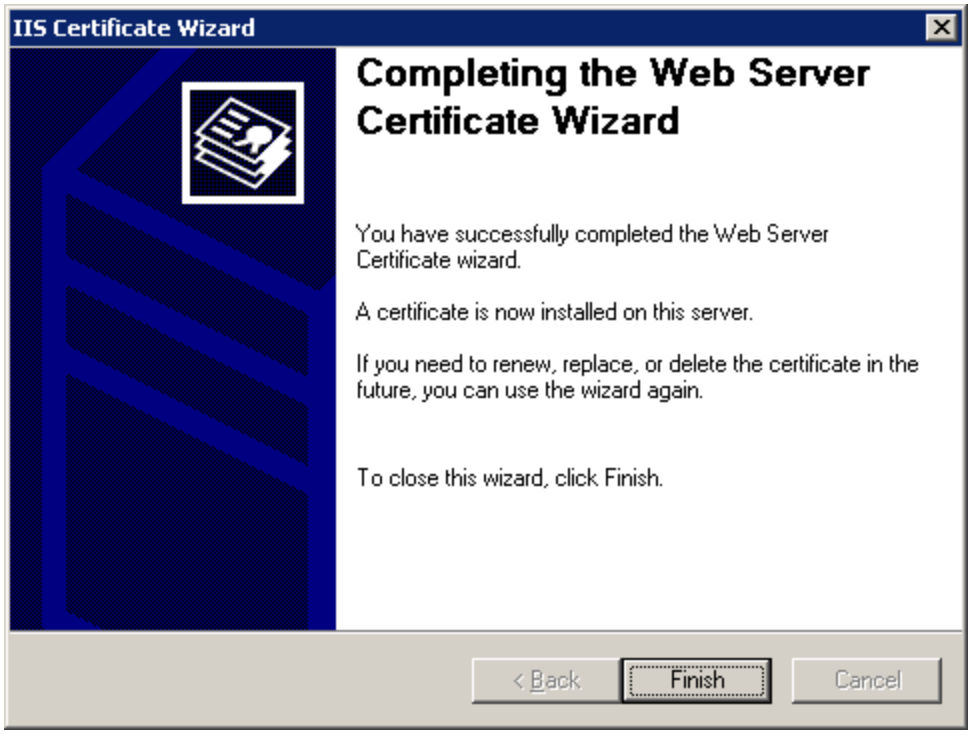
Specify the TCP port to be used for SSL communication and click **Next**.



Verify the information on the screen and click **Next**.

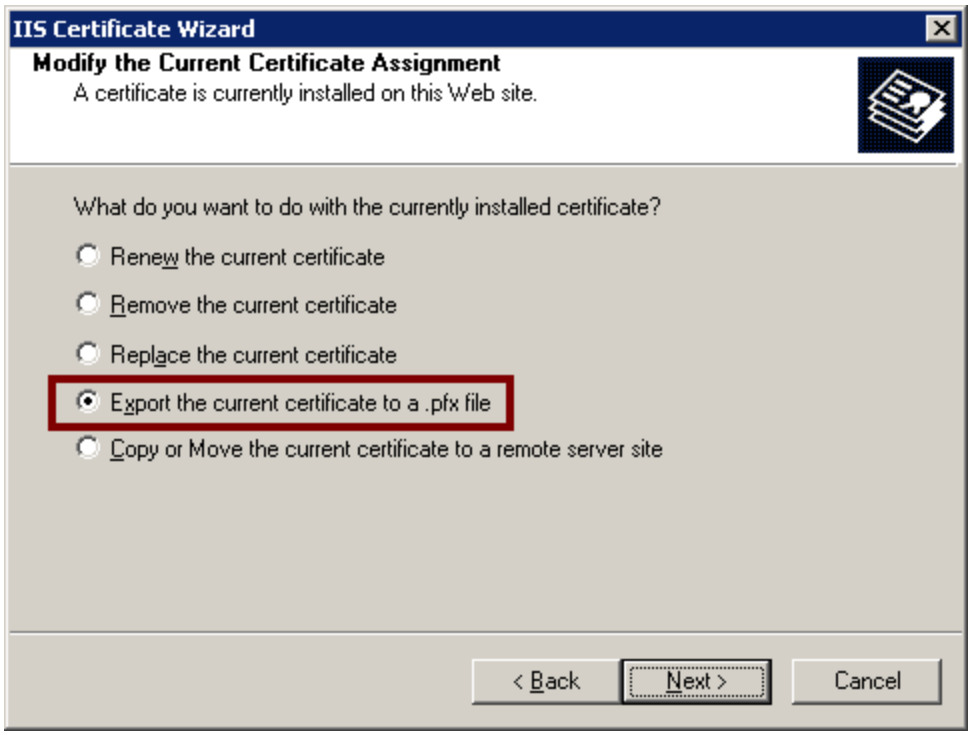


Click **Finish** to exit the wizard.

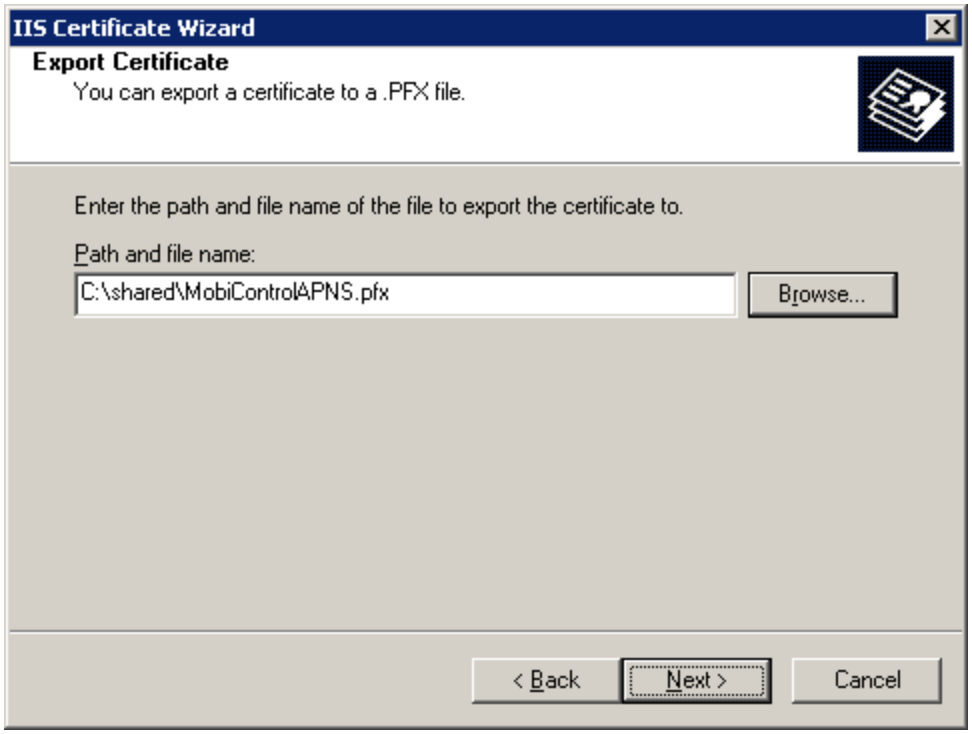


4. Export the APNS Certificate

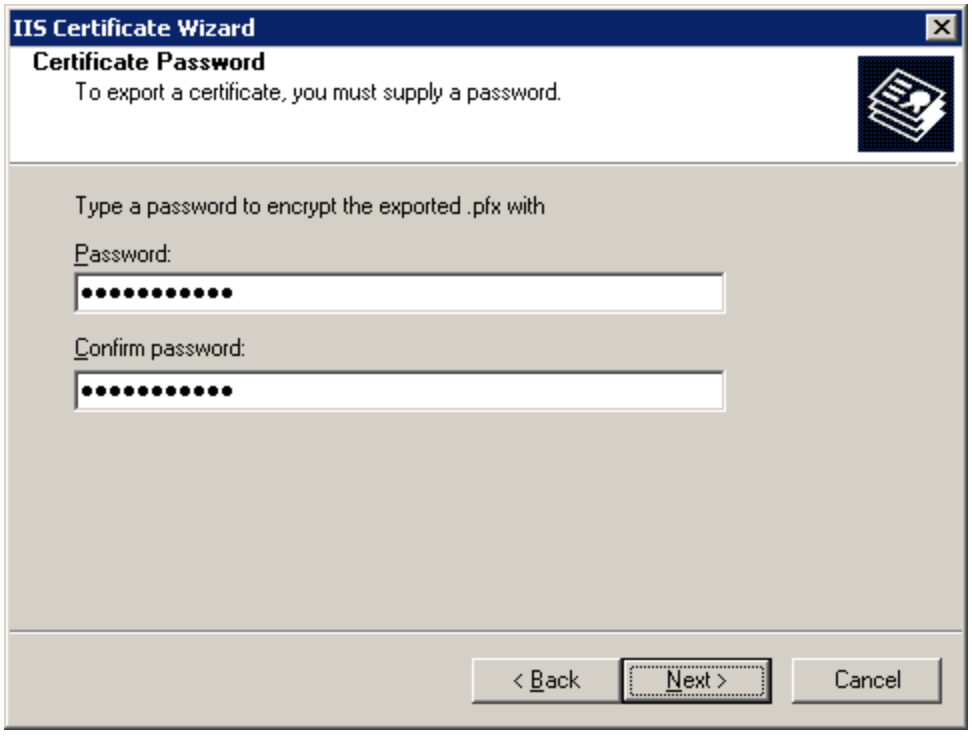
Open the *Internet Information Services* Manager (IIS). Once inside the IIS Manager, right click on the **Default Website** and select **Properties**. From the **Properties** window click on the **Directory Security** tab and click the **Server Certificate** button. Select **Export the current certificate to a .pfx file** and click **Next**.



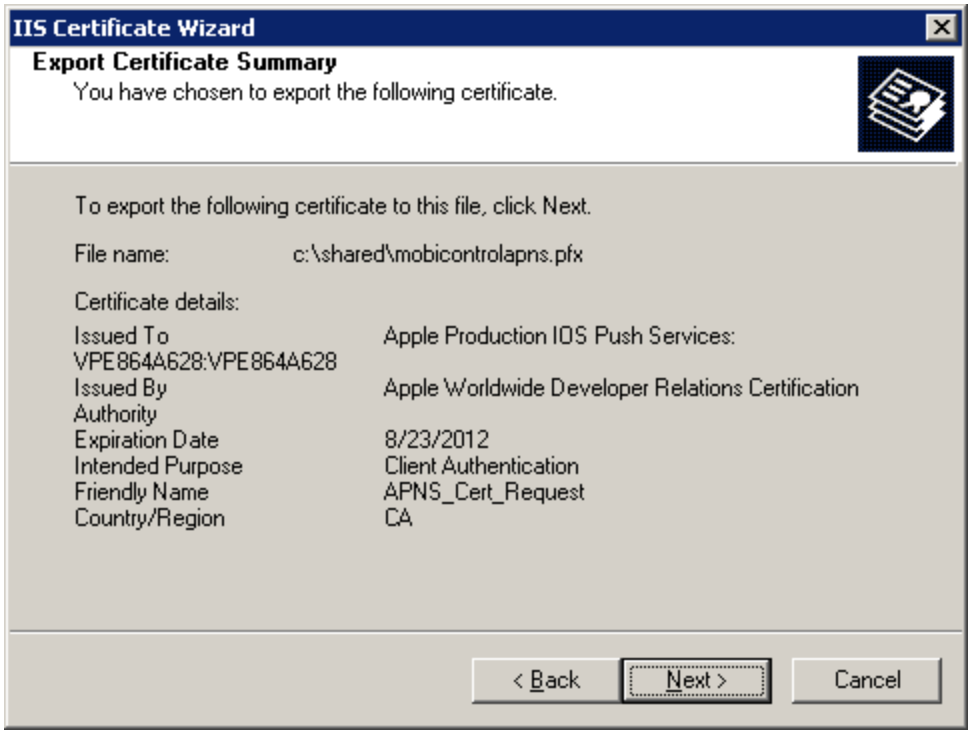
Specify the path of the .pfx file and click **Next**.



Specify a password for the certificate file to be exported and click **Next**.



Verify the details on the screen and click **Next**.



Click **Finish** to close the wizard.

Remember where the .pfx file has been saved to and what the password is as it will be required during the install of MobiControl.

Once you have successfully created an APNS Certificate, you will be able to manage your iOS Devices. Click here to finish the MobiControl Setup wizard.

If you have already installed MobiControl click here to see how to import the certificate into MobiControl.

APNS Certificate Request For Vista, Server 2008 or Windows 7

Windows Vista, Server 2008 or Windows 7

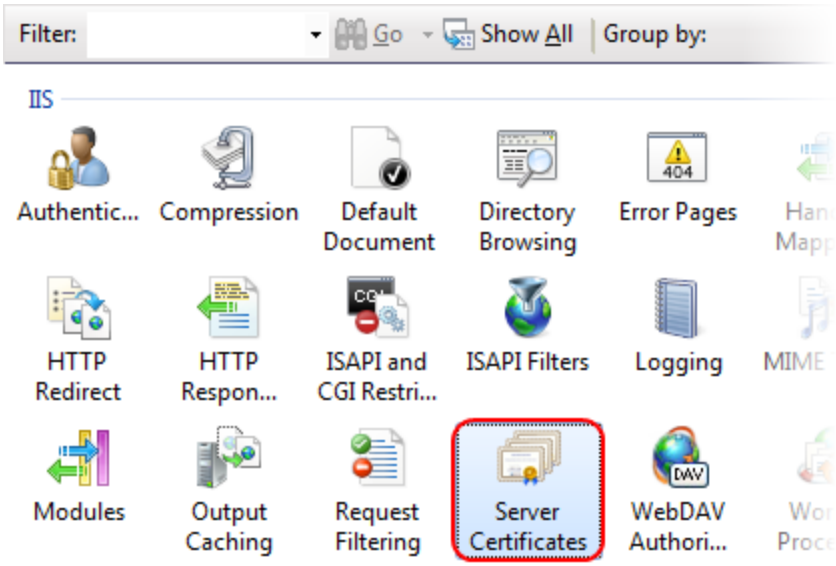
The following instructions are used for creating an APNS certificate request on Windows Vista, Server 2008 or Windows 7.

NOTE:

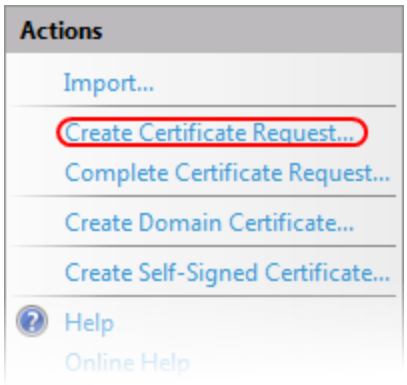
An APNS request can be done from any computer and does not have to be done from a computer with MobiControl installed on it.

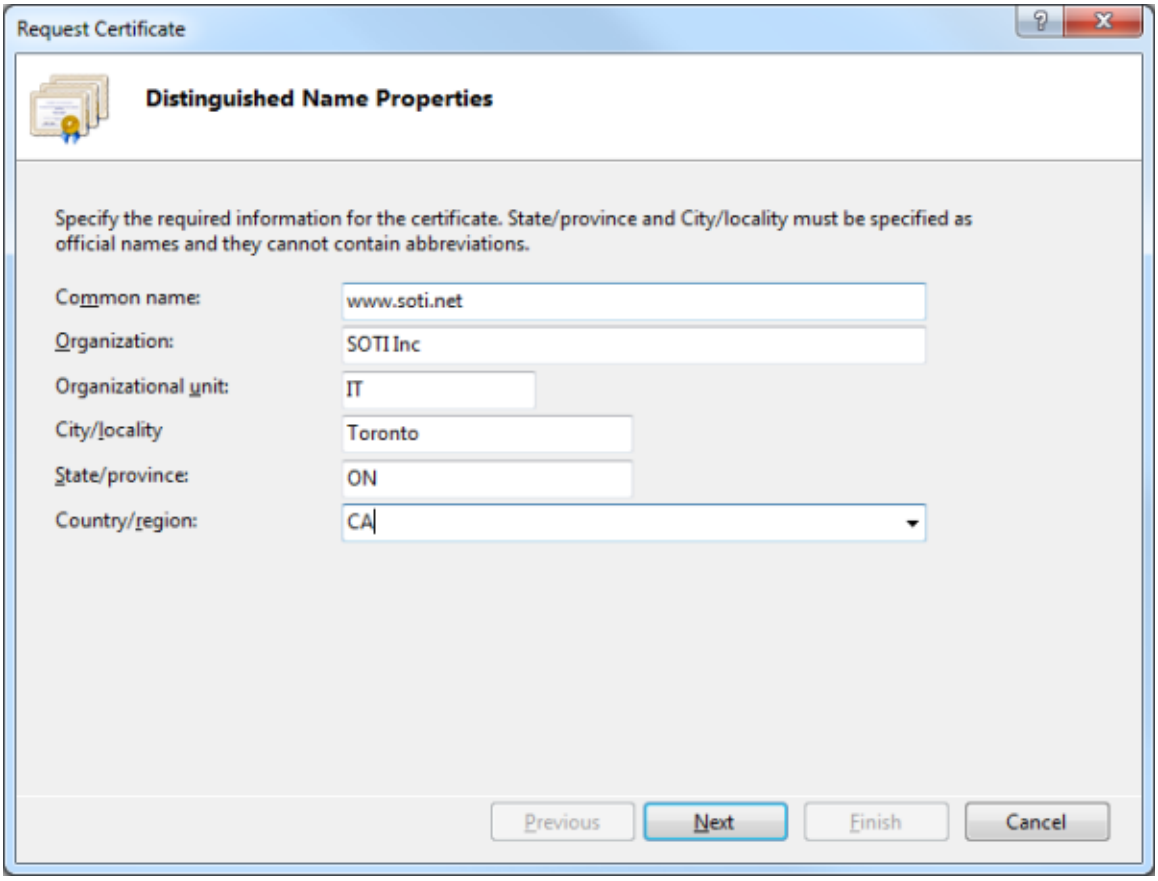
1. Create the Certificate Request

   To create a new APNS Certificate Request, open the *Internet Information Services* Manager (IIS). Once inside the IIS Manager, open Server Certificates from the front page.



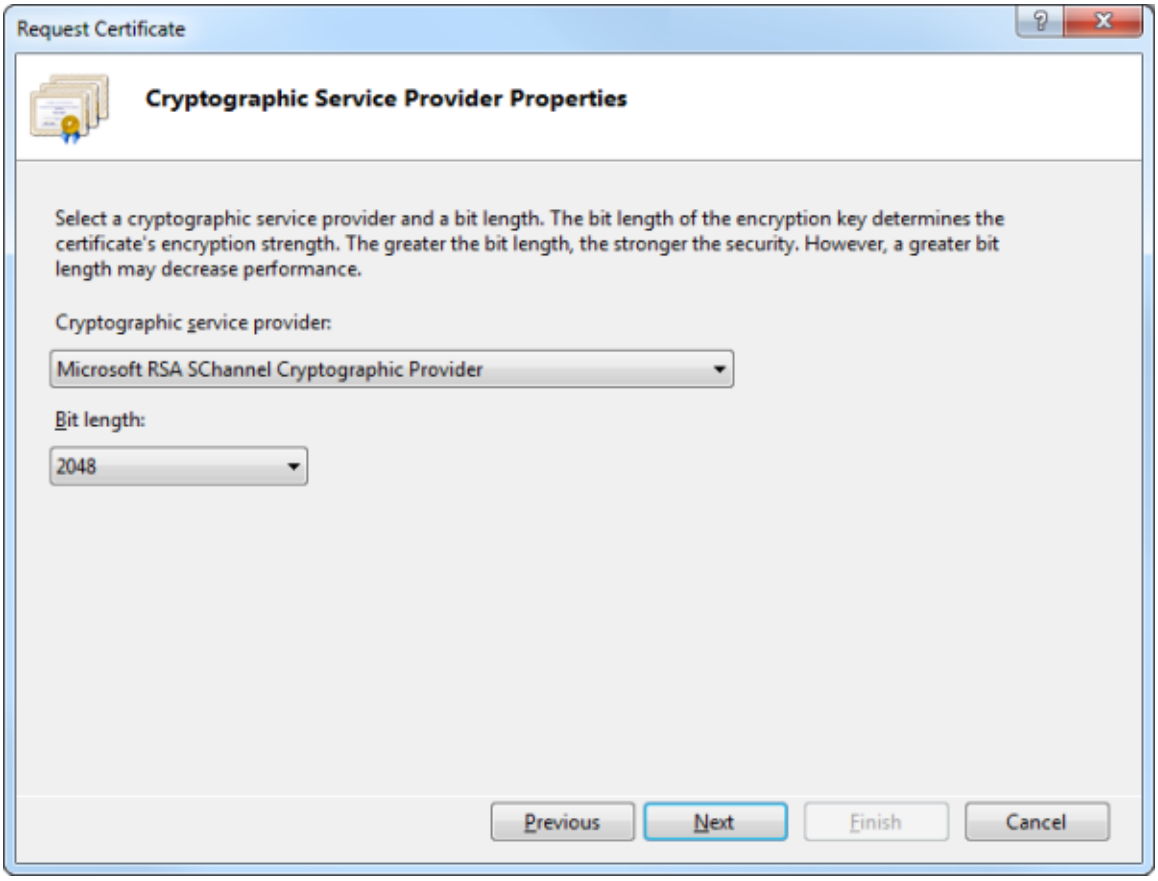
From the Actions pane in the Server Certificates window, select Create a Certificate Request.



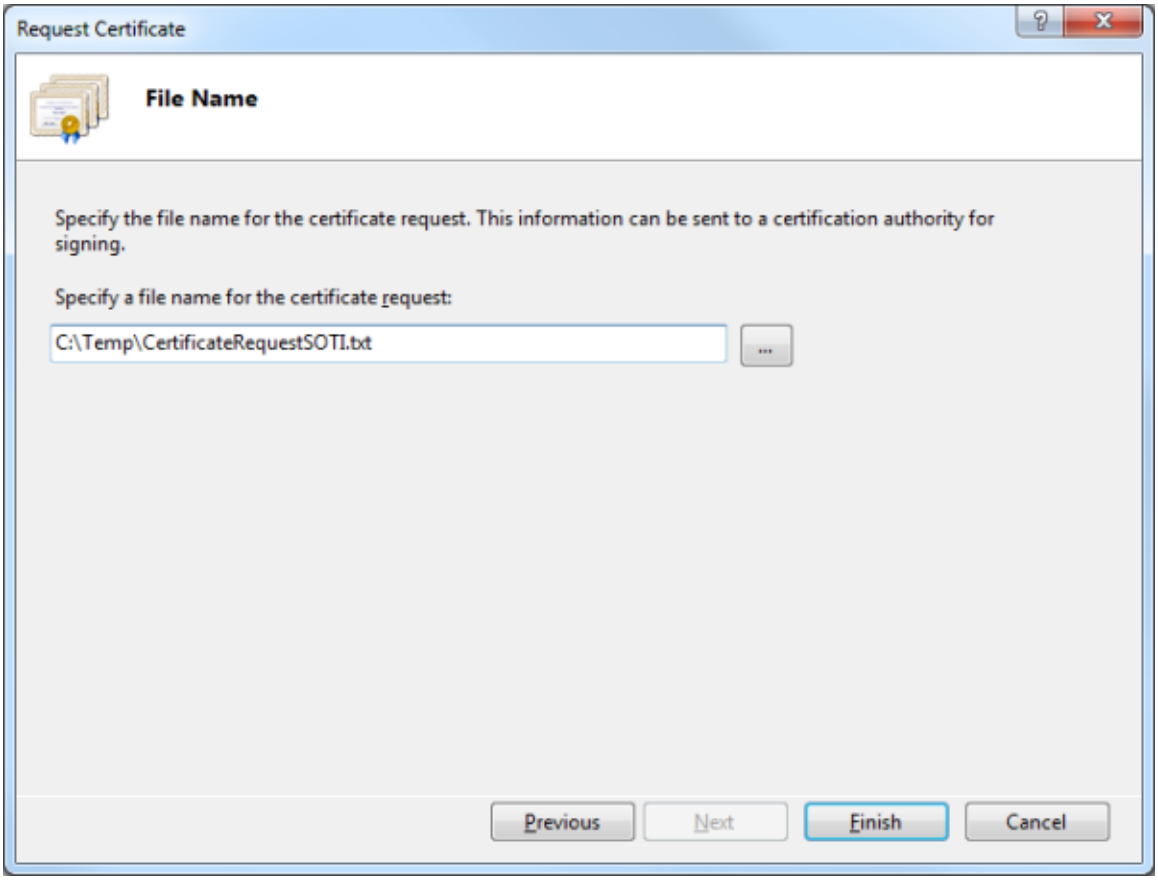


Once all the fields have been entered with valid information select Next.

In the Cryptographic Service Provider Properties page, ensure the Cryptographic Provider Service is set to **Microsoft RSA SChannel Cryptographic Provider** and Bit Length is set to **2048**.



Once the information above has been verified, select Next.



Select a Path where the request will be saved. You can name this file anything you wish. This request will be saved as a .txt file. Then select Finish.

IMPORTANT:

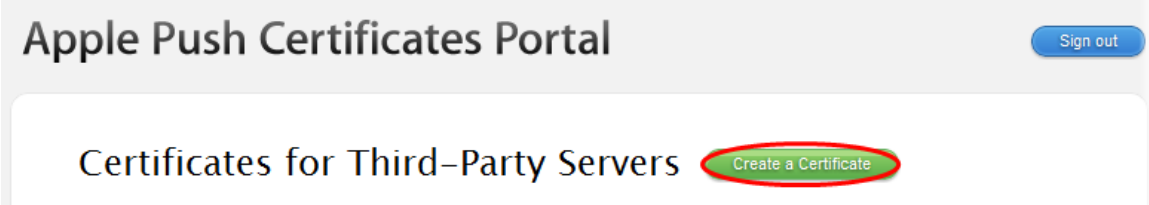
Remember where this .txt has been saved as it will be used later to complete the Certificate Request.

2. Generate the APNS Certificate

To complete the APNS Certificate Request, Click HERE to send us an email containing the Certificate Request generated in the first step. Please make sure to attach the Certificate Request to the email being sent.

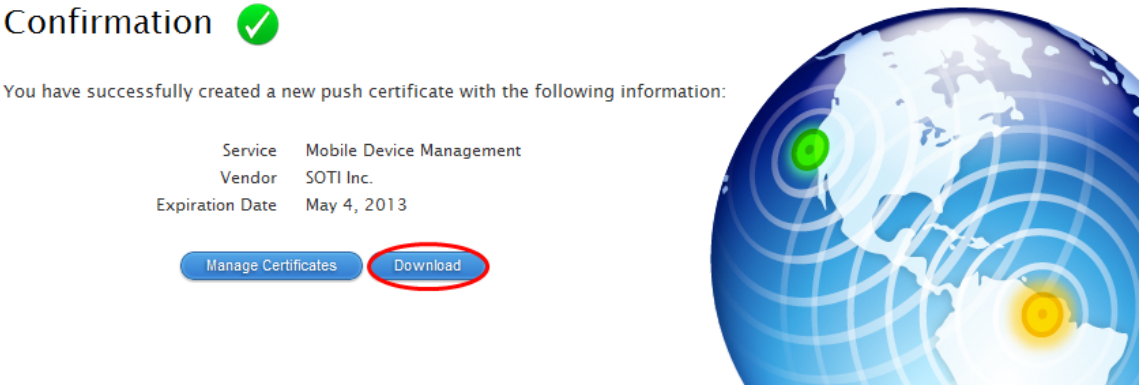
When you receive the Certificate Request back, log into https://identity.apple.com/pushcert with any Apple ID and select Create a Certificate.

IMPORTANT:
The use of Internet Explorer is not recommended. Please use Safari, Firefox or Chrome to complete this step.



Accept the Apple Agreement then browse to the Certificate Request file that you received from SOTI.

Once you have Uploaded the Signed Certificate Request and completed the process you can download the new Push Certificate.

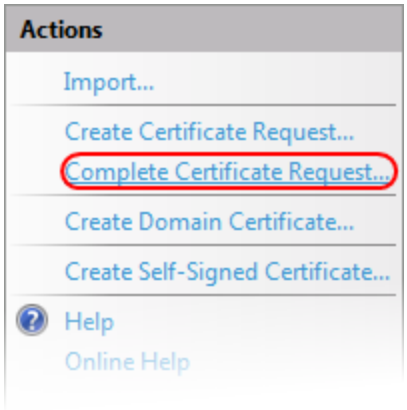


Remember where this file has been saved as it will be used again in the next step.

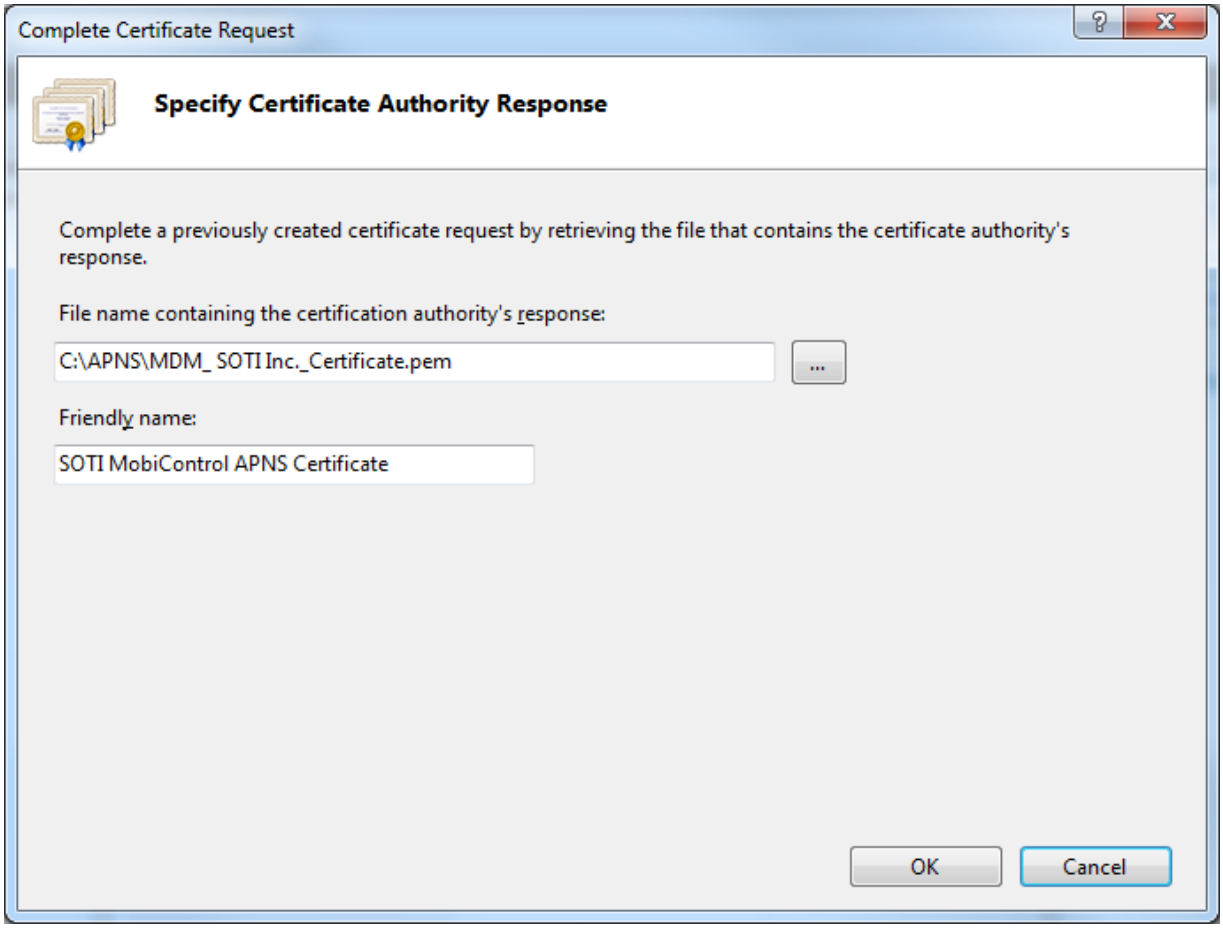
3. Complete the Certificate Request

Windows Vista, Server 2008 and 7

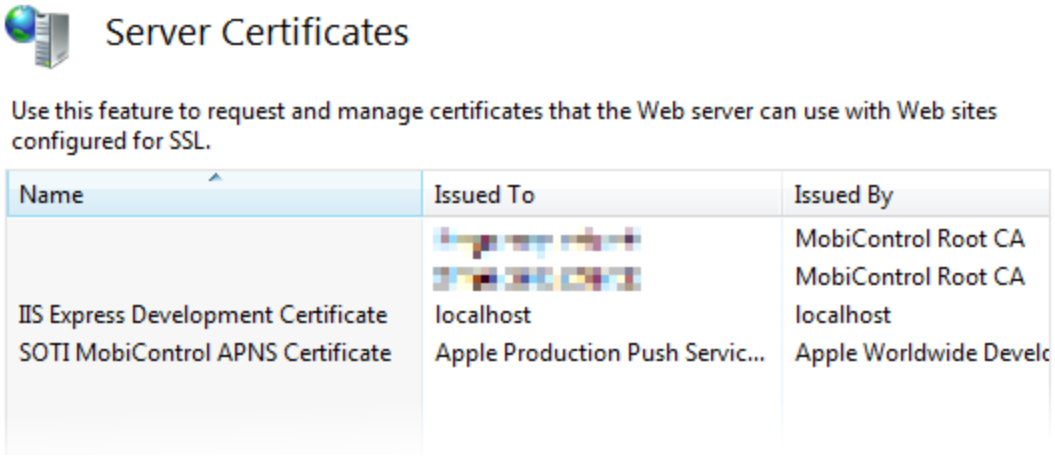
Open the *Internet Information Services* Manager (IIS). Once inside the IIS Manager, open Server Certificates from the front page.



From the Actions pane in the Server Certificates window, click **Complete Certificate Request**.



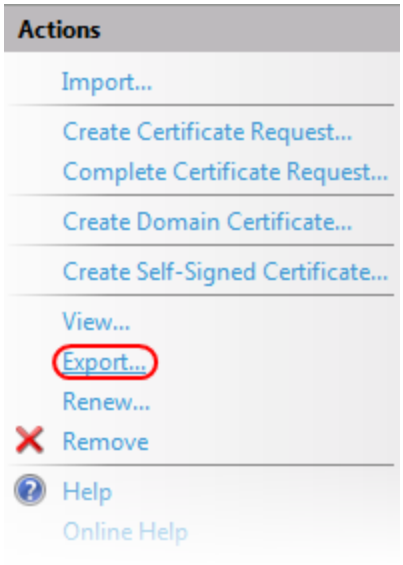
Locate the .pem file that was downloaded from the step above, and provide a friendly name, then select OK. The certificate request will be completed at this point and installed into your IIS environment.



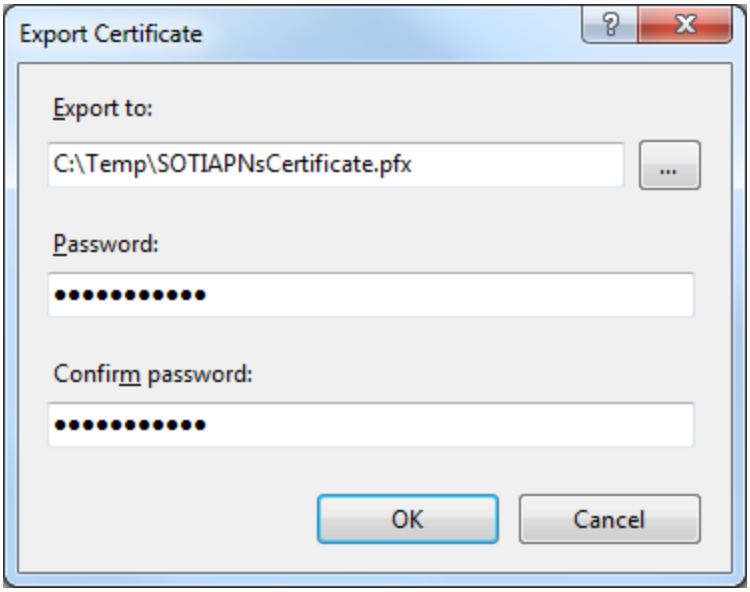
4. Export the APNS Certificate

Open the *Internet Information Services* Manager (IIS). Once inside the IIS Manager, open Server Certificates from the front page.

Highlight the APNS Certificate and select Export from the Actions Pane.



Select a path to export the APNS Certificate to, and enter a password of your choosing.



Remember where the .pfx file has been saved to and what the password is as it will be required during the install of MobiControl.

Once you have successfully created an APNS Certificate, you will be able to manage your iOS Devices. Click here to finish the MobiControl Setup wizard.

If you have already installed MobiControl click here to see how to import the certificate into MobiControl.

APNS Certificate Request for Mac OS X

Mac OS X

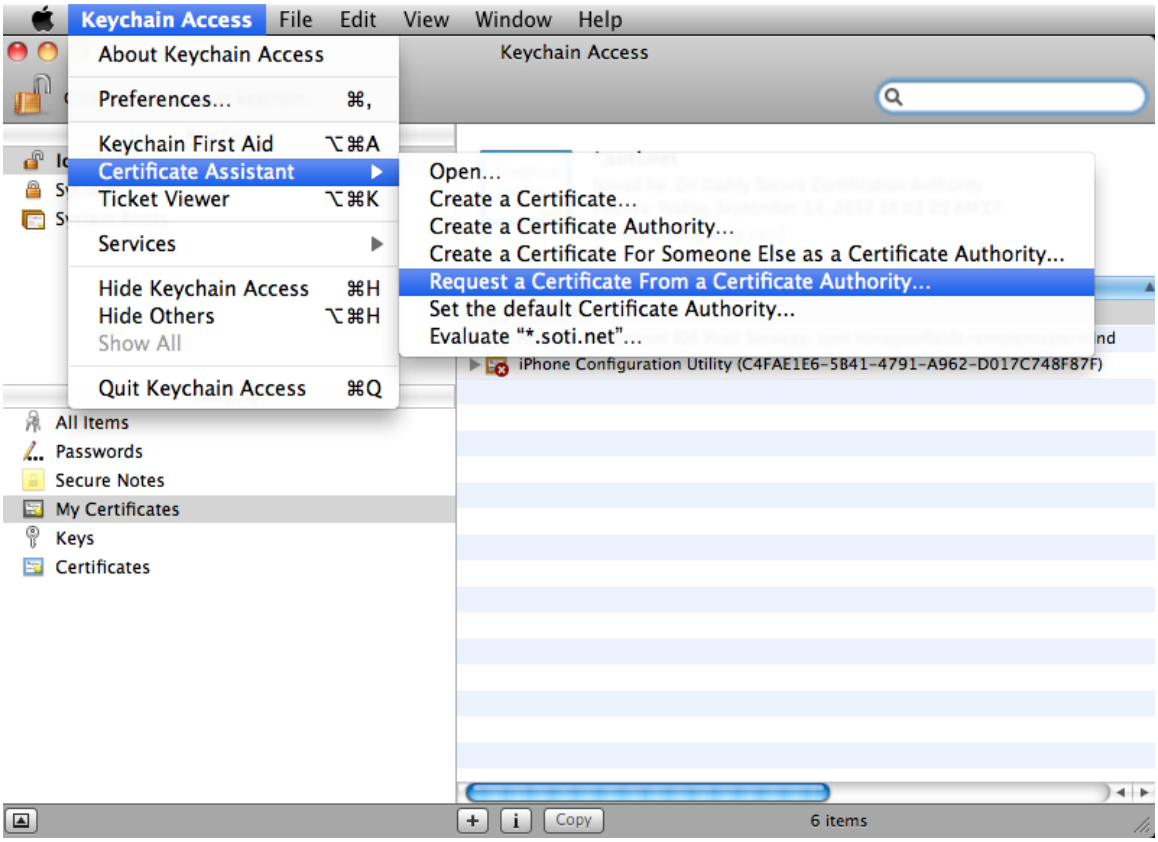
The following instructions are used for creating an APNS certificate request on Mac OS X.

NOTE:

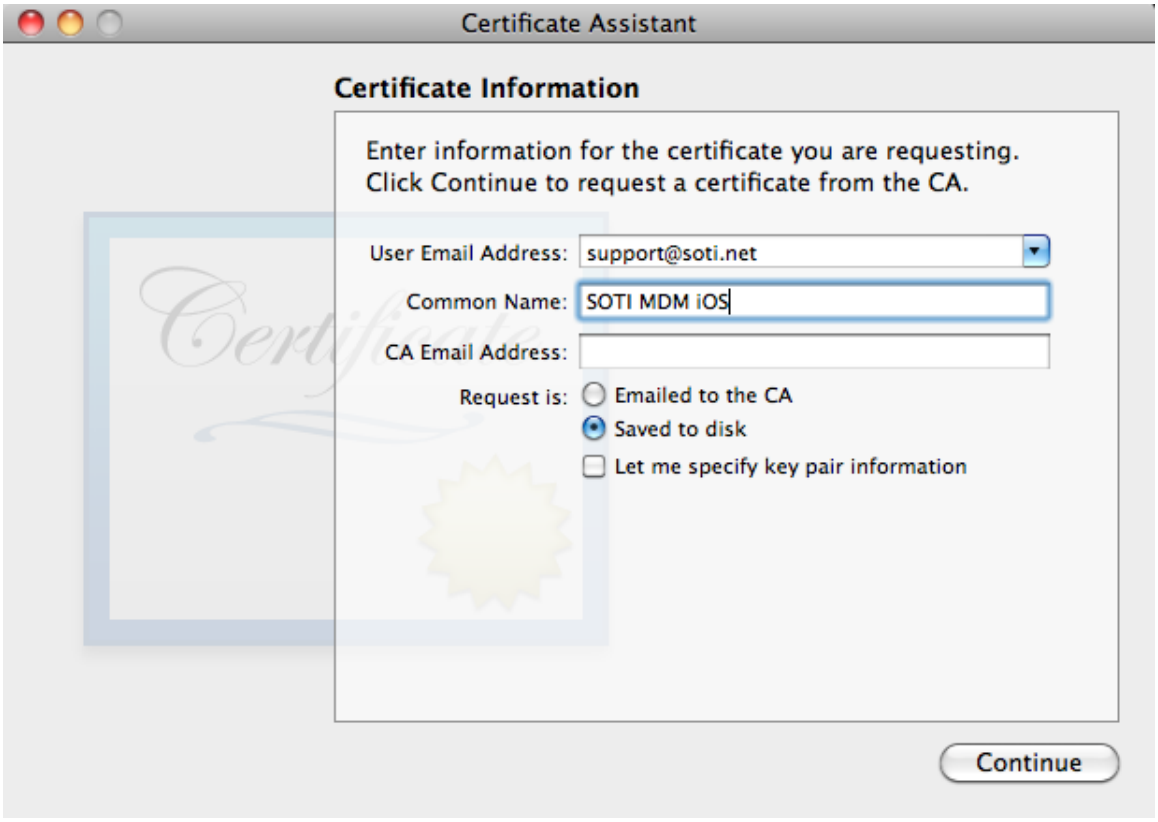
An APNS request can be done from any computer and does not have to be done from a computer with MobiControl installed on it.

1. Create the Certificate Request

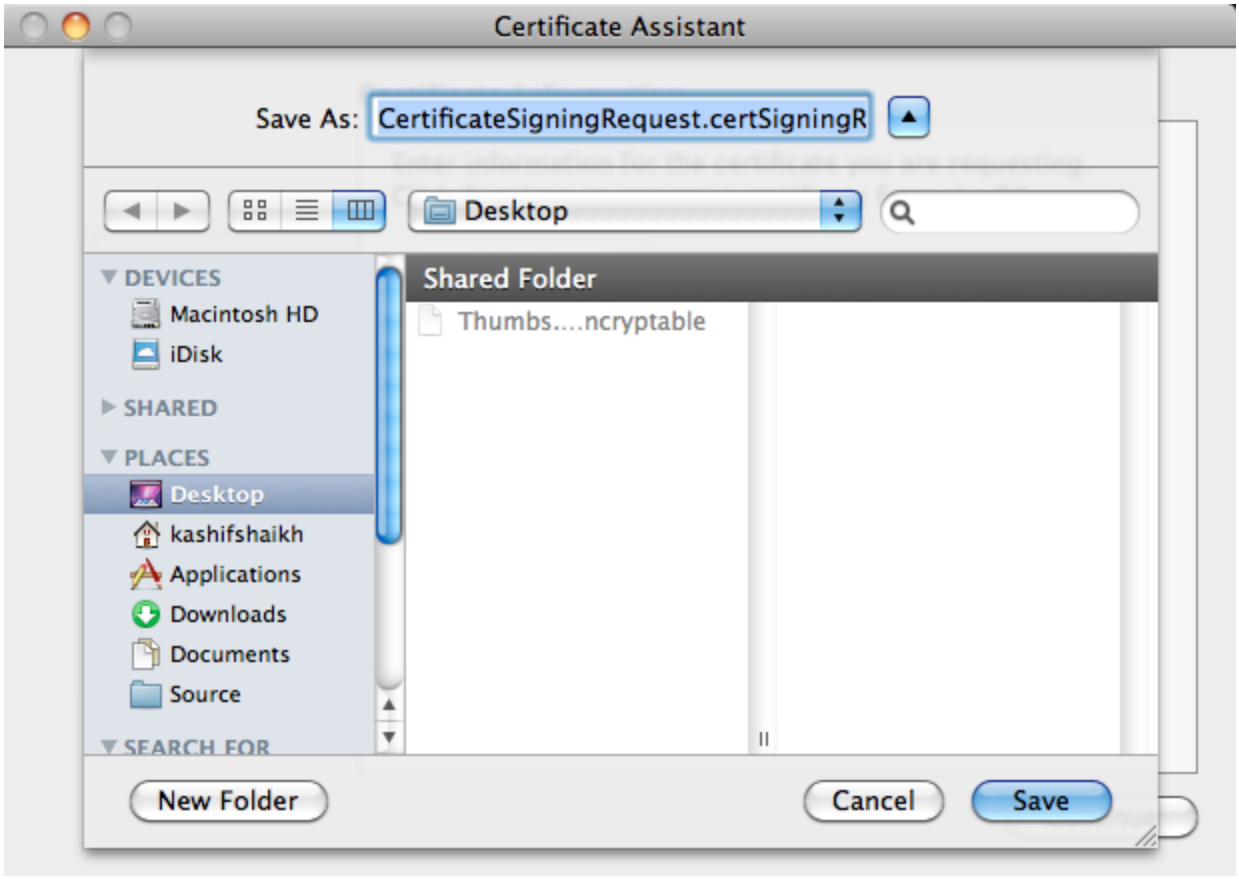
   To create a new APNS Certificate Request, open **Keychain Access**. In Keychain Access, click **Keychain access > Certificate Assistant > Request a Certificate From a Certificate Authority**.



   The Certificate Assistant wizard will appear. From here, enter a **User's Email Address** and any **Common Name** you wish. The common name will just allow you to locate the certificate easier later in this process. After entering the Common Name, make sure that **Saved to Disk** is selected. Click **Continue** to go to the next step.



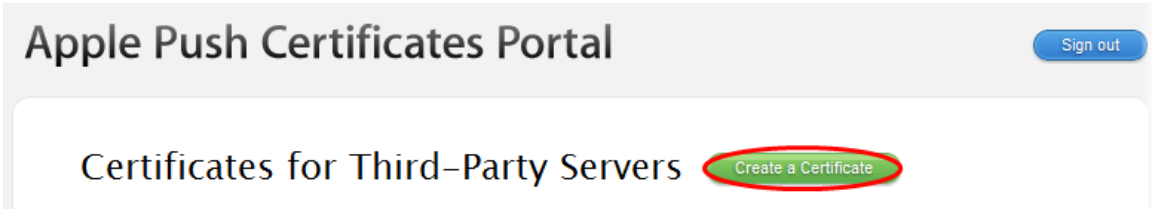
From here, place the CertificateSigningRequest.certSigningRequest anywhere on the computer that is easy to remember and retrieve. Click **Save**.


Certificate Assistant
Save As: CertificateSigningRequest.certSigningR
Desktop
DEVICES
Macintosh HD
iDisk
SHARED
PLACES
Desktop
kashifshaikh
Applications
Downloads
Documents
Source
SEARCH FOR
Shared Folder
Thumbs....ncryptable
New Folder
Cancel
Save

2. Generate the APNS Certificate

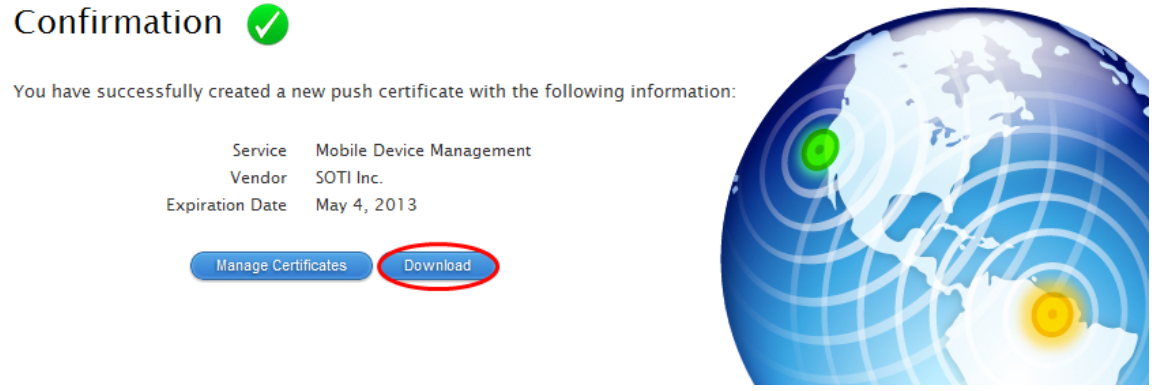
To complete the APNS Certificate Request, Click HERE to send us an email containing the Certificate Request generated in the first step. Please make sure to attach the Certificate Request to the email being sent.

When you receive the Certificate Request back, log into https://identity.apple.com/pushcert with any Apple ID and select Create a Certificate.



Accept the Apple Agreement then browse to the Certificate Request file that you received from SOTI.

Once you have Uploaded the Signed Certificate Request and completed the process you can download the new Push Certificate.



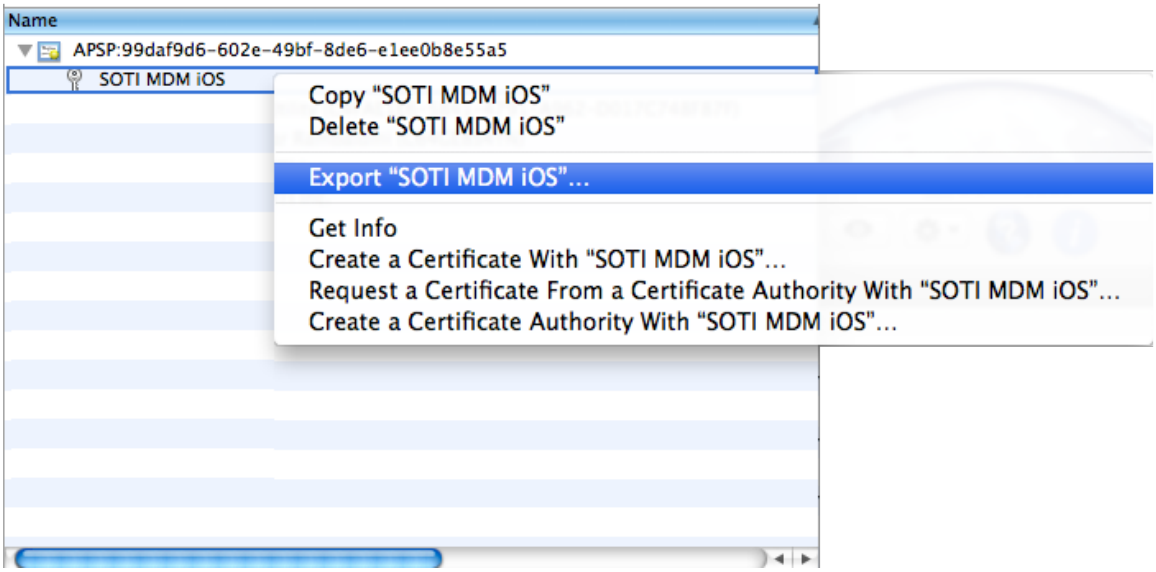
Remember where this file has been saved as it will be used again in the next step.

3. Complete the Certificate Request

   Double click the .pem file that has been downloaded from the Apple Website. This will install the certificate and open Keychain Access.

4. Export the APNS Certificate

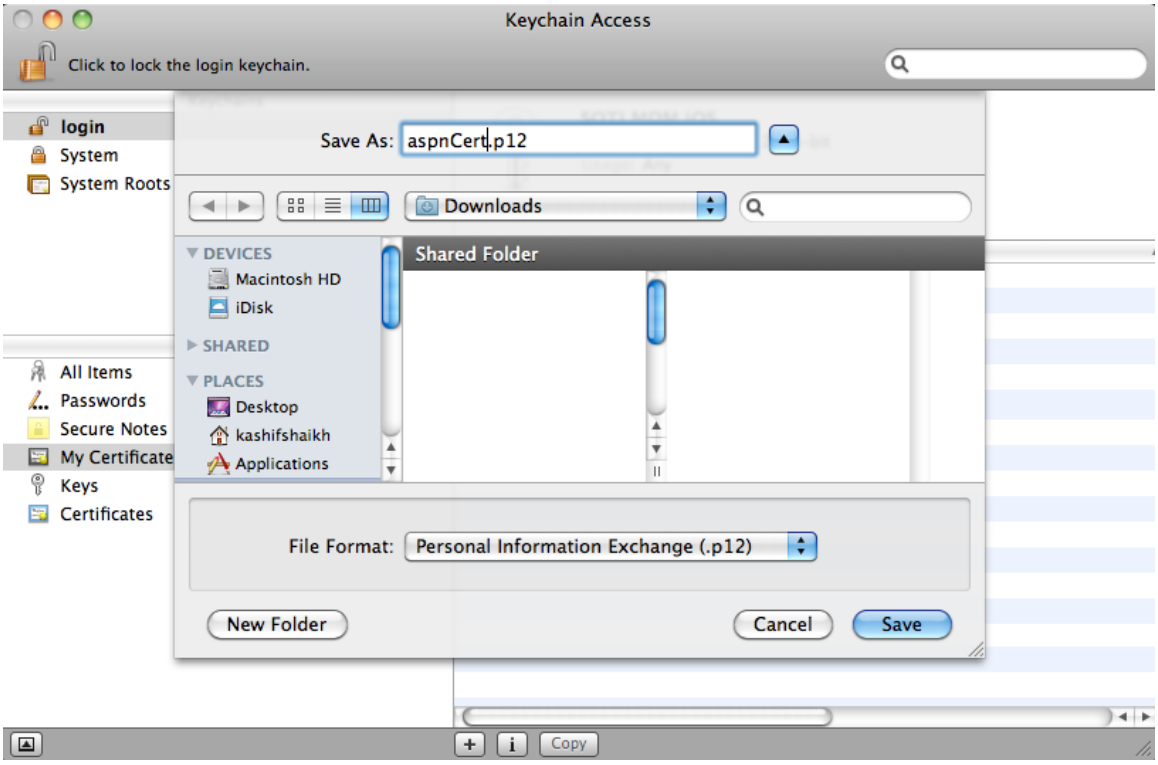
Locate the certificate in Keychain Access. The name of the certificate is the same name that was entered for the Common Name. Once the certificate has been located, **hold Control and click the certificate**. Select **Export**.



Place the exported certificate in a place that is easy to remember. The name of the certificate can be anything you wish. Click **Save**.

NOTE:

If the file format shows up as .cer, something has been done incorrectly and the process must be redone.



Enter a password for this certificate. Please remember this password as it will be required when adding it to MobiControl. Click **OK**.

Once you have successfully created an APNS Certificate, you will be able to manage your iOS Devices. Click here to finish the MobiControl Setup wizard.

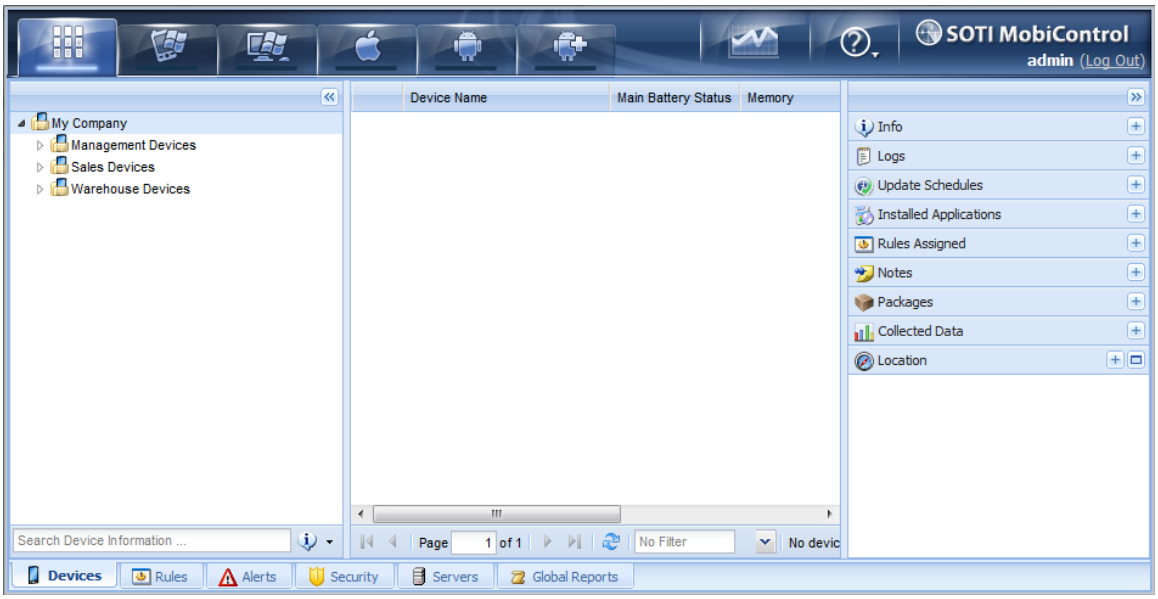
If you have already installed MobiControl click here to see how to install the certificate into MobiControl.

Installing the APNS Certificate

With MobiControl v10, we can now generate and sign the APNS certificate through the web console in a few steps.

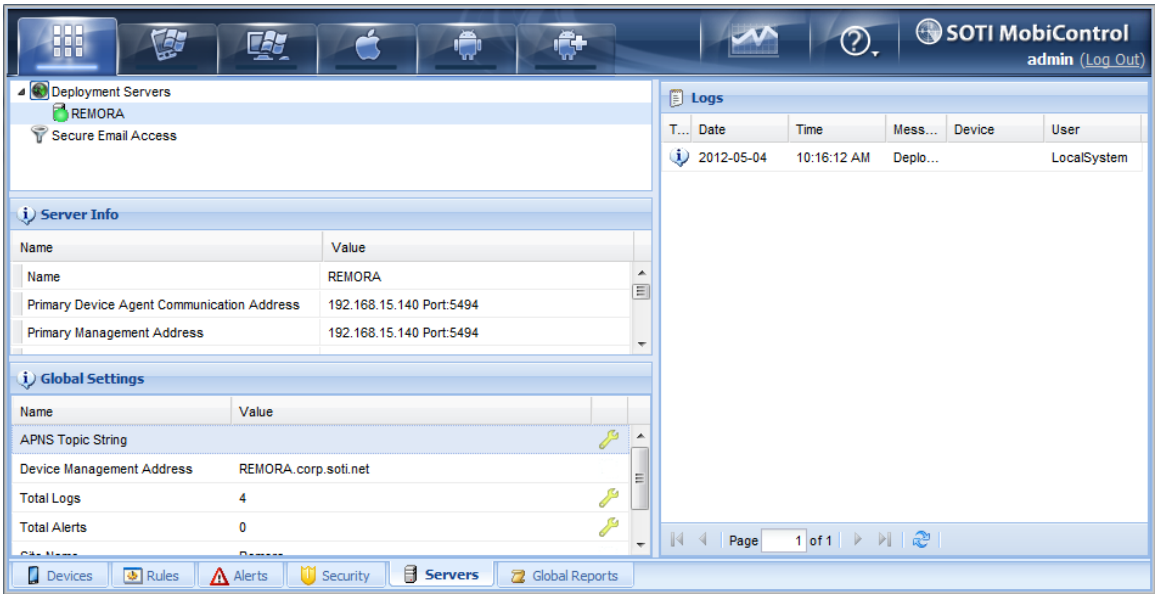
Installing the APNS certificate through the Web Console

1. Log into the MobiControl Web Console and go to the All Devices tab.



All Devices tab

2. Click the **Servers tab** near the bottom of the Web Console. Once in the **Servers** tab click the icon beside the APNS Topic string as seen below.



The Servers tab

3. A new window will appears and from here, the APNS Certificate can be created. Click ***Download the Certificate Signing Request (CSR)*** to download the **signedCSR.plist** file. With this file, we can go to https://identity.apple.com/pushcert and upload the **signedCSR.plist** file.

IMPORTANT:
If you are renewing an APNS certificate, please ensure that renew is selected rather than create new certificate. If a new APNS certificate is imported with a different topic string, all iOS devices must be re-enrolled to receive any updated configurations.

After uploading the **signedCSR.plist** file, we can download the **MDM_SOTIInc._Certificate.pem**. This file can then be uploaded into the iOS APNS Certificate Generator.

Adding the APNS certificate.

The APNS certificate is now uploaded to the MobiControl database through the web console and is now able to enroll iOS devices.

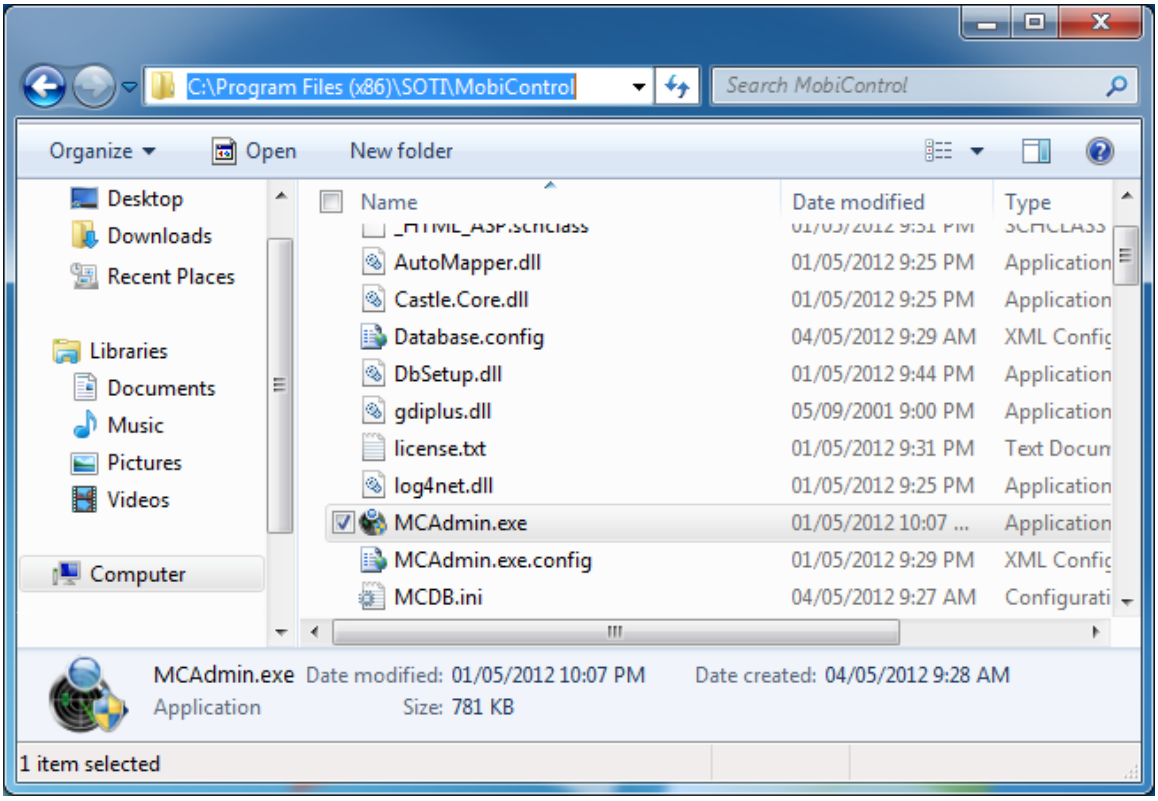
Please see the "Adding iOS Devices" topic on page 1034 for more information on how to enroll your iOS device.

Installing the APNS certificate with the MobiControl Administration Utility

NOTE:

It is recommended to use the iOS APNS Certificate Generator to import the APNS certificate.

1. Open the MobiControl Administration Utility. This is located in the install folder for MobiControl. The default location for 64 bit machines is *C:\Program Files (x86)\SOTI\MobiControl*. For 32 bit machines, it is located at *C:\Program Files\SOTI\MobiControl*.

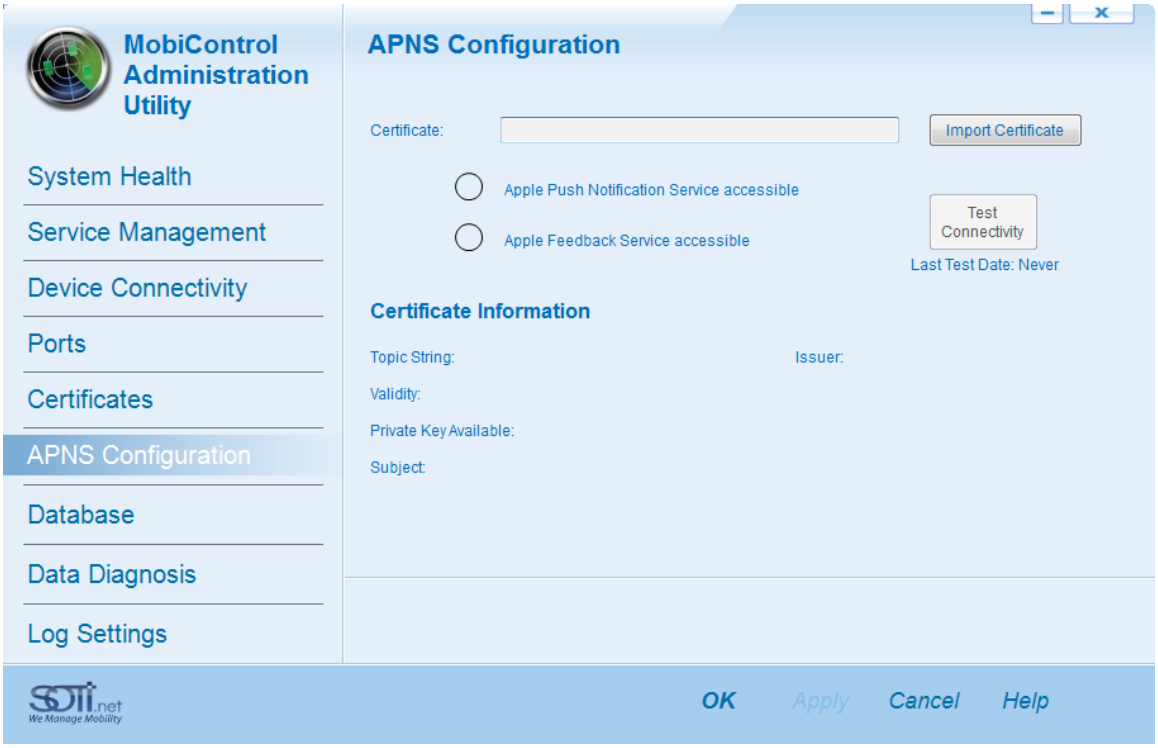


Administration Utility

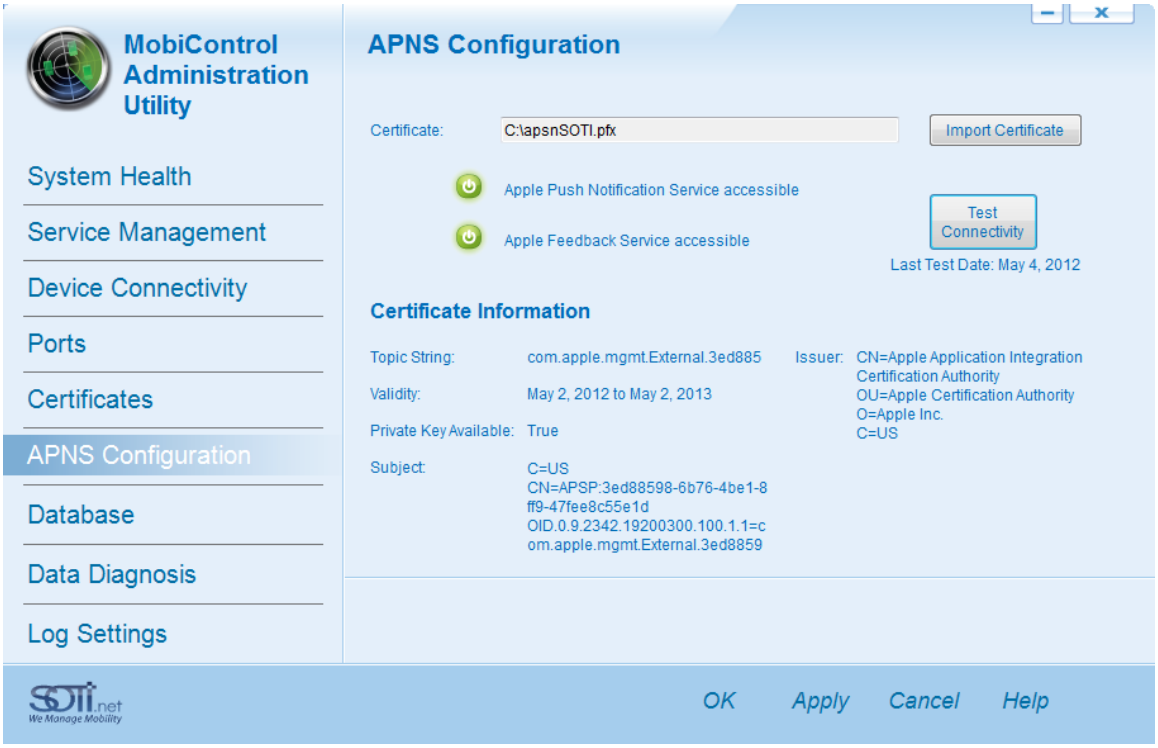
2. Once the MobiControl Administration Utility is opened, go to the **APNS Configuration** tab on the left hand side.

The MobiControl Administration Utility

3. In the APNS Configuration Panel, click **Import** and browse to the APNS Certificate that was exported during the request process. This should be a .pfx or a .p12 file.
   Enter the password that was set up for this certificate.



4. After the certificate has been imported, click the **Test Connectivity** button. The Apple Push Notification Service and Apple Feedback Service lights should show up green .



APNS Configuration

5. Click Apply , and you are now ready to enroll your iOS devices.

Please see the "Adding iOS Devices" topic on page 1034 for more information on how to enroll your iOS device.

Installing MobiControl Web Console

MobiControl Prerequisites

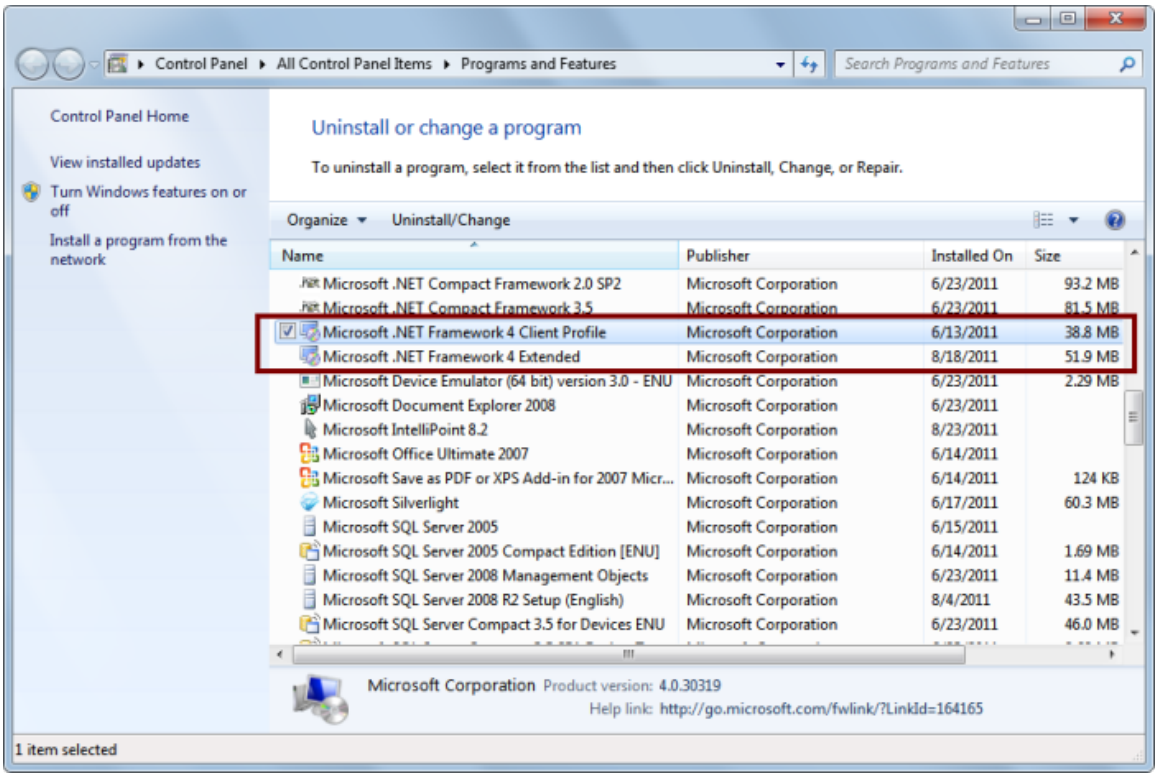
In order for the MobiControl Web Console to be installed separately from the initial MobiControl installation the following conditions must be met:

- MobiControl Deployment Server must be installed and running within the network.
- Microsoft .Net Framework v4 must be installed on the machine that will receive the web console.

For assistance installing MobiControl for the first time, please visit Installing MobiControl.

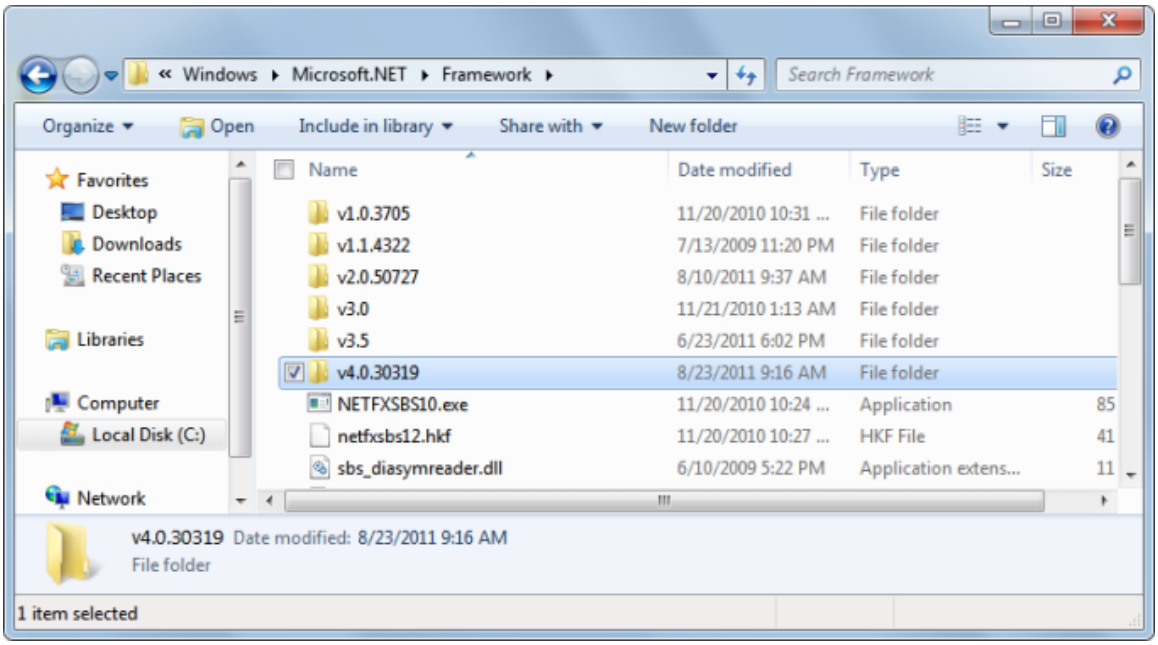
To verify if Microsoft .Net Framework is installed on the computer:

- Check Programs and Features to see if a line item exists for Microsoft .Net Framework 4



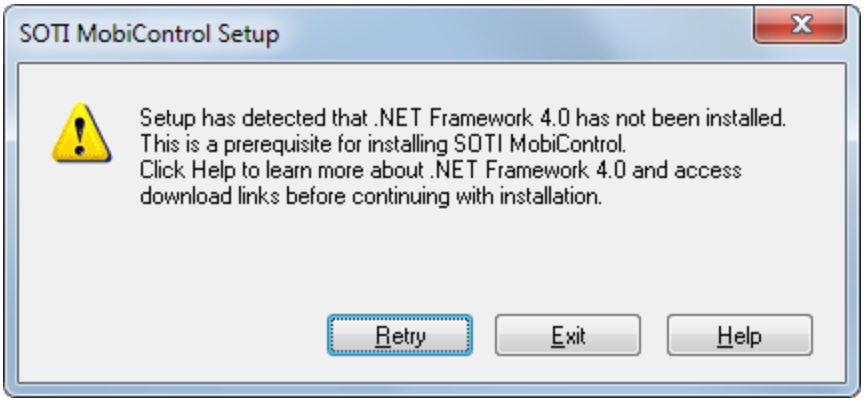
Programs and Features

- Check the Windows file system to see traces of Microsoft .Net Framework 4 in `c:\windows\Microsoft.Net\Framework\`



Windows file system

If Microsoft .Net Framework 4 isn't installed the following error will occur:



To resolve this issue, please install the appropriate version of .Net Framework 4. For systems other than Windows Server 2008 sp1, click here. For Windows Server 2008 sp1, click here.

Install MobiControl Web Console on a separate server

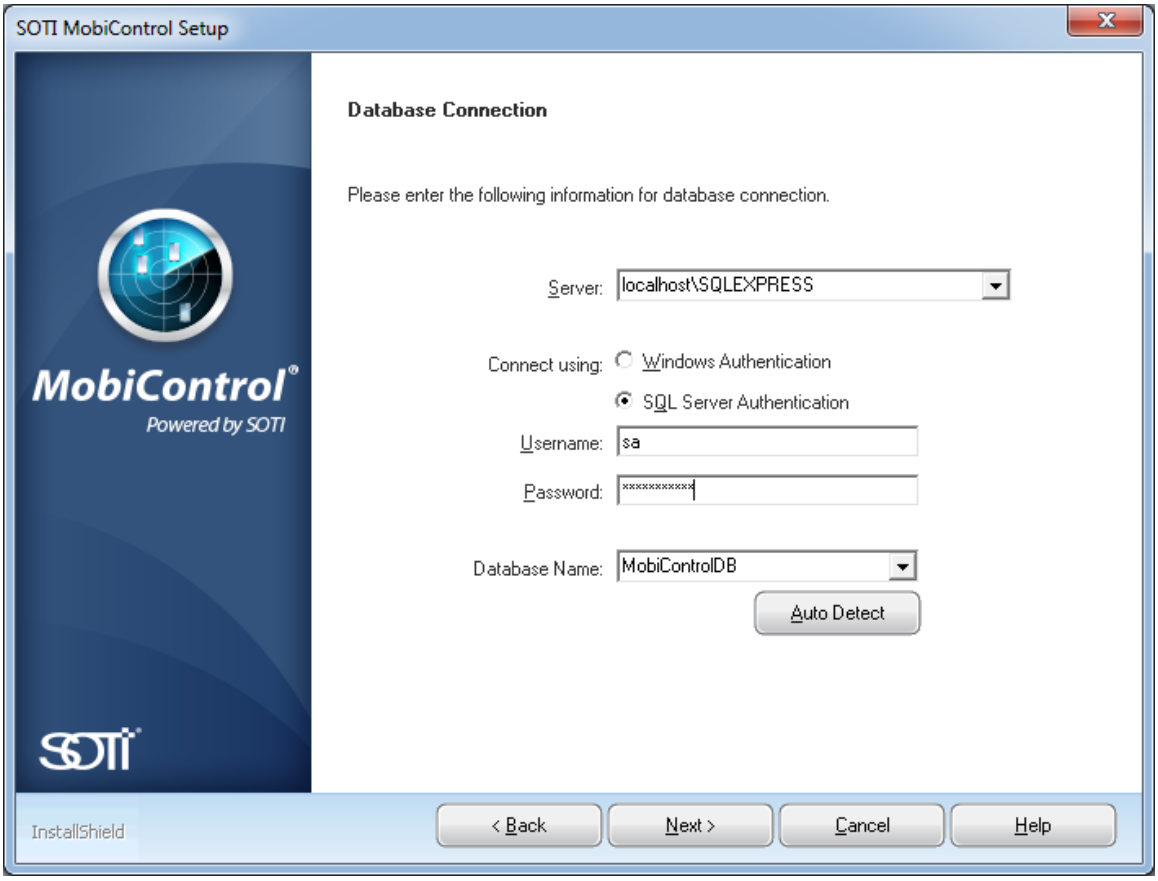
The following steps must be completed to install the MobiControl Web Console on a server other than the deployment server.

1. Launch the MobiControl Installer

   Launch the MobiControl installer on the computer that will become the MobiControl Web Console host will be and navigate to the installation screen and ensure that only Web Console is selected

2. Provide SQL Connection Info

   Enter the appropriate SQL connection information and continue.



3. Continue through the installation and press **Finish**.

Install MobiControl Web Console on an existing deployment server

The following steps must be completed to install the MobiControl Web Console on an existing the deployment server.

1. Launch the MobiControl Installer

   Launch the MobiControl installer or access **Programs and Features** select MobiControl and click **Change**.on the computer that will become the MobiControl Web Console host will be and navigate to the installation screen and ensure that when placing the check box on Web Console no other components check box is changed. Removing the checkbox will cause that component to be uninstalled.

2. Continue through the installation and click **Finish**.

Secure Email Access Install

The Secure Email Access Filter allows you to achieve greater control with devices receiving email from your Exchange Service. When the filter is installed, you can block access to Exchange on certain devices as well as other controls.

To successfully install the Exchange ActiveSync Filter, the MobiControl Root CA must be installed on the server that is publishing the Exchange ActiveSync Service.

Below shows how to install the filter on your Exchange Server.

1. Prerequisite Steps
2. Install MobiControl's Secure Email Access filter
3. (Optional) 3rd party Exchange ActiveSync Filter Configuration

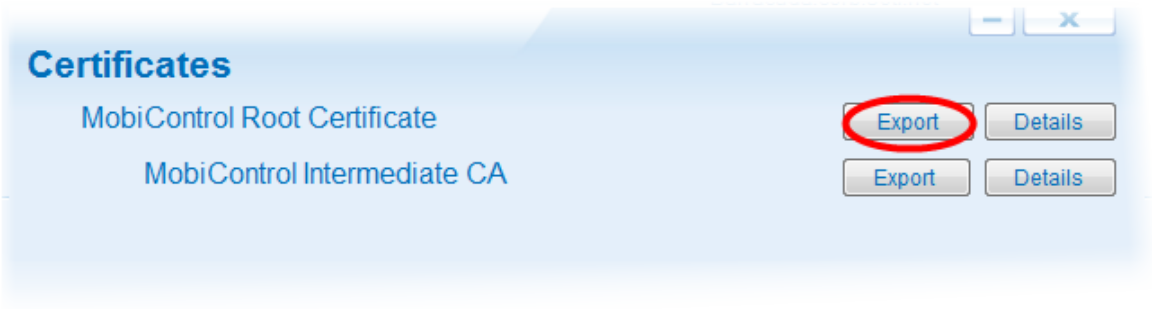
Prerequisite Steps

The prerequisite steps show how to install the MobiControl Root CA on the Exchange Server.

1. Go to the MobiControl Administration Utility and go to **Certificates**.

The MobiControlAdministration Utility (MCAU)

2. Click the **Export** button at beside the MobiControl Root Certificate label.

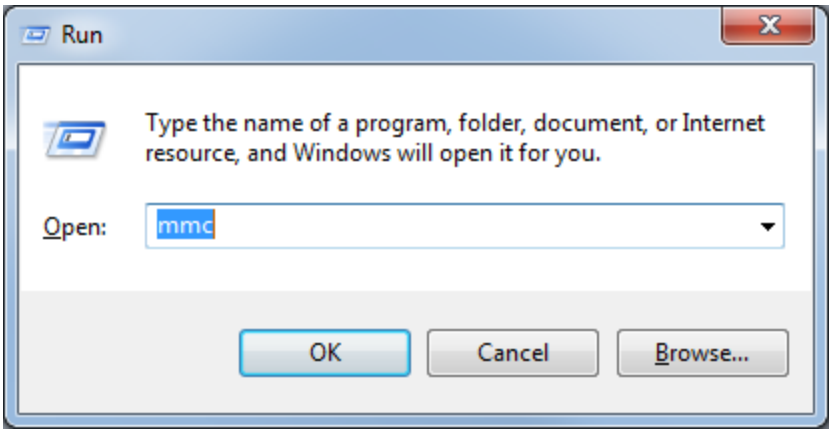


Export the MobiControlRoot Certificate

3. Save the exported certificate in a directory that is easy to remember.

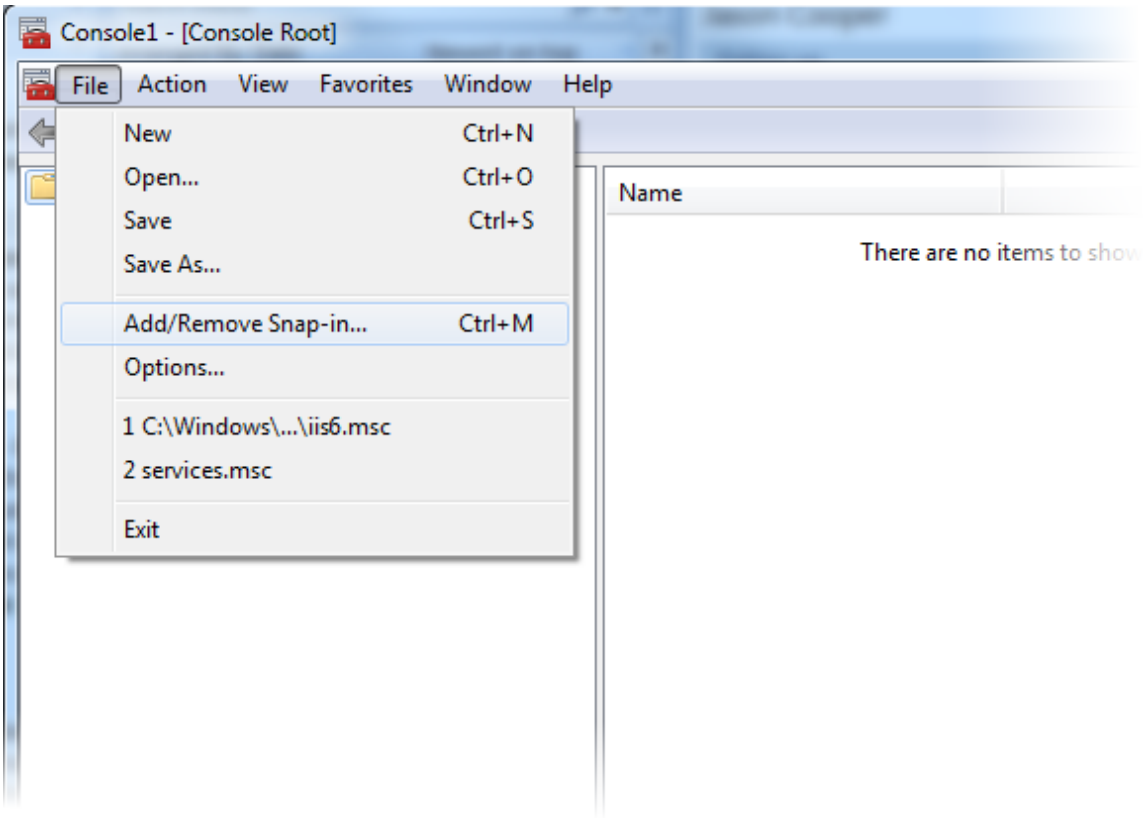
Next we need to go to the server with the Exchange ActiveSync Service.

1. Open the Microsoft Management Console (MMC) by opening up the run command and typing **mmc**.



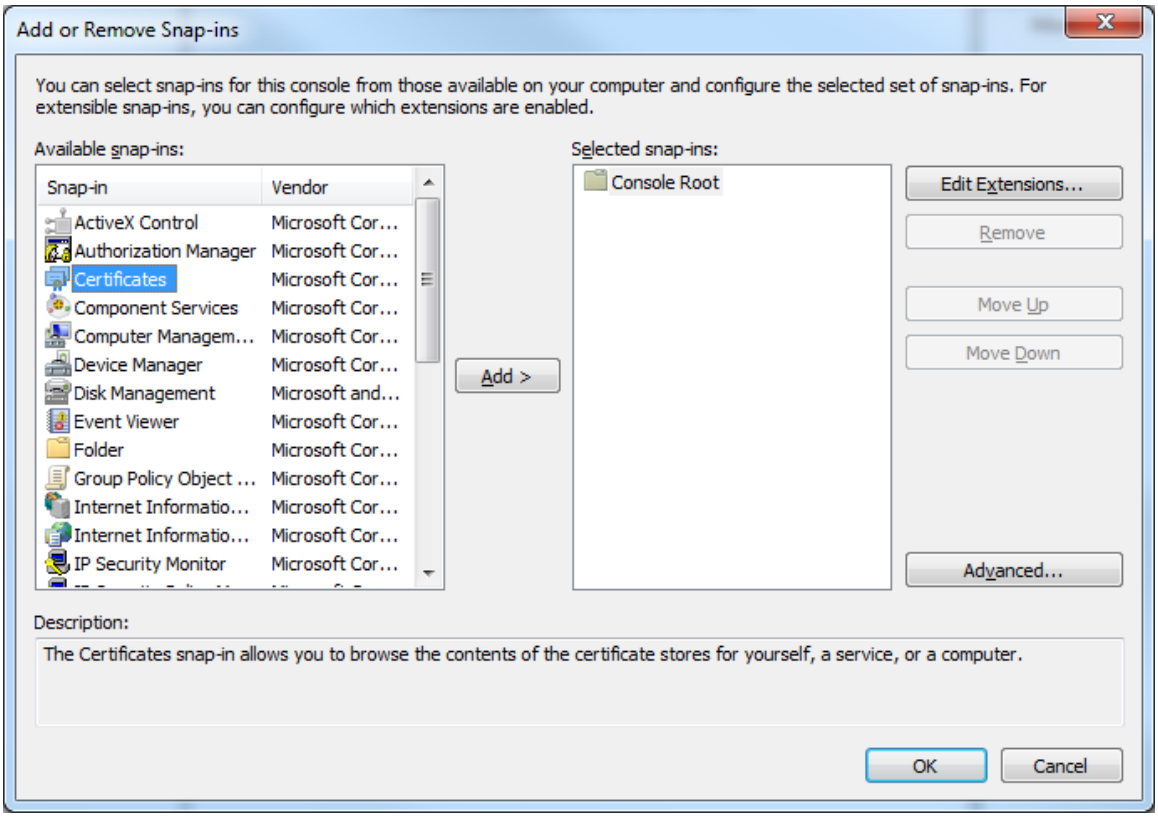
Open the Microsoft Management Console.

2. In MMC, click File then **Add/Remove Snap In...**



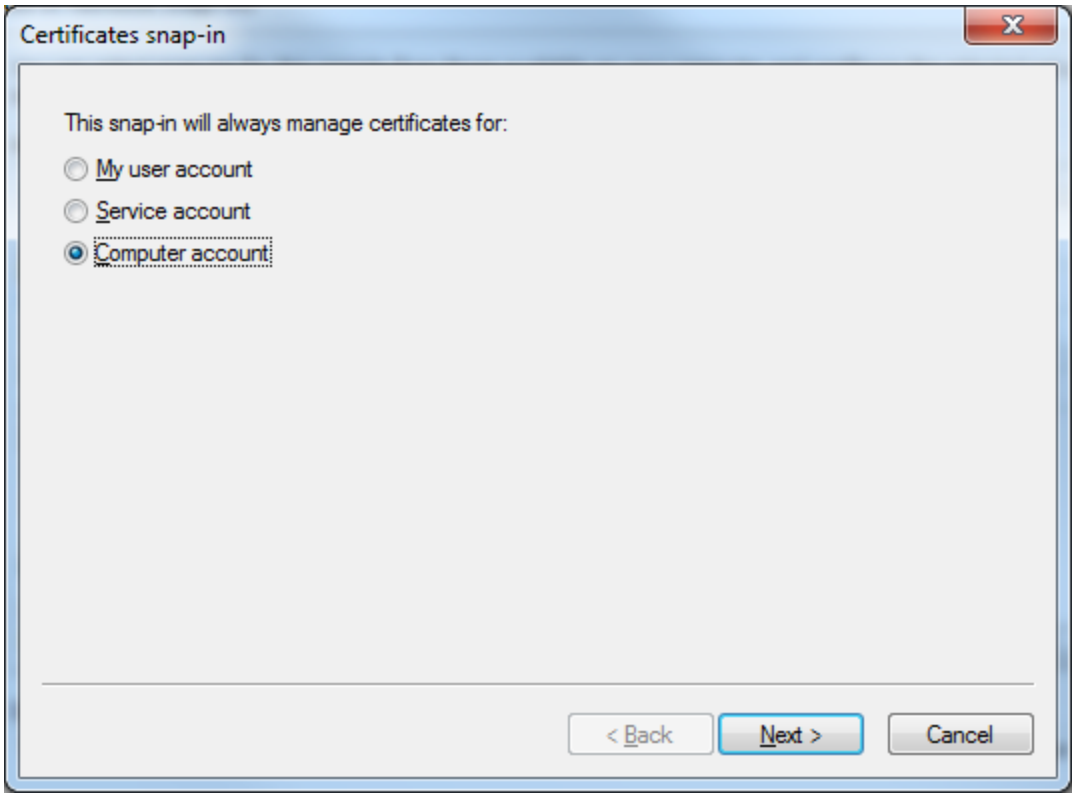
Adding Snap-ins

3. Select the **Certificates** snap-in and click **Add >**.



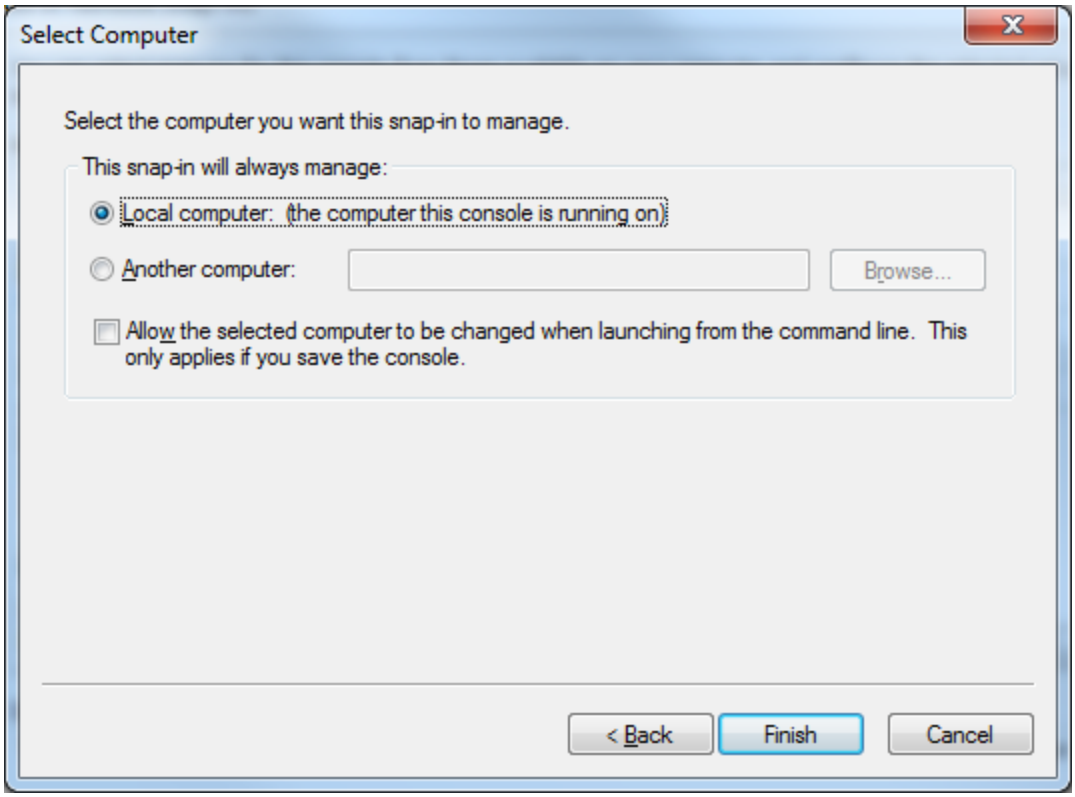
Adding the Certificates Snap-in

4. A new window will appear asking to select an account. Select the **Computer account** and click **Next**.



Select the Computer Account.

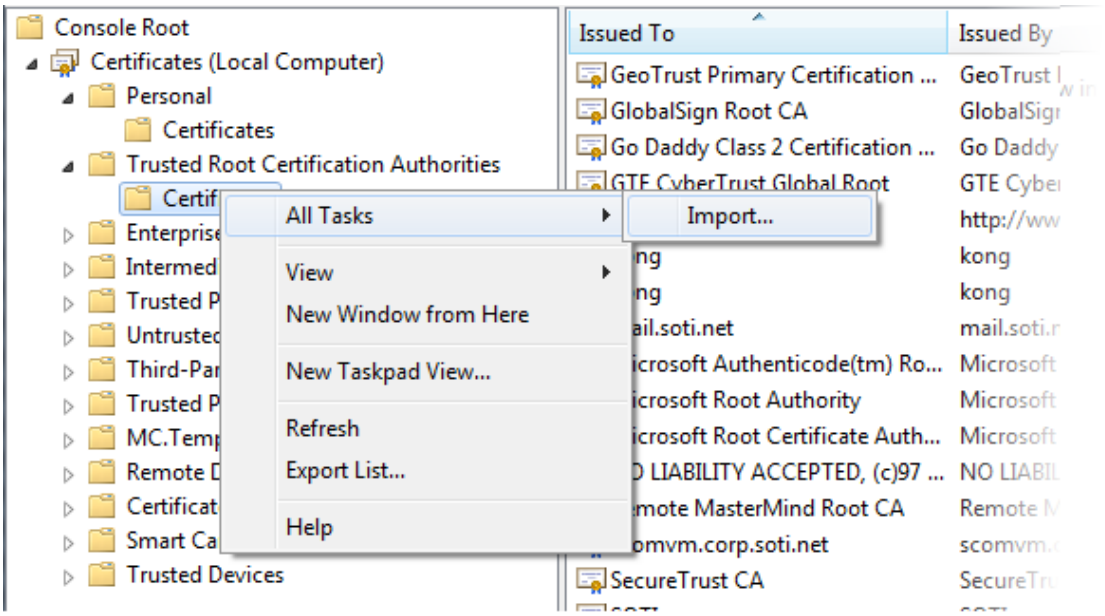
5. On the next screen select **Local Computer** and click **Finish**.



Select Computer

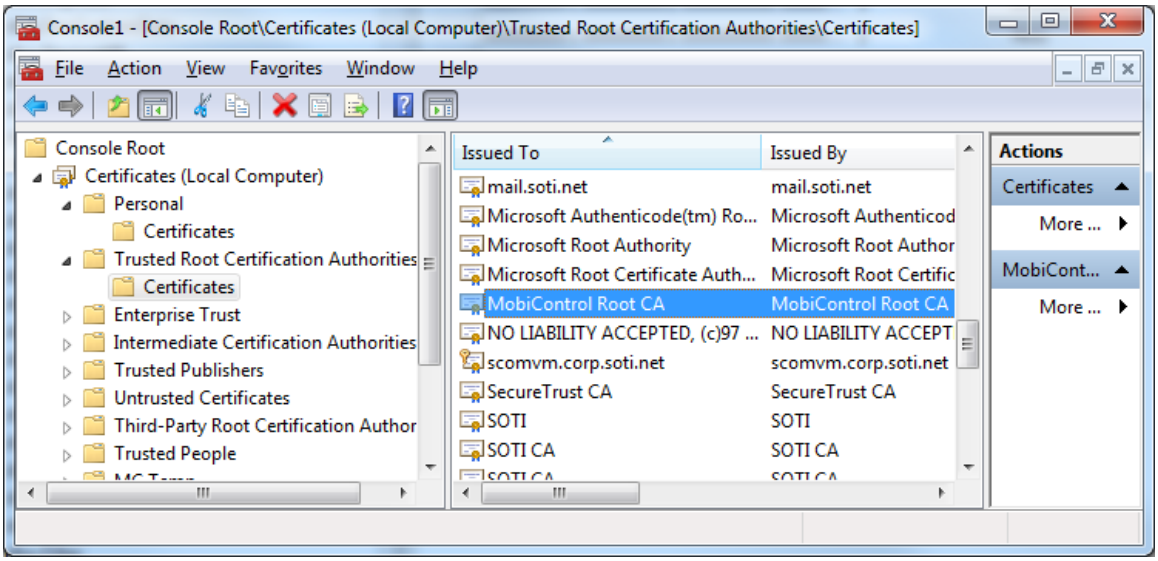
6. After clicking Finish, click **OK** in the Add or remove Snap-ins window.

7. Expand the Certificates (Local Computer) tree on the left side and go to Trusted Root Certification Authorities, then Certificates. Right click the Certificates folder and go to All Tasks then **Import**.



Importing a new CA

8. Follow the steps in the Certificate Import Wizard leaving all settings default. After the wizard has finished you will see the MobiControl Root CA in your Trusted Root Certification Authorities.

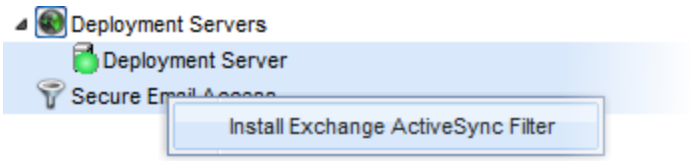


The MobiControl Root CA

Install MobiControl's Secure Email Access filter

MobiControl's Secure Email Access Filter must be installed on the server that is publishing the Exchange ActiveSync service. Typically this is the same computer that is hosting OWA (Outlook Web Access).

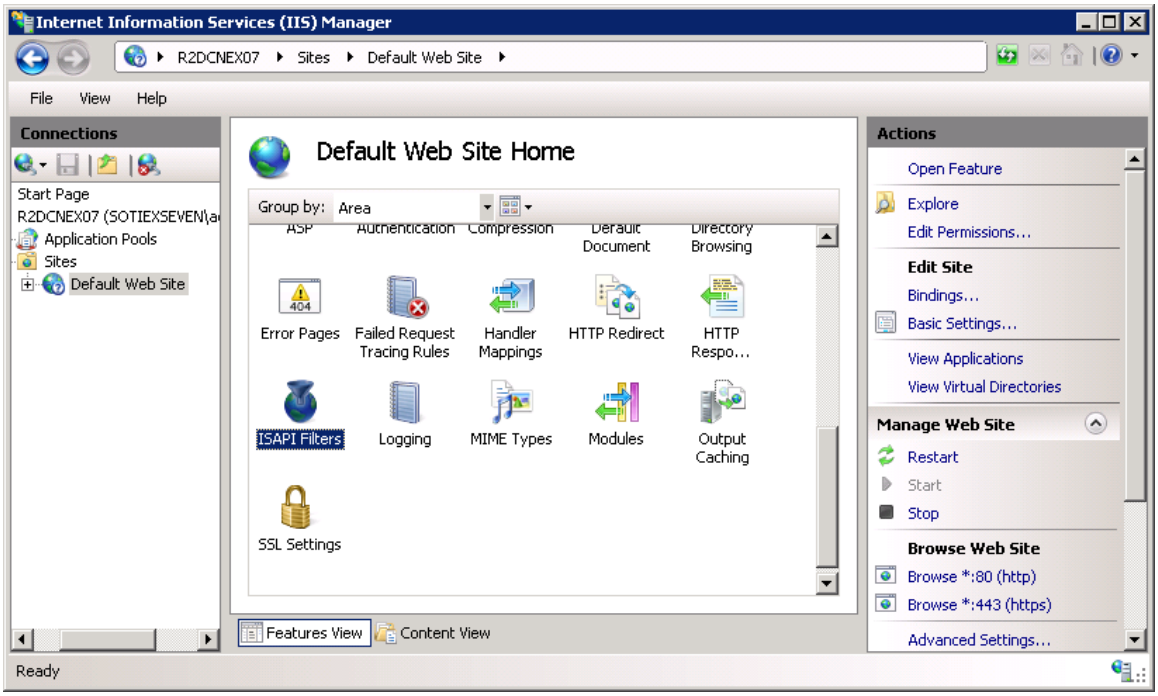
1. From the server where the Secure Email Access filter will be installed, open Internet Explorer and browse to the MobiControl Web Console
2. Log in to the Web Console as an Administrator based account that has the "Configure Deployment Servers" permission
3. Select the All Devices tab at the top of the MobiControl Web Console and then select the Servers tab located along the bottom of the Web Console
4. Right click on the Secure Email Access filter listed under the Deployment Server, and select Install Exchange ActiveSync Filter



5. Save and then run the ExchangeActiveSyncFilter.exe program. This will place the needed files onto the server.

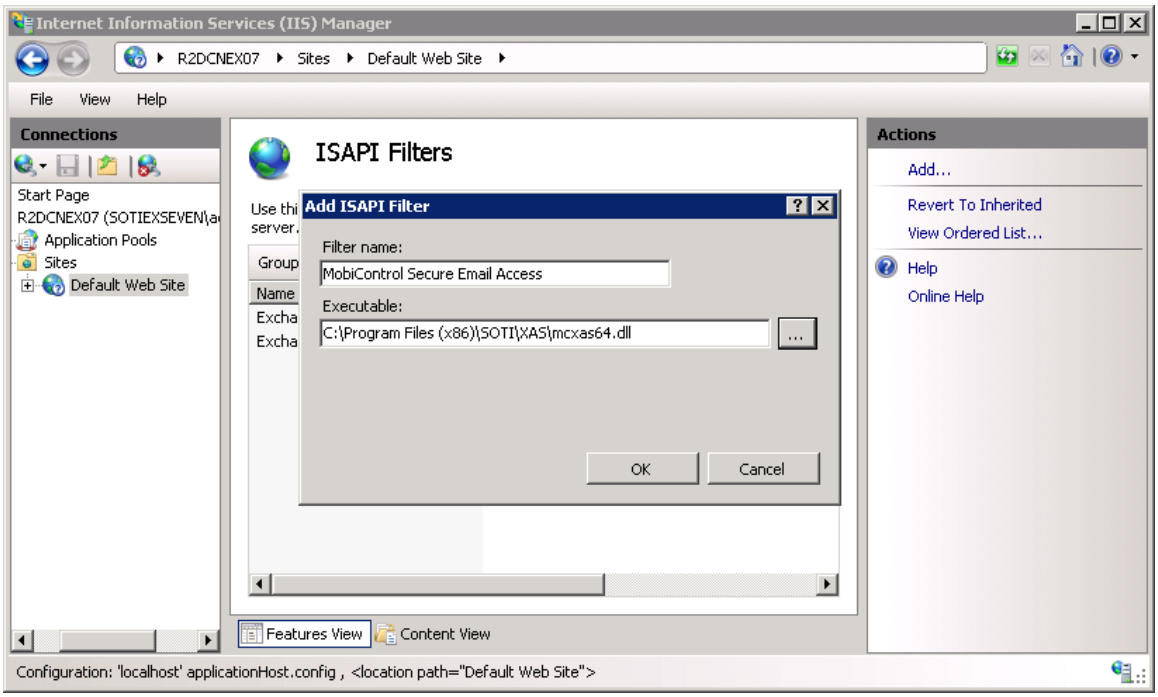
> **NOTE:**
>
> Depending on your Internet Explorer settings, you may be prompted to allow file downloads from the web page

6. Open IIS manager and select the web site that is publishing Exchange ActiveSync
7. Select ISAPI filters and select Add from the list of actions



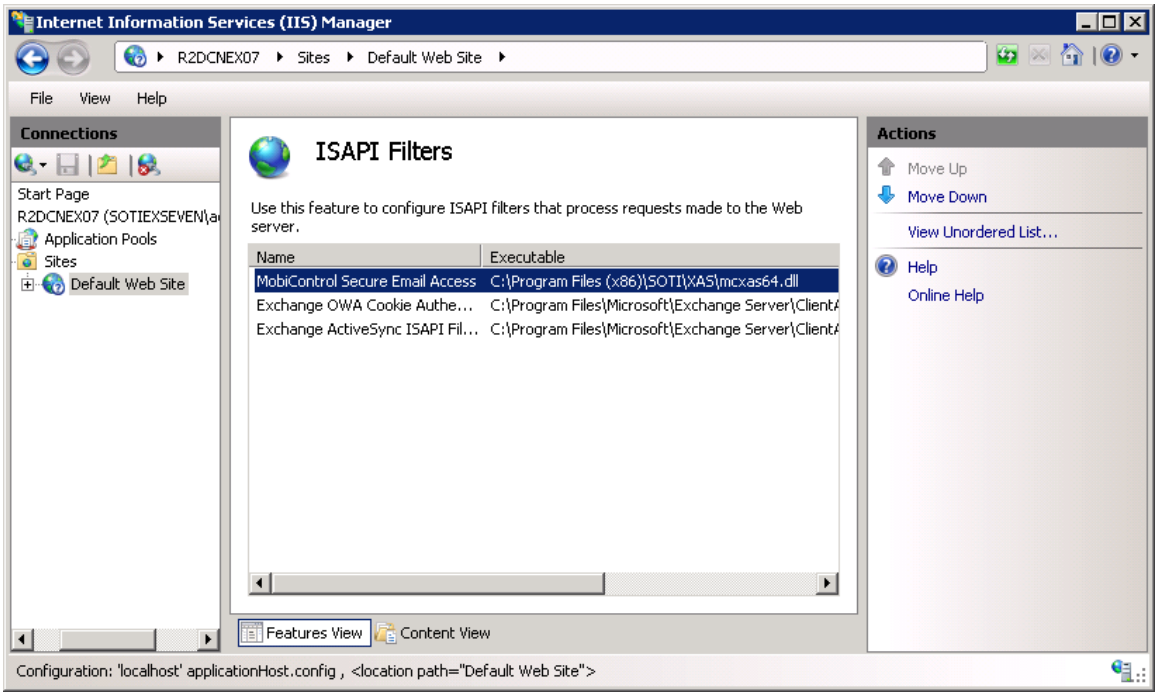
8. Enter MobiControl Secure Email Access as the filter name

9. For the Executable, If the Exchange ActiveSync site is running in a 32-bit application pool, select \Program Files\SOTI\XAS\mcxas.dll or, if the Exchange ActiveSync site is running in a 64-bit application pool, select \Program files\SOTI\XAS\mcxas64.dll



10. Select OK to save the filter

11. In the resulting list of filters, ensure that the MobiControl Secure Email Access filter is listed above the Microsoft Exchange ActiveSync filter. If this is not the case, select View Order List from the available actions, highlight MobiControl Secure Email Access and select Move Up to place it at the top



NOTE:

MobiControl's Secure Email Access required communication between the server that is publishing Exchange ActiveSync where the filter is installed, to the MobiControl Web Console. This communication happens over SSL on port 443.

3rd party Exchange ActiveSync Filter Configuration

Before you begin, the following components must be installed/enabled.

1. IIS 7 with ASP.NET role service enabled.

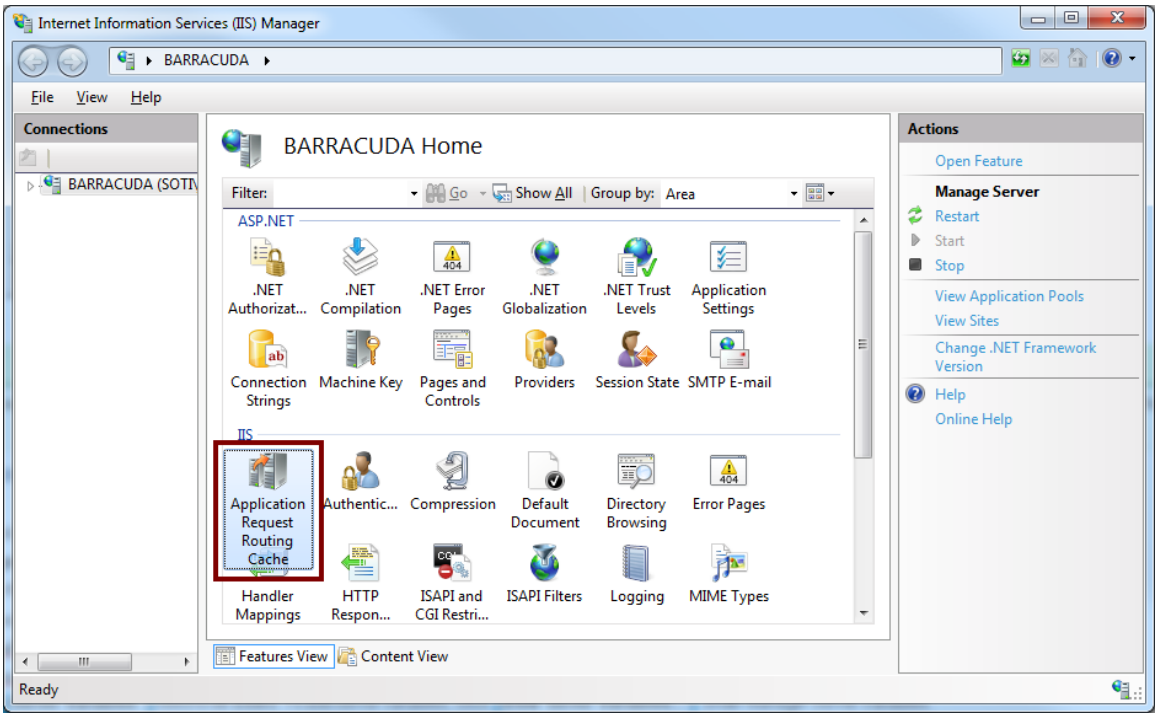
2. URL Rewrite Module installed (version 2.0 is required)

3. Application Request Routing version 2.5 (Link)

The URL Rewrite Module and Application Request Routing version 2.5 are both installed at the same time.

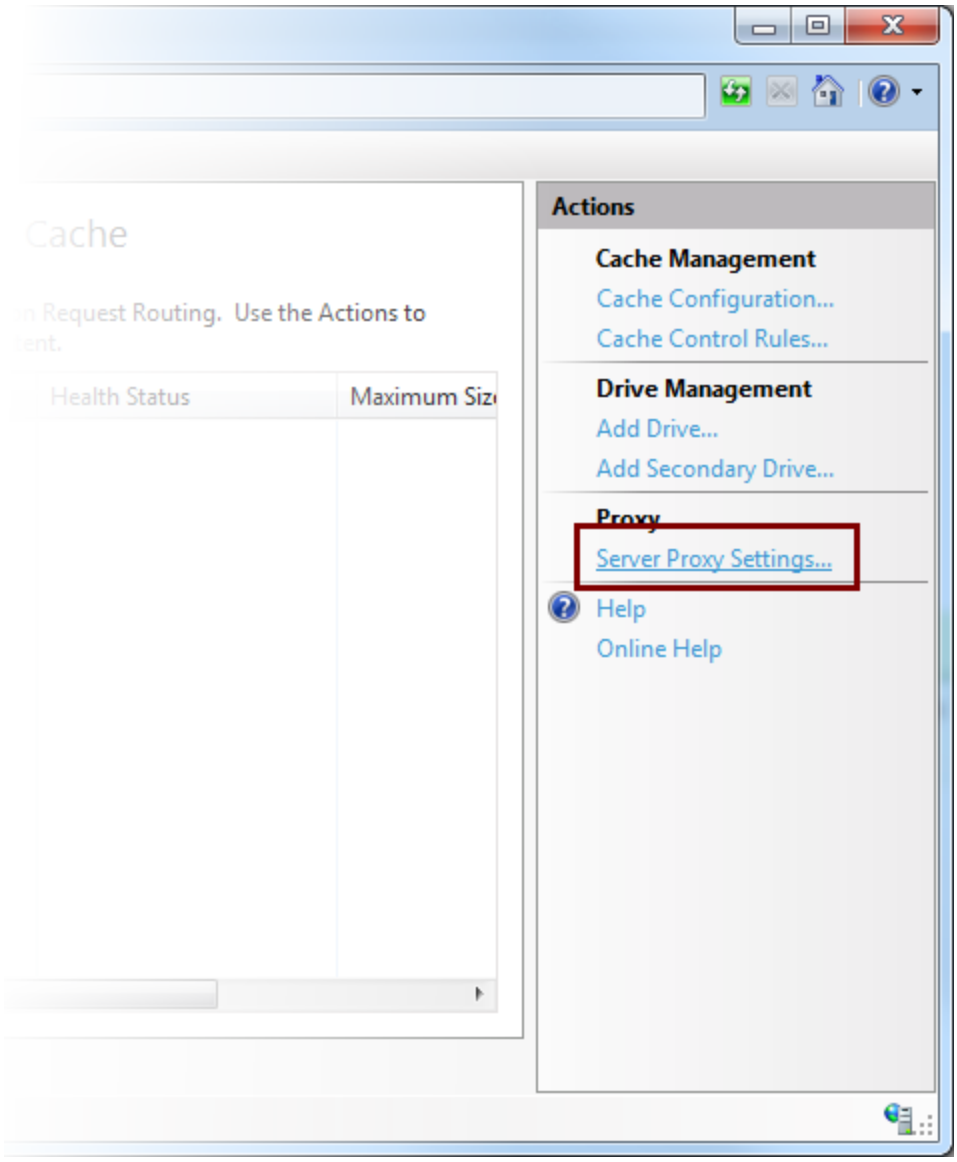
After installation, please follow these steps:

1. Open the IIS manager
2. Select the server in the tree view on the left hand side and then click on the **Application Request Routing** feature.



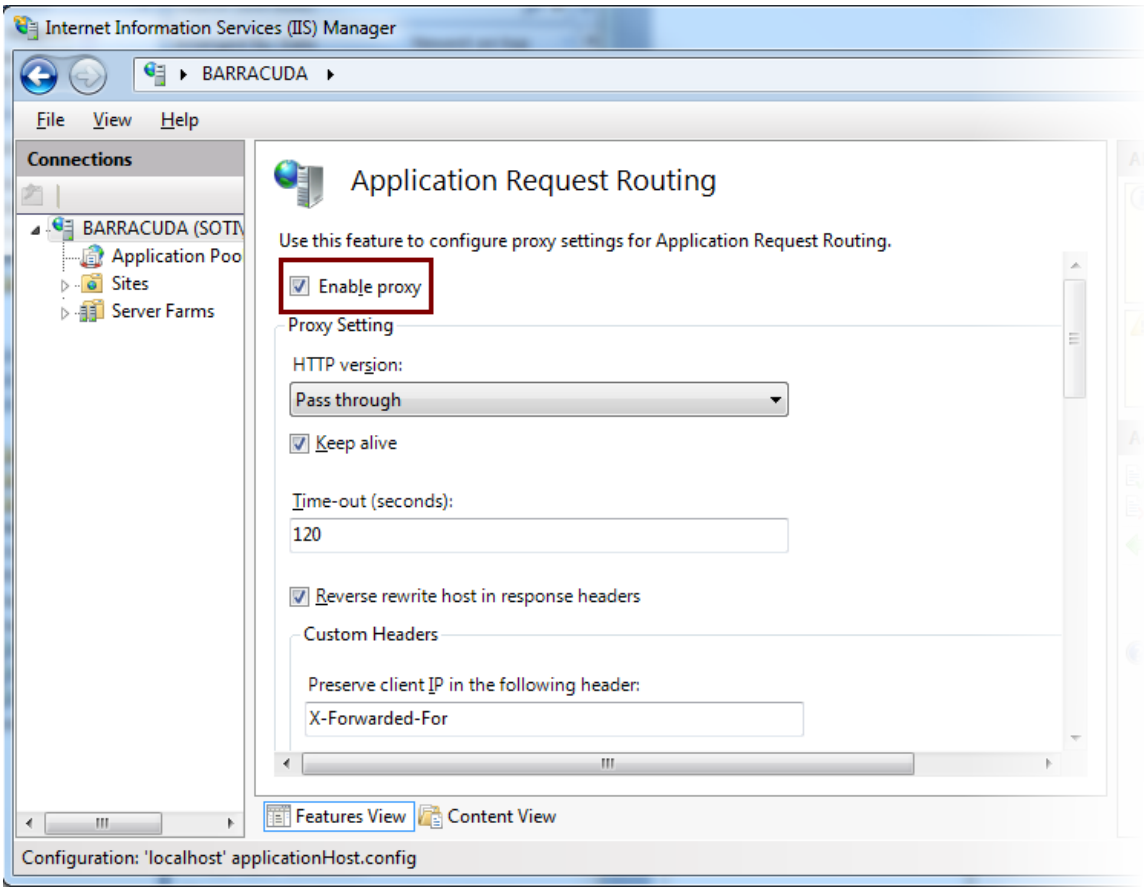
Application Request Routing

3. On the right menu, click **Server Proxy Settings** in the Proxy Section



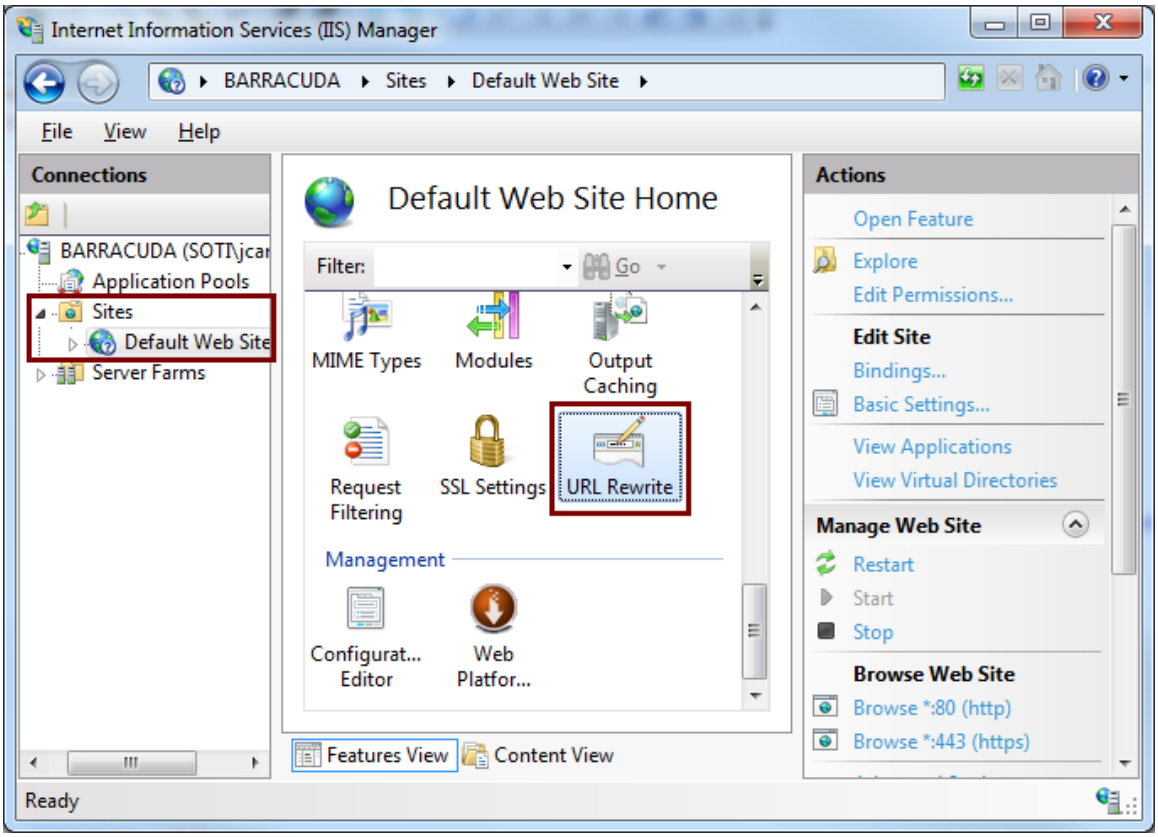
Server Proxy Settings

4. Check the **Enable Proxy** check box. Leave the default values for all the other settings on this page. Click Apply on the right side to commit the change.



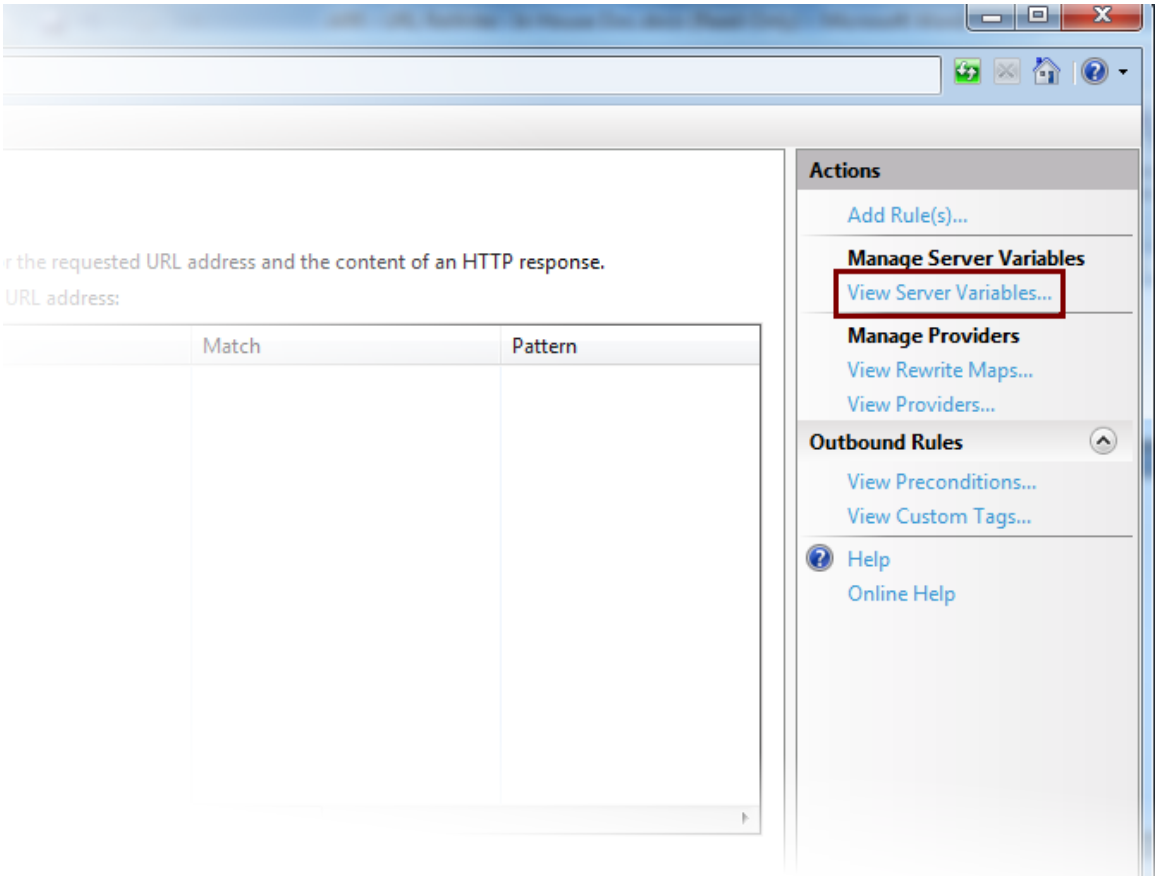
Enable Proxy

5. Next step is to add the **HTTP_ACCEPT_ENCODING** server variable and **Inbound and Outbound** rules. To do this, please go to the left hand panel and select the **Default Web Site** and then select **URL Rewrite**.



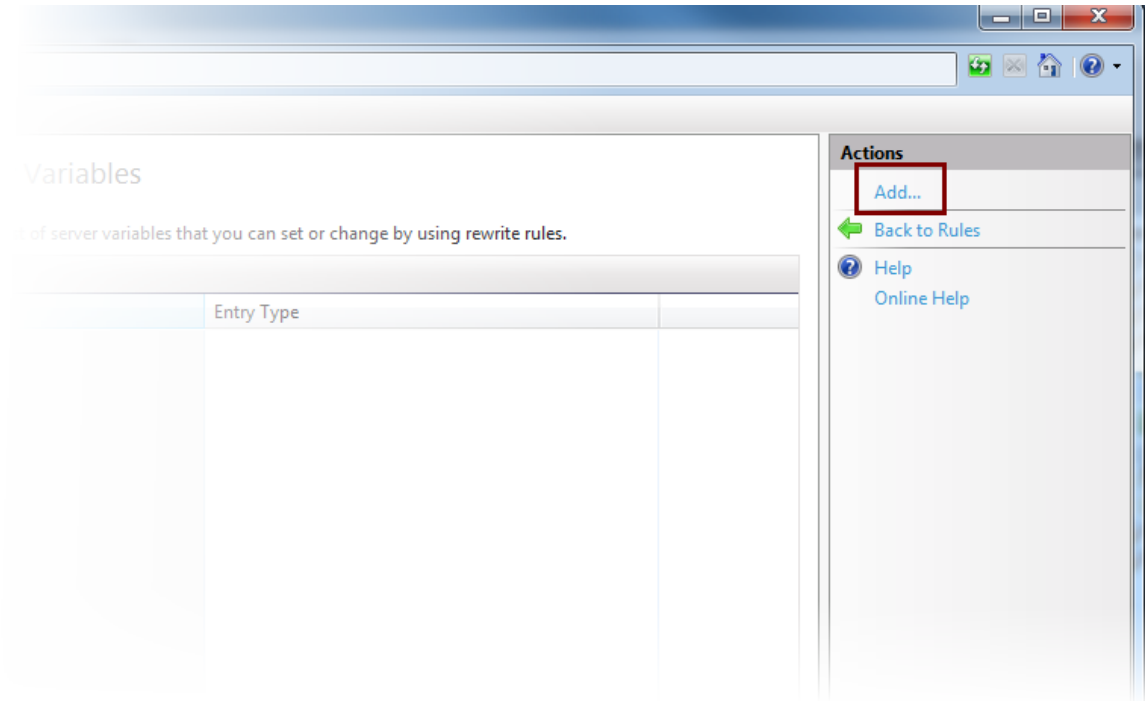
URL rewrite

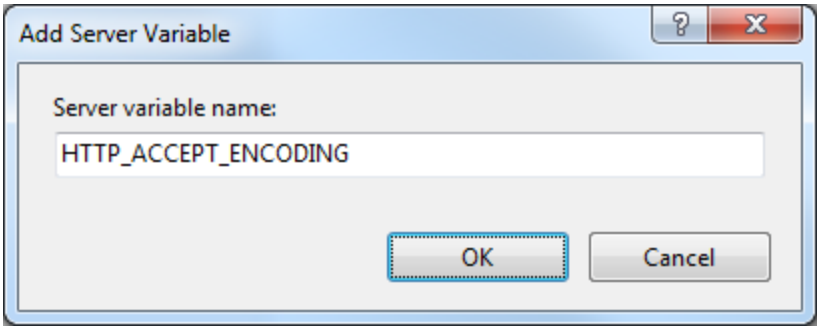
In the URL Rewrite page, select **View Server Variables** on the right hand side.



View Server Variables

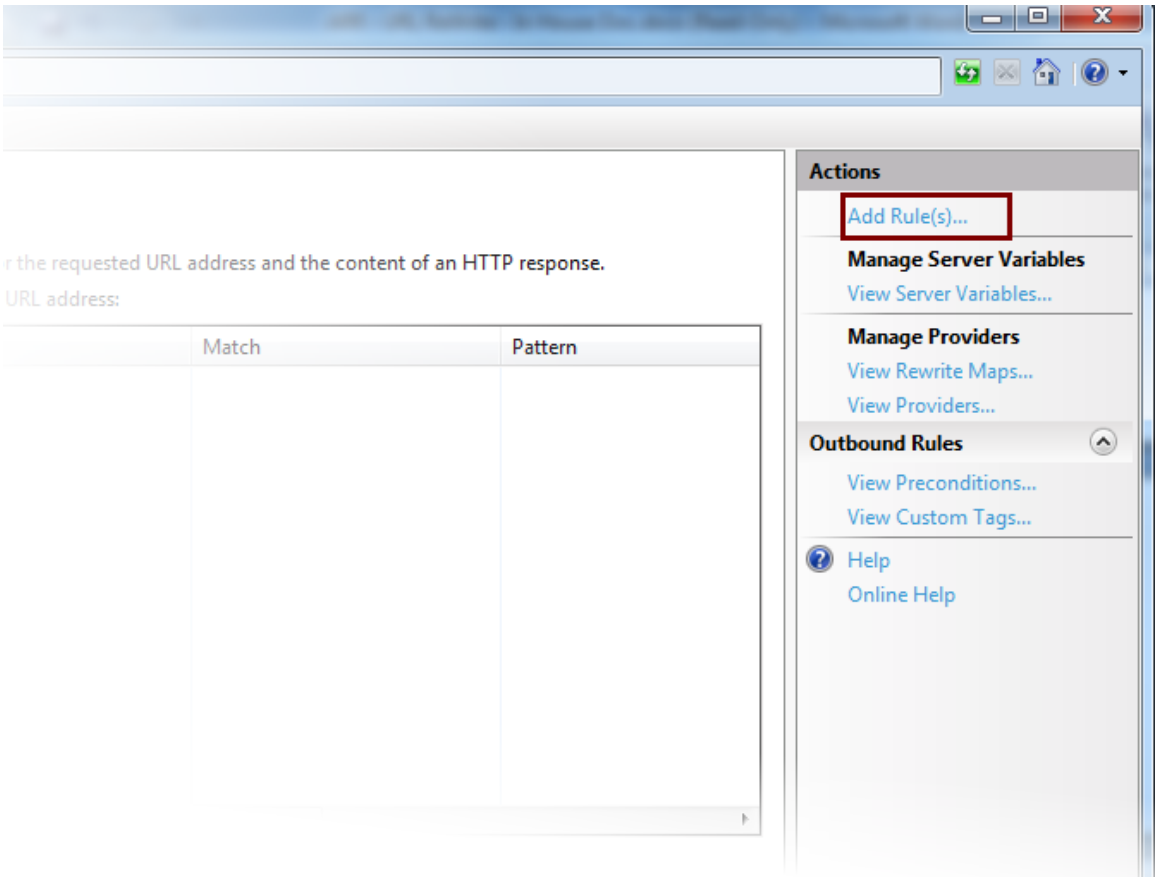
6. Click the **Add...** link on the right side of the page to add the **HTTP_ACCEPT_ENCODING** variable. Click **OK** then **Back to Rules**.





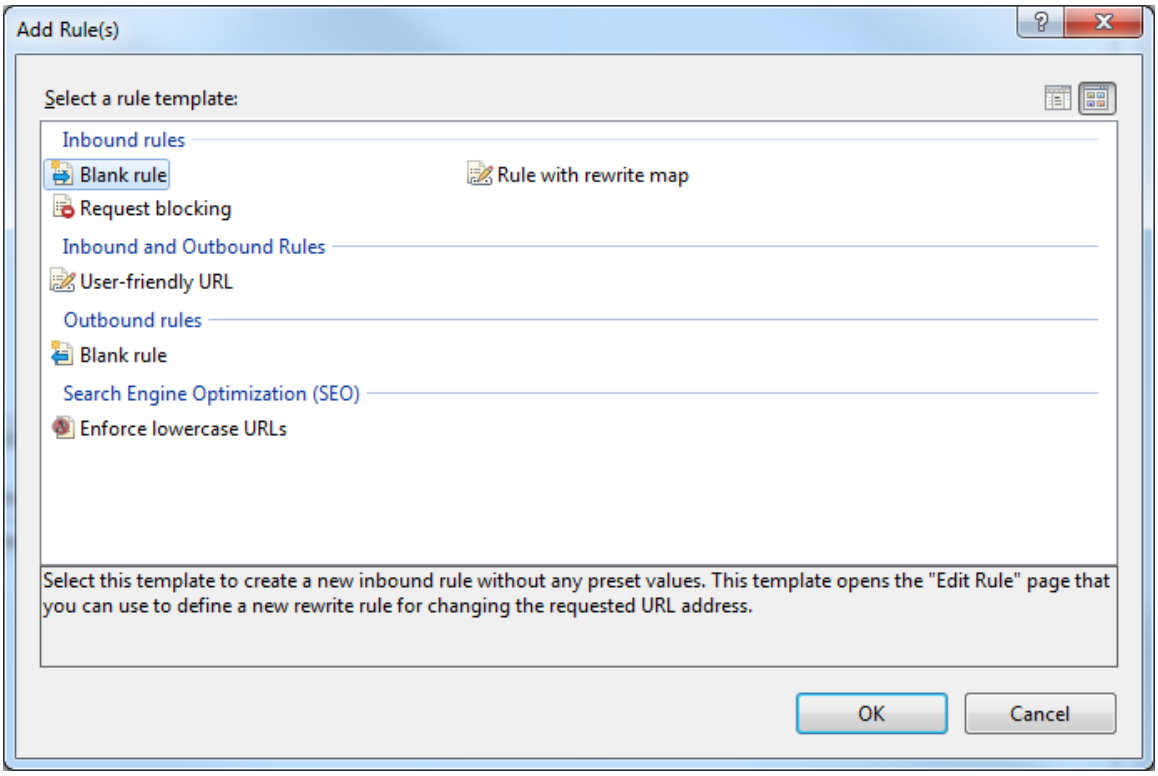
Adding a server variable

7. Click the **Add Rule(s)...** link on the right side to add Inbound and Outbound rules.



Add rule(s)...

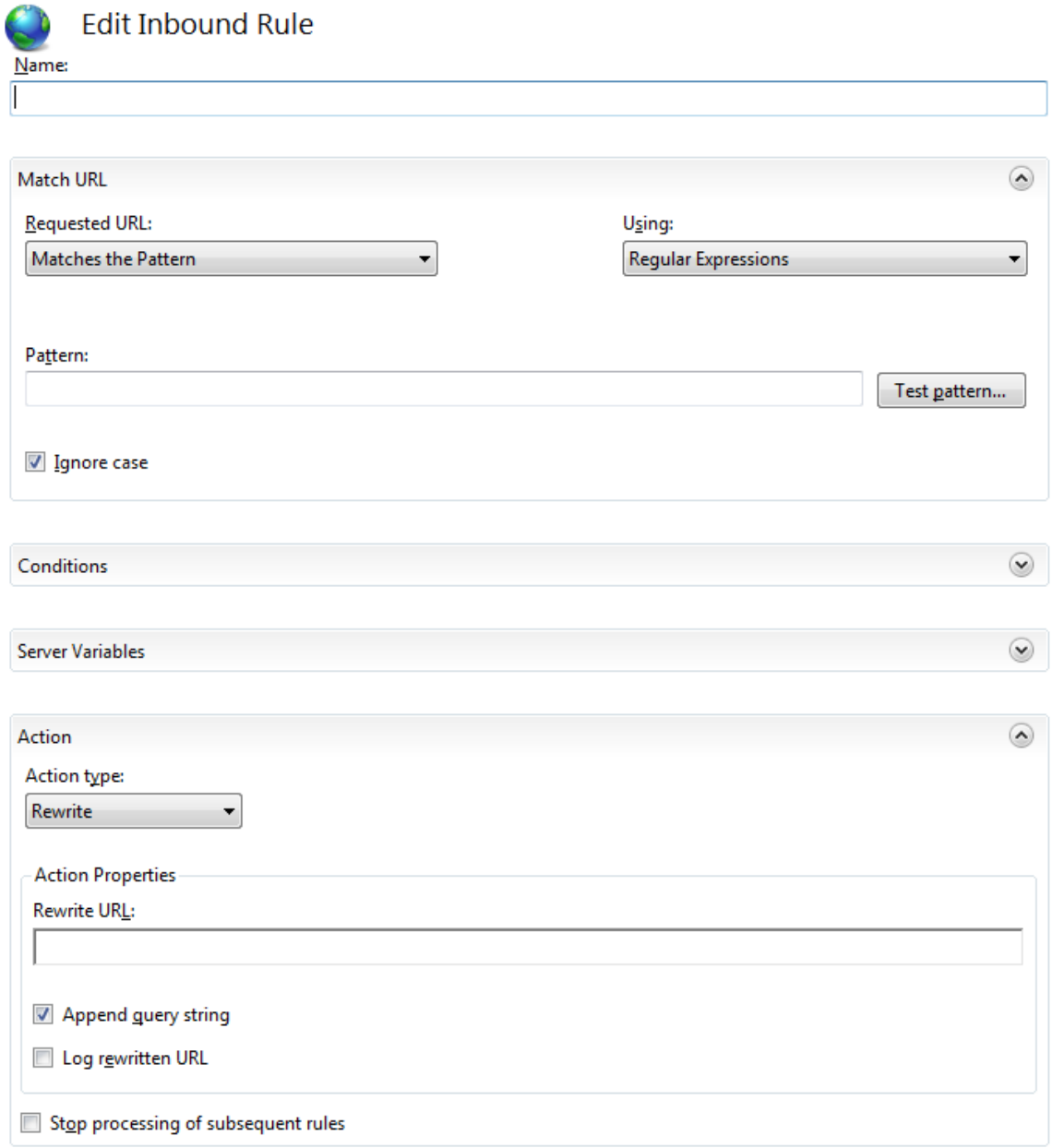
8. When creating the Inbound and Outbound rules, select **Blank Rule** under the respected heading and click **OK.**



Adding a Blank Inbound or Outbound rule

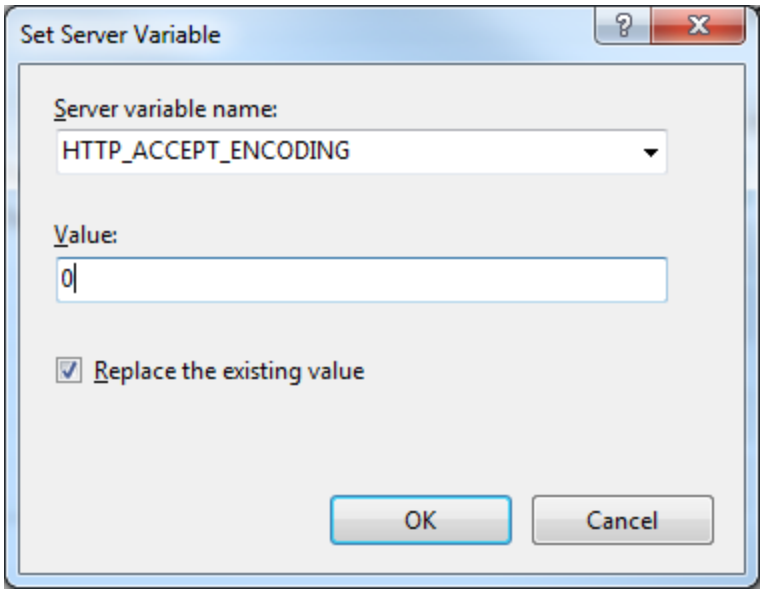
9. On the page shown below, the following fields need to have values entered (Please ensure that you enter your appropriate owa address):

Name	ReverseProxyInboundRule1
Pattern	^(.*)
Rewrite URL	https://owa.myDomain.com/{R:1}



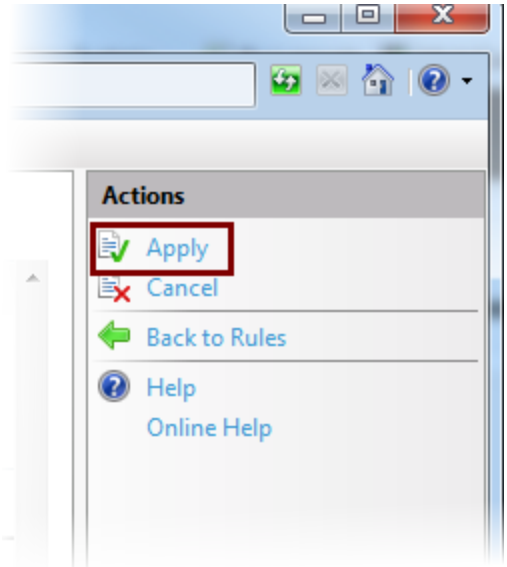
Inbound Rule creation page

After the values have been entered, the server variable needs to be added. To do this, expand the **Server Variables** panel. Click Add and choose **HTTP_ACCEPT_ENCODING** from the drop down menu. Under value, enter **0**, then click OK.



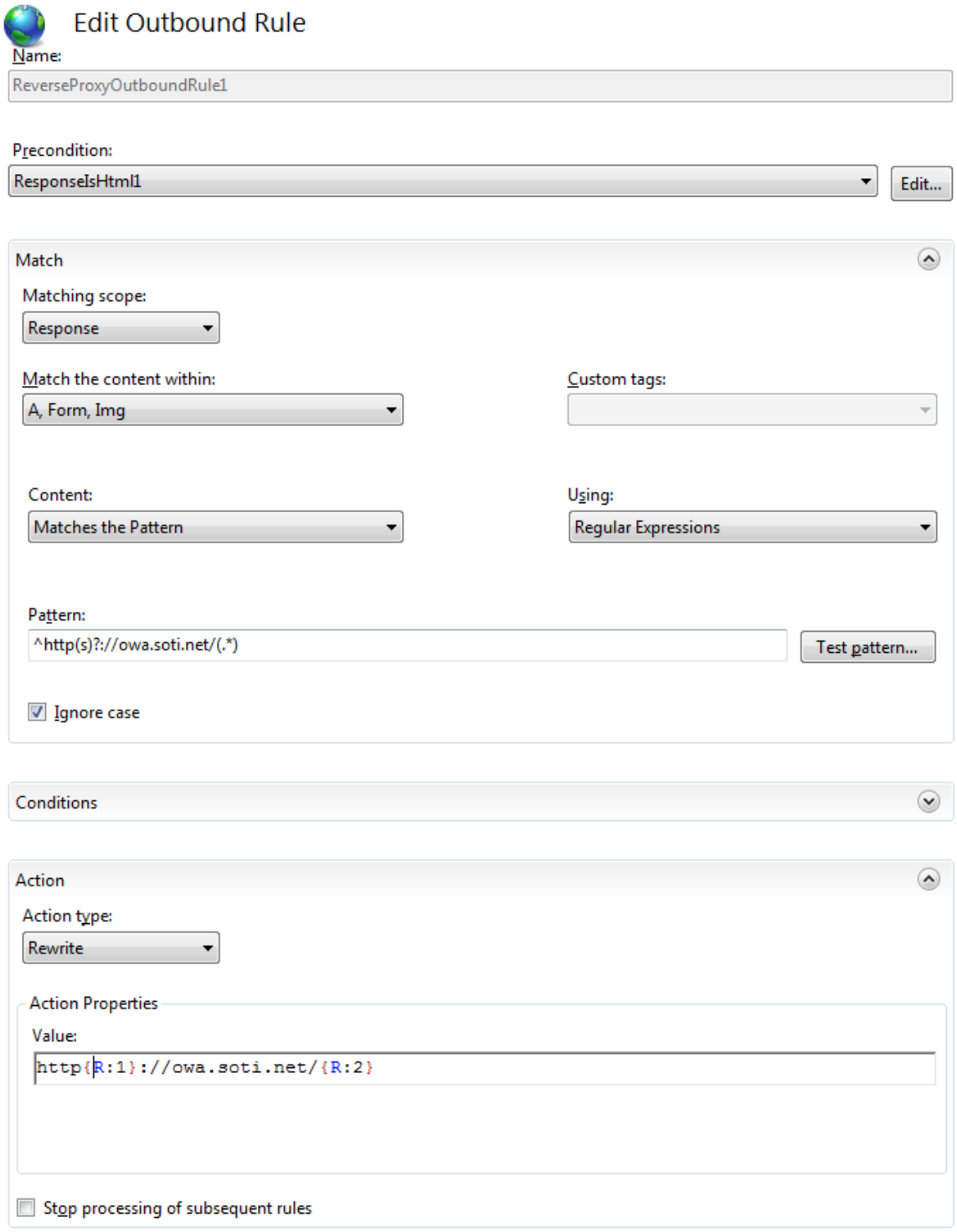
Set Server Variable

After entering all required values, click **Apply**.



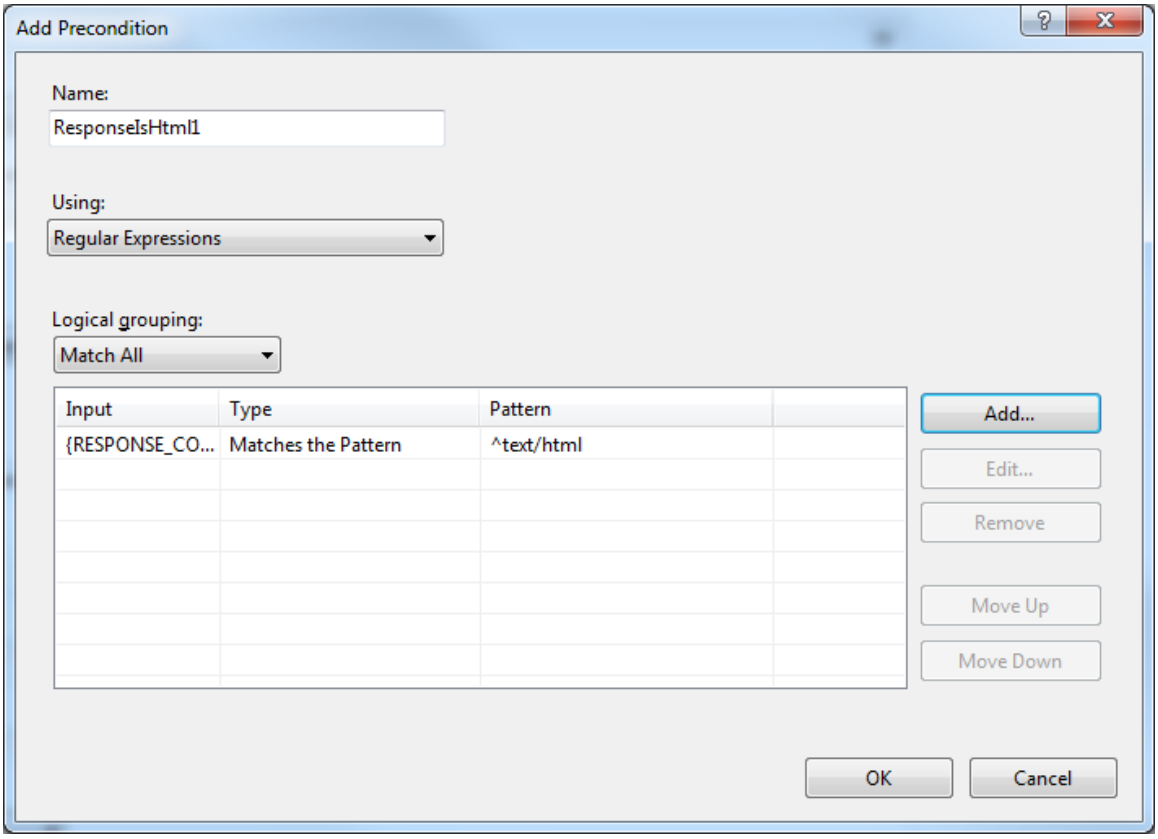
Apply Inbound Rule

10. Create a new blank rule to create an Outbound Rule. Please see below for what values to set on this page:

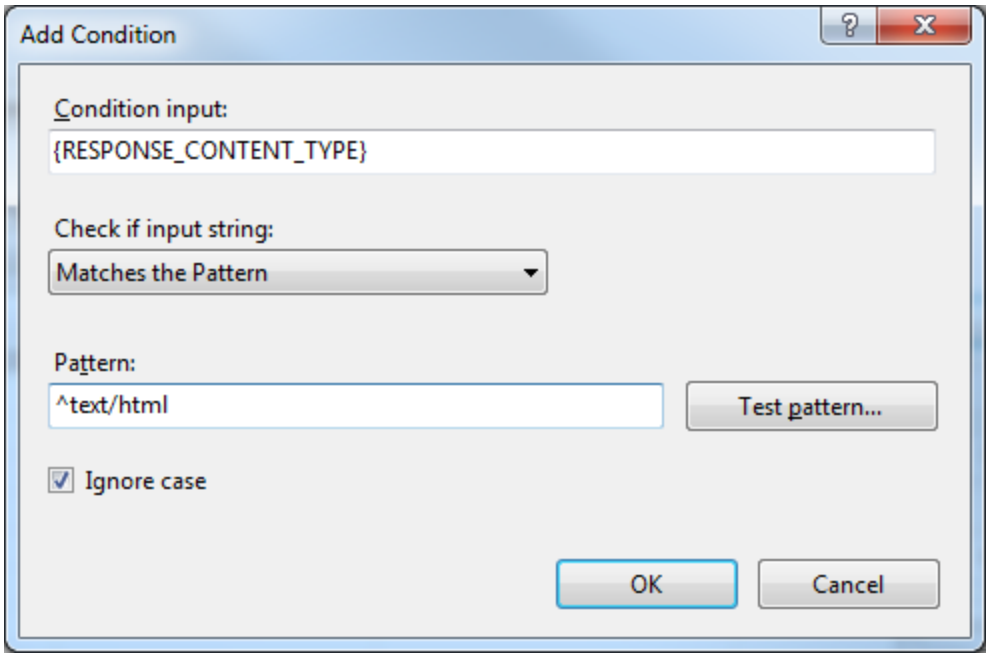


Outbound rule page

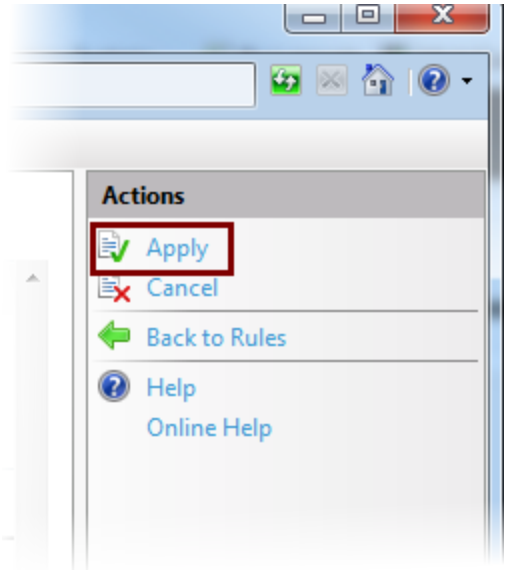
Under precondition, you will need to create a new condition. To do this, select **<Create New Precondition...>**. When the pop up window appears, click **Add...** to add a pattern:



Add Precondition



After entering all required values, Click OK then click **Apply**.



Apply Outbound Rule

11. After the rules have been created, click the IIS server, and restart.

To confirm that everything has been configured properly, go to C:\inetpub\wwwroot and open the web.config file in notepad. Your file should look similar to this:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
        <rewrite>
            <rules>
                <rule name="ReverseProxyInboundRule1">
                    <match url="^(.*)" />
                    <serverVariables>
                        <set name="HTTP_ACCEPT_ENCODING" value="0" />
                    </serverVariables>
                    <action type="Rewrite" url="https://owa.soti.net/
{R:1}" />
                </rule>
            </rules>
            <outboundRules>
                <rule name="ReverseProxyOutboundRule1" preCondition="
ResponseIsHtml1">
                    <match filterByTags="A, Form, Img" pattern="^http
(s)?://owa.soti.net/(.*)" />
                    <action type="Rewrite" value="http{R:1}://owa.sot
i.net/{R:2}" />
                </rule>
                <preConditions>
                    <remove name="ResponseIsHtml1" />
                    <preCondition name="ResponseIsHtml1">
```

MobiControl Administration Utility

What is the MobiControl Administration Utility?

The MobiControl Administration Utility is a new utility that provides the MobiControl Administrators access to multiple configuration and status options on a single screen that previously existed in multiple locations. From the MobiControl Administration Utility the administrator can:

- Check on the status of the deployment
- Check on and test the status of services
- Adjust device connectivity settings
- Adjust Web Console connection ports
- Configure Deployment Server and APNS Certificates
- Configure the MobiControl Database connection
- Manage and configure the deployment server and management console logs

System Health

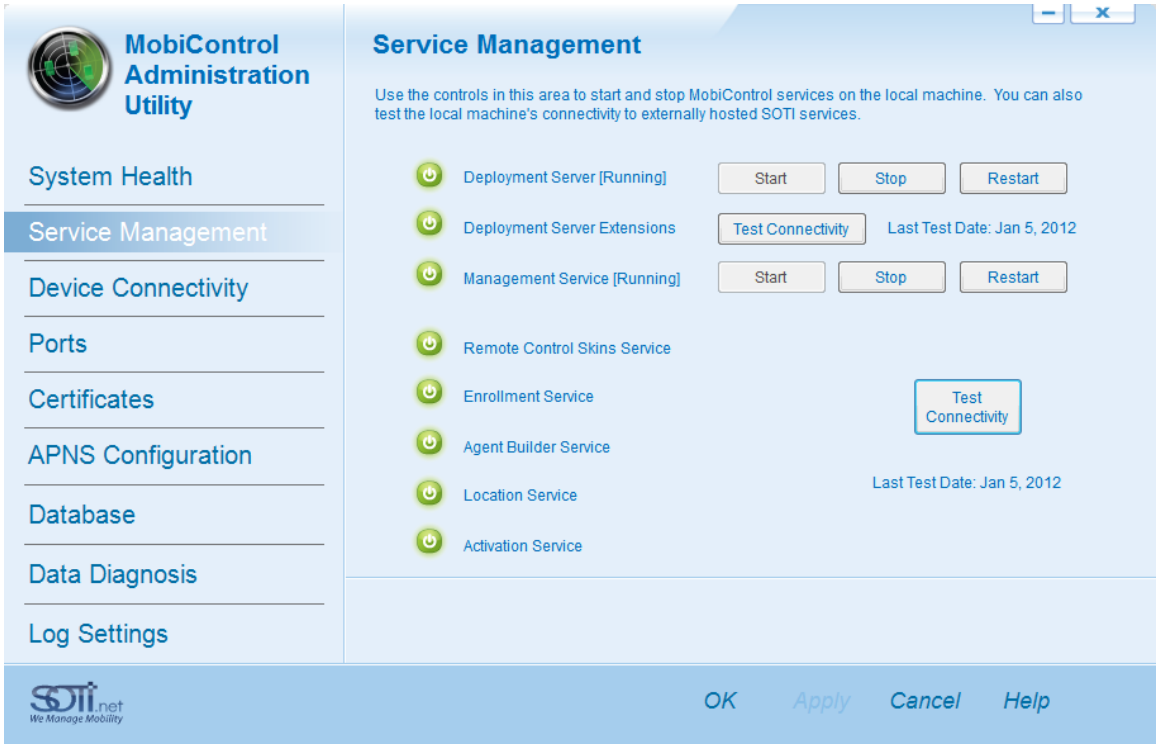
The **System Health** window allows the MobiControl administrator to see the status of all the main components in MobiControl along with their status. If the connection is good, it will appear Green. If not, it will appear Red.

System Health

Feature	Description
Deployment Server	Displays the status of the Deployment Server
SOTI Services	Displays the status of the SOTI Services
Database	Displays the status of the Database
Web Console	Displays the status of the Web Console

Service Management

The **Service Manager** section allows the MobiControl Administrator to view the status of all SOTI Services as well as test their connection. From this window the MobiControl Administrator can also perform Stop / Start and Restart functions on the **Deployment Server** and **Management Service** services without needing to access **services.msc**.



Service Manage

Feature	Description
Deployment Server [*Status*]	Displays the current running status of the Deployment Server service.
Deployment Server Extensions	Displays the current status of the Deployment Server Extensions enabling Apple iOS and Google Android devices to communicate properly.

Feature	Description
Management Service [*Status*]	Displays the current running status of the Management Service.
Remote Control Skin Service	Displays the current status of access ability to the Skin Catalog.
Enrolment Service	Displays the current status of the Deployment Servers connection to the SOTI Enrolment Service for Apple iOS and Google Android devices.
Agent Builder Service	Displays the current status of the connection to the Device Agent Manager stored on SOTI Servers for use in creating Windows Mobile device agents within the Web Console.
Location Service	Displays the current status of access ability to SOTI's Location Based Services.
Activation Service	Displays the current status of access ability to SOTI's Activation Server.

Device Connectivity

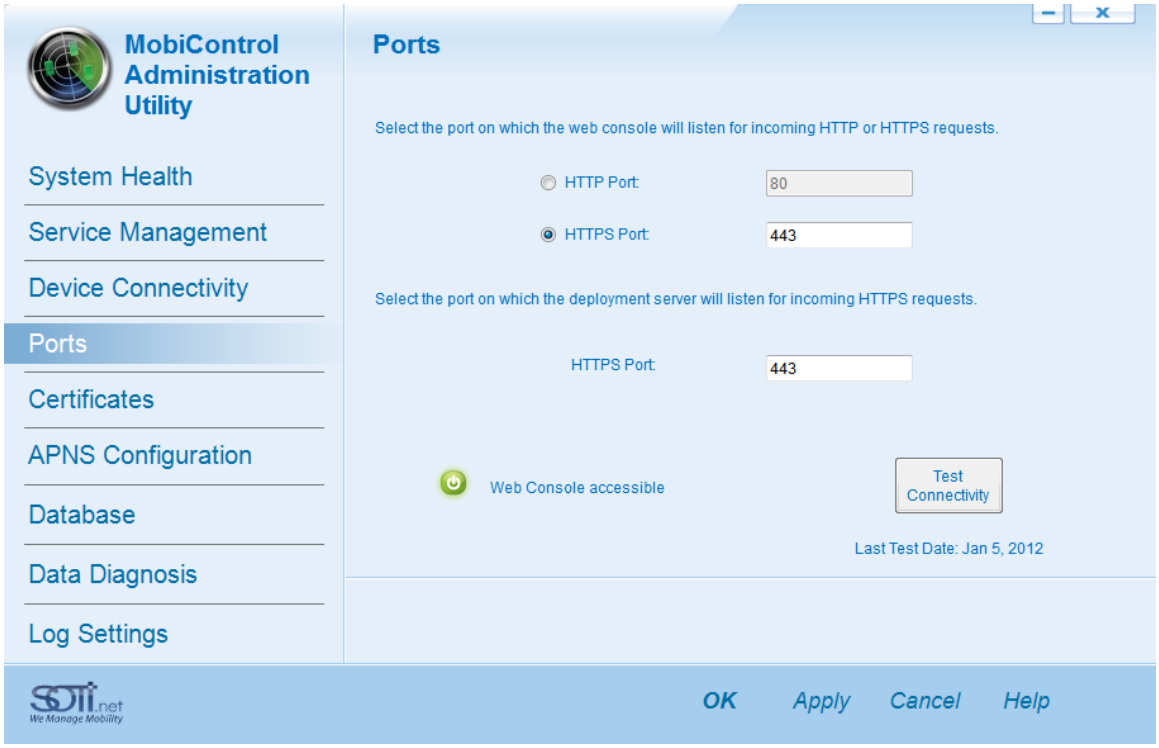
The **Device Connectivity** screen provides the MobiControl Administrator access to the main connection settings for both the **Management Consoles** and **Device Agents**. From this screen the MobiControl Administrator can change the Deployment server configuration without having to access the Deployment Server properties as well as the General Settings.

Device Connectivity

Feature	Description
Site Name	Displays the deployment's Site Name and allows the administrator to change it.
Deployment Server Name	Displays the Deployment Server(s) name and allows the administrator to change it.
Primary Agent Address and Port	Displays the primary IP or FQDN address for device connectivity along with it's assigned port.
Secondary Agent Address and Port	Displays the secondary IP or FQDN address for device connectivity along with it's assigned port.
Device Management Address and Port	Displays the external FQDN address for Apple iOS and Google Android device connectivity along with it's assigned HTTPS port.
Device Agent Access Available	Indicates whether network traffic to the indicated primary and secondary IP or FQDN and port are functional.
Device Management Access Available	Indicates whether network traffic to the indicated external FQDN and HTTPS port are functional.

Ports

The **Ports** screen allows the MobiControl Administrator to adjust the HTTP(S) ports for use with the MobiControl Web Console as well as specify the HTTPS port for the Apple iOS and Google Android to communicate over.



Ports

Feature	Description
HTTP / HTTPS Port	Displays the current web protocol and port being used for the MobiControl web console and administrator to change it.
HTTPS Port	Displays the current port being used for Apple iOS and Google Android device communicate and administrator to change it.
Web Console accessible	Displays the current status of the MobiControl web console.

Certificates

The **Certificates** screen provides the MobiControl Administrator the ability to view and update the current certificate that is bound to TCP port 443 and additional certificates needed for device management.

Certificates

Feature	Description
MobiControl Root Certificate	You can export and view the details of the Root Certificate
MobiControl Intermediate CA	You can export and view the details of the MobiControl CA

Certificate Bindings

Feature	Description
Component	The component where the certificate is bound
Certificate	The certificate bound to the selected component

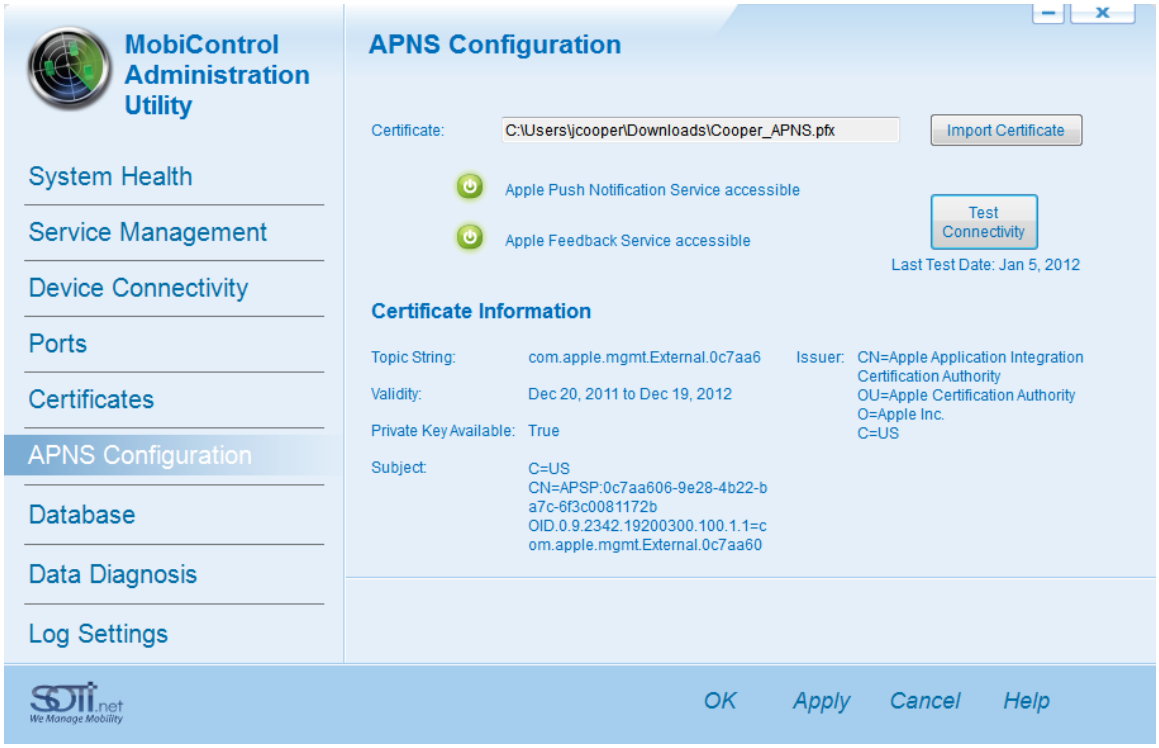
iOS Profile Signing Certificate

Feature	Description
Internal MobiControl Signing Certificate	The default certificate used for enrolling iOS devices

Feature	Description
Custom Certificate	A user specified certificate used for enrolling iOS devices

APNS Configuration

The **APNS (Apple Push Notification Service)** screen provides the MobiControl Administrator the ability to update and change the APNS certificate attached to the deployment as well as view the connection status to Apple's servers.

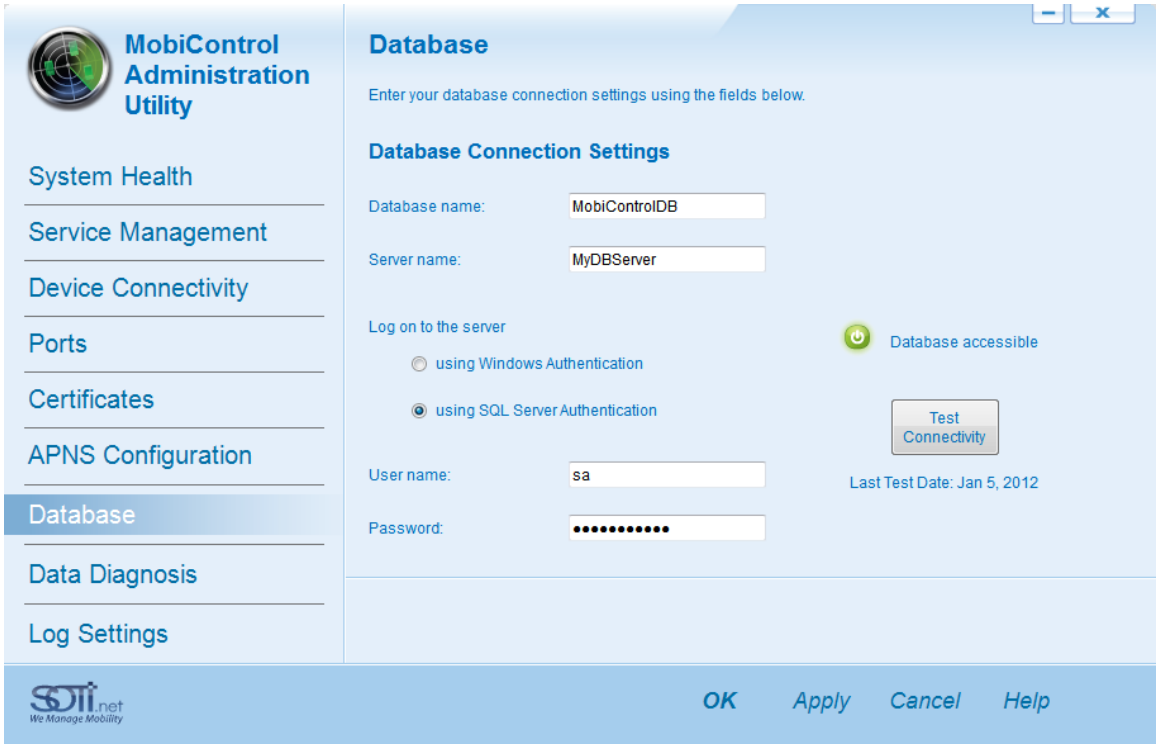


APNS Configuration

Feature	Description
Certificate	Identifies the location of the APNS Certificate
Import Certificate	Allows the MobiControl Administrator to import a new APNS certificate.
Apple Push Notification Service accessible	Identifies if the deployment server can connect to Apple's APNS servers.
Apple Feedback Service accessible	Identifies if the deployment server can connect to Apple's Feedback Service servers.

Database

The **Database** section gives the MobiControl Administrator access to the MobiControl SQL Database Connection.

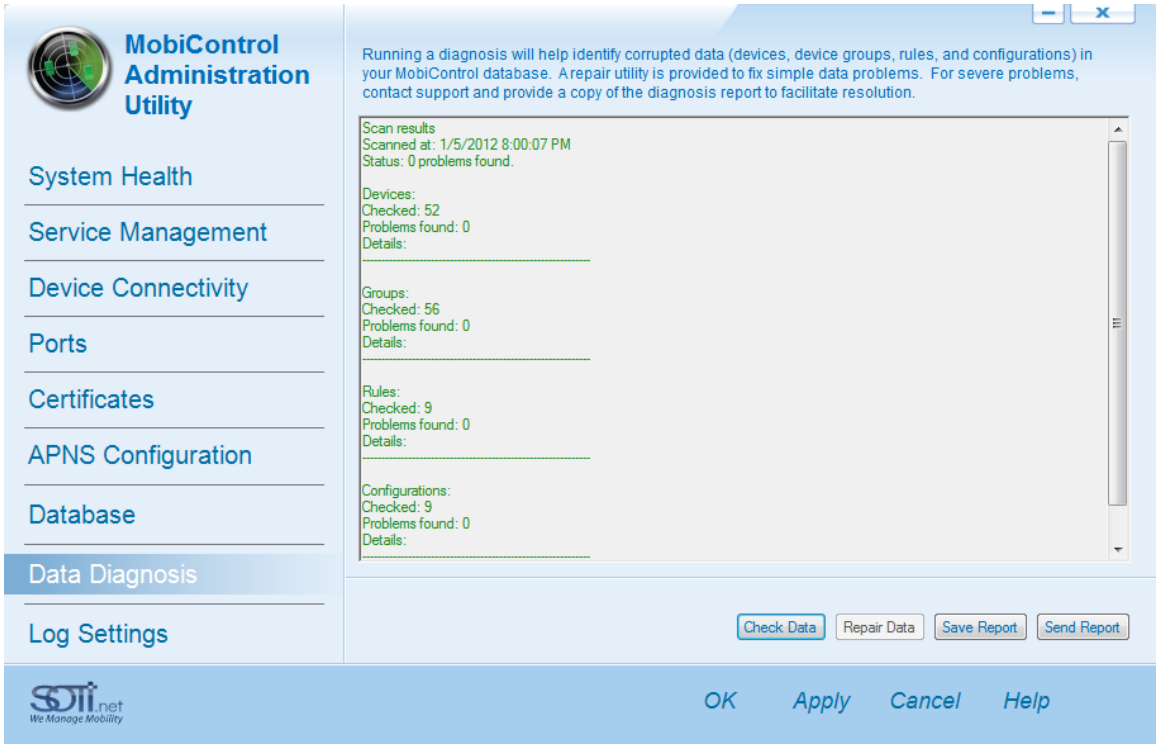


Database

Feature	Description
Database Name	Displays the current database name and provides the MobiControl the ability to change it.
Server Name	Displays the current deployment server name and provides the MobiControl the ability to change it.
Windows Authentication	Specifies the authentication to the deployment server to use Windows NT Authentication.
SQL Server Authentication	Specifies the authentication to the deployment server to use a specific SQL user.
User Name	Specify the name of the SQL use to be used to authenticate to the database.
Password	Specify the password of the SQL use to be used to authenticate to the database.
Database Accessible	Indicates whether or not the SQL database is accessible to the deployment server

Data Diagnosis

Running a diagnosis will help identify corrupted data (Devices, Device Groups, Rules, and Configurations) in the MobiControl Database.



Database Diagnosis

A repair utility is provided to fix simple errors and data problems. For more severe problems, See the"Contact Us" page for Support and provide a copy of the diagnosis report.

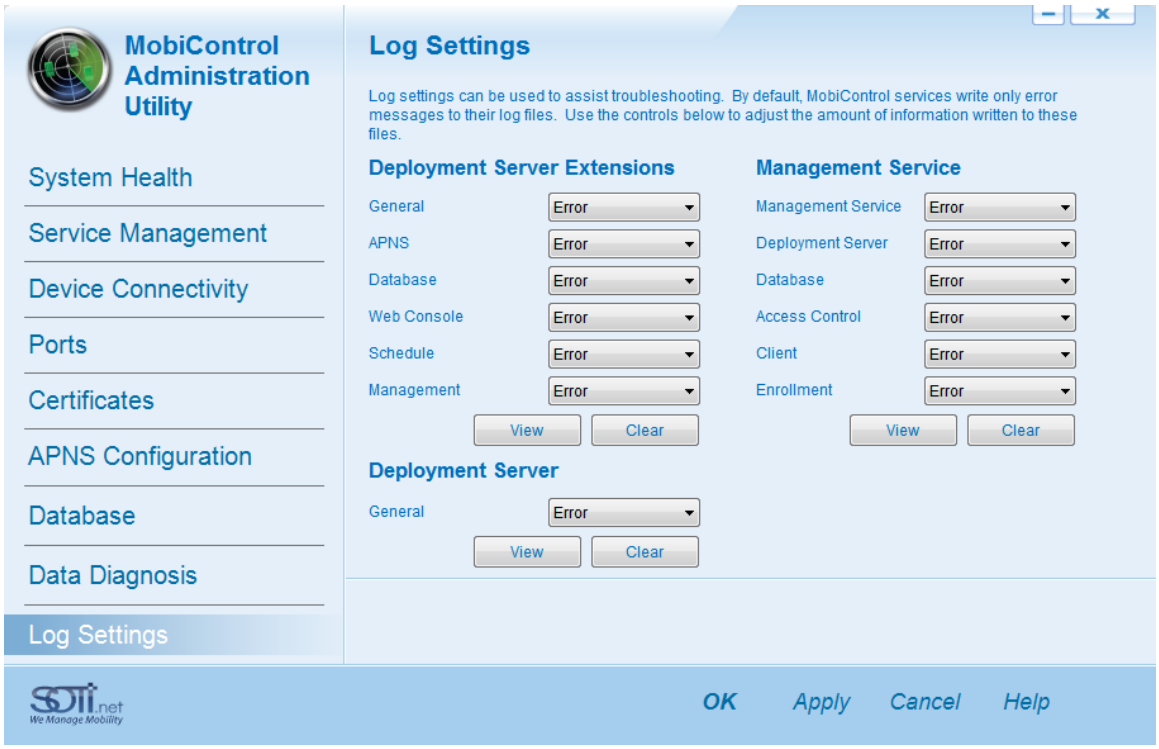
Feature	Description
Check Data	Check your MobiControl Database for errors or corrupted data
Repair Data	Repair simple errors found in your MobiControl Database
Save Report	Save the report to a specific location
Send Report	Send the report to a Technical Support Representative

Log Settings

The **Log Settings** screen allows the MobiControl Administrator to specify the detail of log they wish to collect with each specified function.

The following list contains the different log details:

Detail Type	Description
Off	No logs will be recorded.
Error	Only records errors in the log file.
Warning	Only records warnings in the log file.
Info	Only records information items in the log file.
Verbose	Records everything in the log file. This is also known as Debug Logging.



Log Settings

Area	Item	Description
Deployment Server Extensions	General	Collects information about the deployment server extensions to write to log.
	APNS	Collects information about the Apple Push Notification Service to write to log.
	Database	Collects information about the database to write to log.
	Web Console	Collects information about the web console to write to log.
	Schedule	Collects information about the update schedule to write to log.
	Management	Collects information about the manager to write to log.
Management Service	Management Service	Collects information about the management service to write to log.

Area	Item	Description
	Deployment Server	Collects information about the deployment server connection to write to log.
	Database	Collects information about the database to write to log.
	Access Control	Collects information about console security to write to log.
	Client	Collects information about the Management Console client to write to log.
	Enrolment	Collects information about the enrolment service connection to write to log.
Deployment Server	General	Collects information about the deployment server to write to log.

Feature	Description
View	Allows the MobiControl Administrator to view the log.
Clear	Allows the MobiControl Administrator to clear the log.

Upgrading MobiControl

IMPORTANT: - PLEASE READ BEFORE UPGRADE -

General

- We strongly recommend that all MobiControl (Server and Agent) upgrades are first attempted in a User Acceptance Testing environment prior to upgrading MobiControl in a live environment.
- Upgrade the MobiControl Management Console at all locations then upgrade the devices in batches.
- Please note that ALL components MUST be upgraded at ALL locations for the upgrade to be successful. This must be done before the devices can be upgraded.

Upgrading from v5.03 and below

- If upgrading from MobiControl v5.03 or below, SSL security **MUST** be disabled as Windows CE devices will not update correctly.

Upgrading from v8.51 or below

- If you have upgraded from MobiControl v8.51 or below, you will notice the Windows Desktop devices no longer appear in the Management Console. Like iOS and Android devices, they are now strictly available in the web console.
- If you have upgraded from MobiControl v8.51 or below the and you have manually installed the Windows Desktop Lockdown Utility via a package, it must be Uninstalled from the devices prior to upgrading. Once upgrade is complete you can enable the Windows Desktop Lockdown via the MobiControl Web Console.

Upgrading from v8.51 with Android devices

- To ensure that your Android Devices are upgraded correctly to the newest version of MobiControl you must first uninstall the agents from every Android Device. After uninstalling the agent, download and install the newest agent (either from Google Play, your OEM Marketplace or the Android Add Device Rule). After installing the agent, re-enroll the devices to MobiControl. If you do not re-enroll your devices, they will appear with a red explanation point and you will not be able to enable the agent upgrade.
- Since the Administrator password was not implemented before v9.02, the Authentication Policy will become disabled. Please see the "Android Authentication" topic on page 1142 for more information on how to set up an administrator password. An administrator password is needed to enable the device lockdown.

Upgrading to v9.03

- If you are upgrading to MobiControl v9.03, please ensure that Active Directory security is turned off from the Web Console before proceeding with the update.

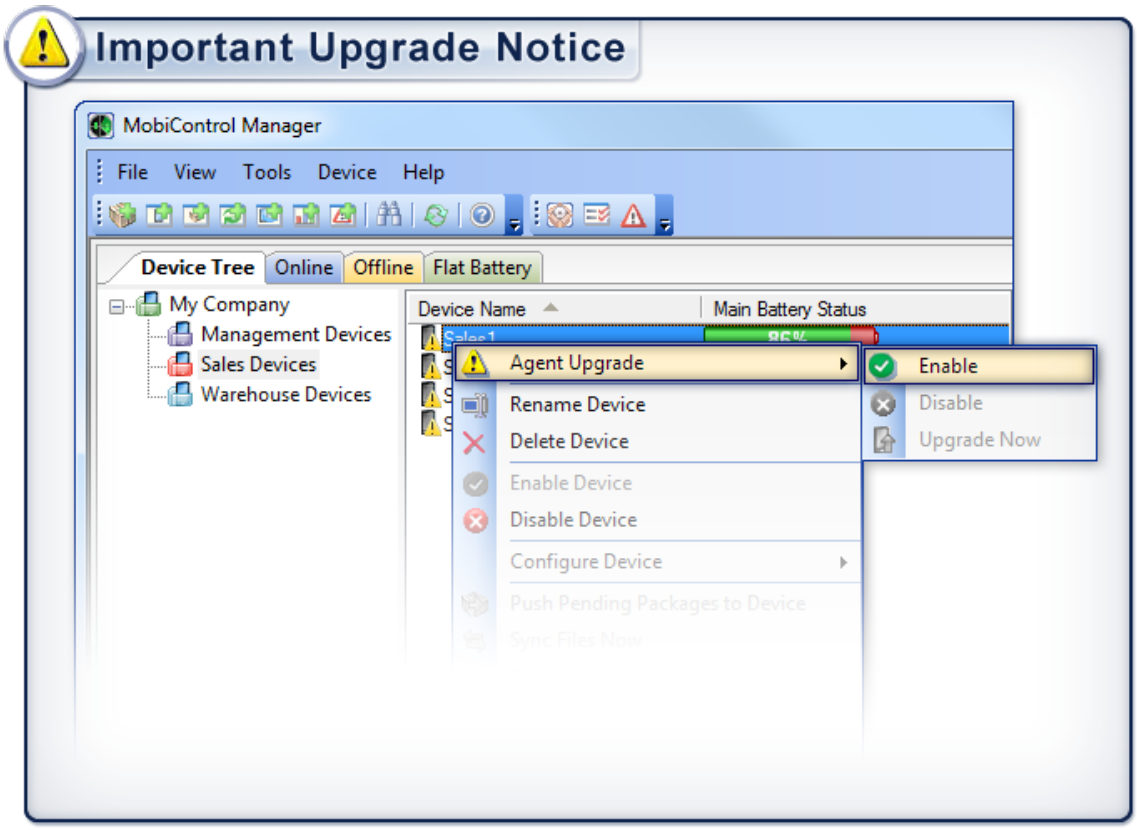
Upgrading to v10

- Please ensure that if you are using Active Directory credentials for the web console, to turn it off. After upgrading, you may re-enable it.

The following steps outline the procedures for upgrading an existing MobiControl installation. Please read all of these instructions before proceeding.

Once the Manager and Deployment Server software has been upgraded, the devices will appear in the Manager console with a warning sign. This is an indication that Agent Upgrade must be enabled in order for the automatic upgrade of the Device Agent to proceed.

For example, if after enabling a few test devices for which problems are found with the agent, the upgrade can be "rolled back" and the majority of devices will avoid the failed upgrade.



1. Back up MobiControl file store.

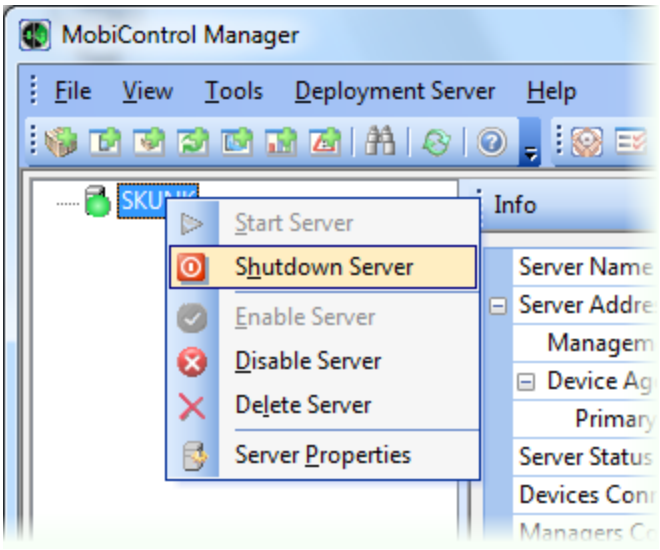
   This is only applicable to MobiControl versions 2.06 and earlier. To back up your file store, use the Microsoft File Explorer to copy the contents of the file store to a backup folder.

2. Back up the MobiControl database.

   This step is optional, since the MobiControl Setup Wizard will automatically back up your database. However, as an extra precautionary measure, you may back it up independently.

   If you are running the full Microsoft SQL Server, you can backup your database using the Backup tool provided with Microsoft SQL Server Enterprise Manager. Optionally, you may use a third-party back-up utility.

3. Close all MobiControl Manager windows and shut down all MobiControl Deployment Servers.



NOTE:

It is recommended to test the upgrade procedure in a staging environment using a copy of the production database.

4. Run the updated Setup program.

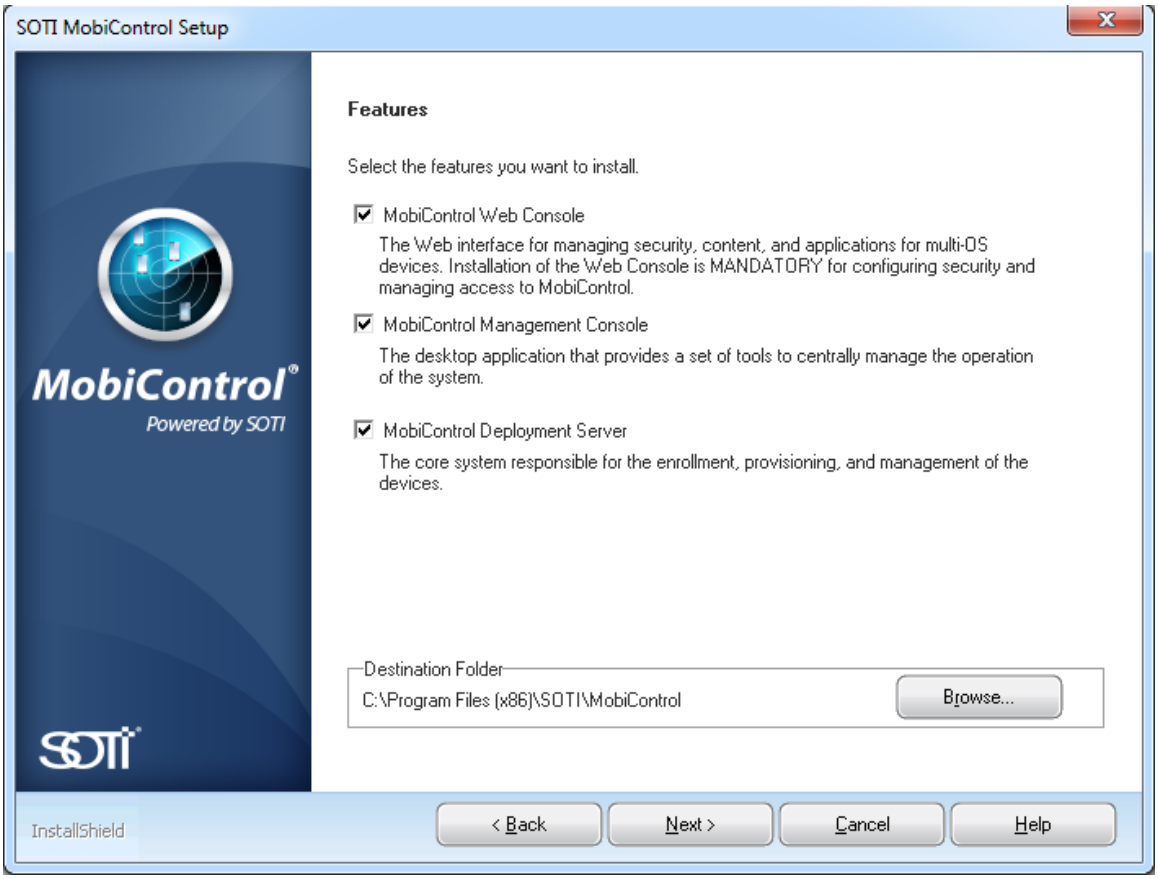
   Select the features that wish to be updated. Having the MobiControl Web Console selected, will install all device tabs.

   NOTE:

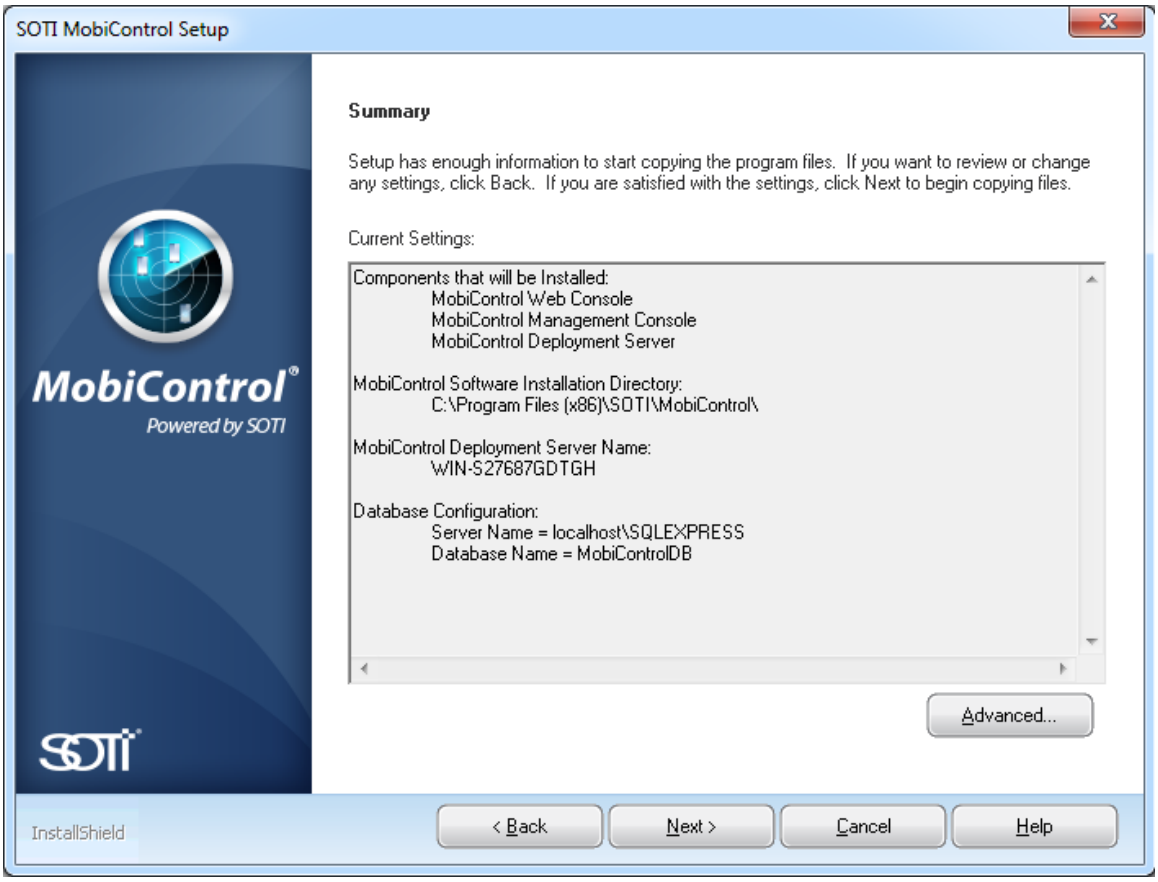
   Previous versions of MobiControl allowed us to specifically define which tabs get installed. If you wish to only have specific tabs shown, please contact us.

   If a feature was installed previous, and becomes unselected, the installer will remove that feature.

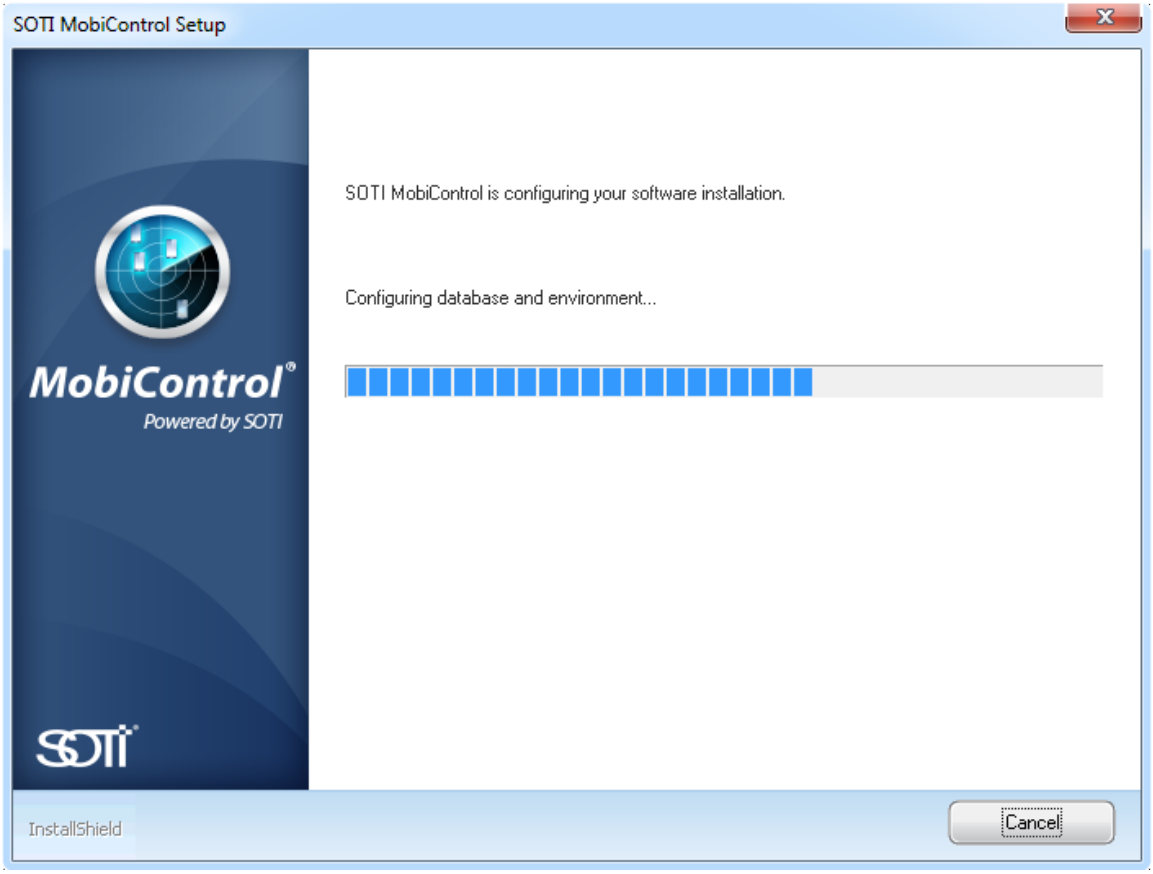
   Click **next**.



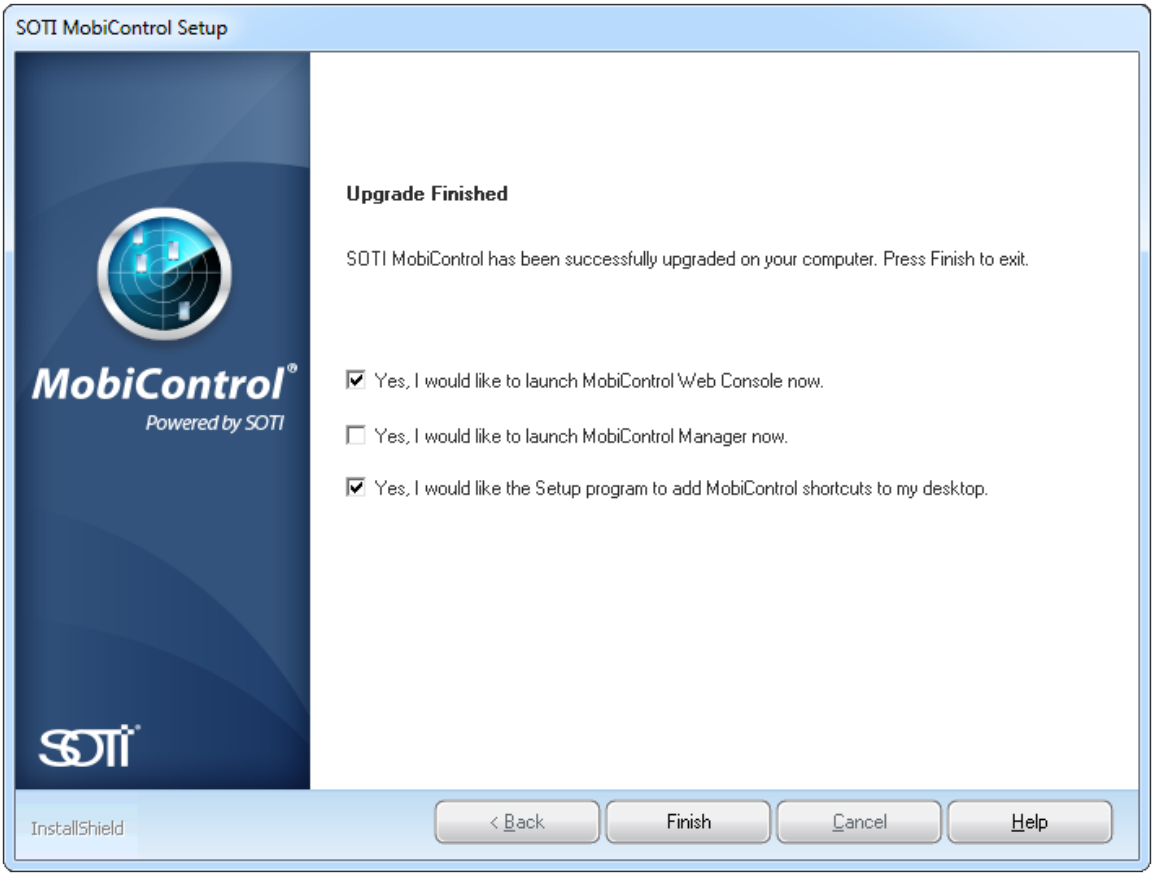
The next dialog will show a summary of the upgrade. The installer will automatically detect the database settings. Click **next** once everything is confirmed.



The MobiControl installer will automatically backup, and upgrade the database and MobiControl at this point.


SOTI MobiControl Setup
MobiControl®
Powered by SOTI
SOTI MobiControl is configuring your software installation.
Configuring database and environment...
InstallShield
Cancel

5. Complete the Installation.



Repeat step 4 on each computer that has MobiControl Manager, Package Studio or a Deployment Server installed.

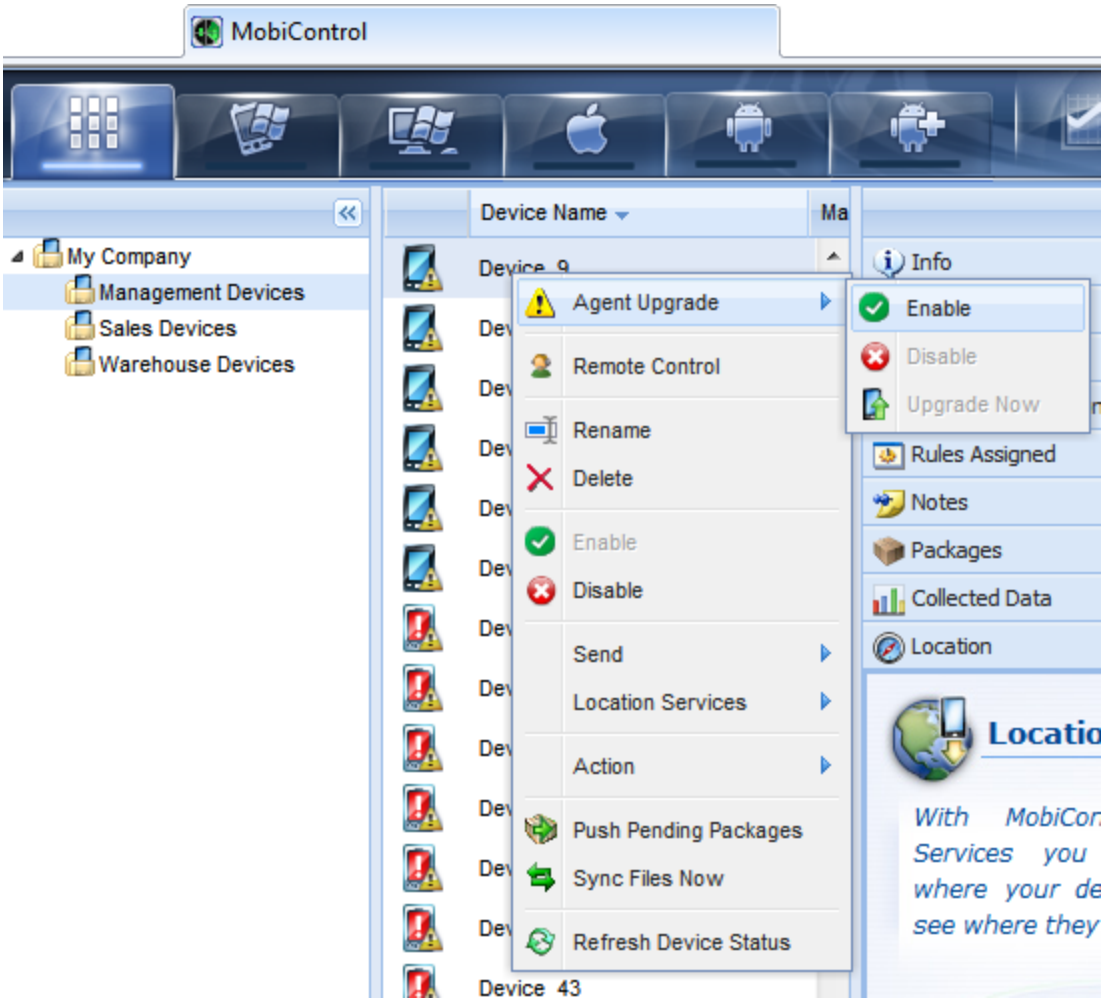
IMPORTANT:

At this point, all the devices in the device tree will appear with a warning sign. This is an indication that agent upgrade must be enabled in order for the automatic upgrade of the Device Agent devices to proceed. Automatic upgrade is not enabled by default so that agent upgrade can be performed gradually. This allows you to upgrade a controlled set of devices and verify the new agent performs well before upgrading the agents of all your devices.

For example, if after enabling for a few test devices, problems are detected with the new agent, the upgrade can be rolled back, and the majority of the devices will avoid the failed upgrade.

6. Enable upgrade for one device.

   Right-click on a device, select **Agent Upgrade,** and click **Enable.** If the device is already online, select **Upgrade Now.** If the device is not yet online, there is no need to select **Upgrade Now,** as the new agent will be automatically delivered upon connection to the Deployment Server when upgrade is enabled.

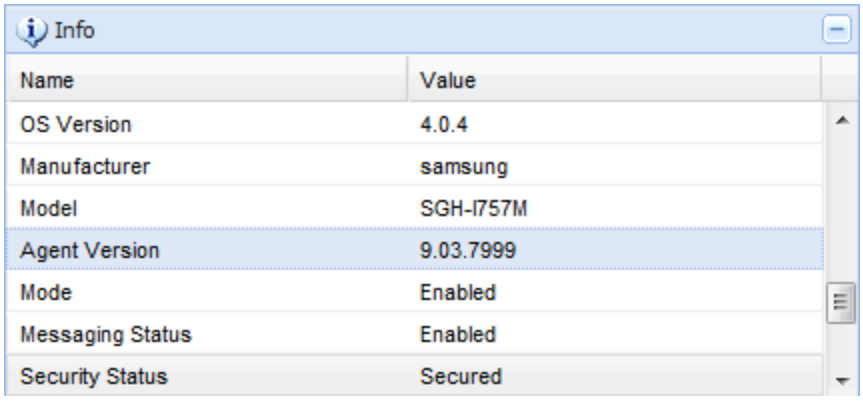


NOTE:

As part of the upgrade process, the device will disconnect from the MobiControl server and go into the offline state. The upgrade will proceed on the device while it is disconnected, and then upon completion it will automatically re-connect and return to the online state. When the device goes offline, the warning sign will re-appear on the device icon in the device tree. This is normal, and done intentionally to prevent the device from repeating its attempt to upgrade if the upgrade process fails on the device. When the upgrade is successful, the warning sign will automatically disappear when the device returns online.

5. Verify the build number.

When the device returns online, verify the build number by selecting the device and looking at the Info panel. If there is any conflict with the version you have installed (compare to the version information in the Manager's about window), and the version currently on the device, or if there are any error messages in the log panel, please contact us.



6. Verify communication with the selected device.

   Try remote controlling it. Verify the MobiControl configuration by checking for installed packages, file sync rules, lockdown, etc. If you are unable to connect to the device or experience any issues, please contact us.

7. Gradually enable upgrade for all devices.

   Enable one group at a time in the device tree, and verify the devices in each group have been updated successfully.

   The device menu option **Agent Upgrade** will automatically disappear once all devices have been upgraded. In the event problems are detected during upgrade, select **Agent Upgrade** and click **Disable** to prevent the upgrade from taking place on devices for which upgrade has been enabled, but has not yet taken place. If the upgrade does not complete successfully after one attempt (three attempts in Windows Mobile 5 and above) the upgrade agent will disable itself and you will have to enable it again to continue the upgrade process.

   If you experience any difficulties or unexpected behavior, contact us.

Uninstalling MobiControl

MobiControl Manager

To uninstall the MobiControl Manager from a workstation, double-click the **Add/Remove Programs** icon in the Control Panel. Select **SOTI MobiControl** from the list, and then click the **Remove** button.

MobiControl Deployment Server

To uninstall the MobiControl Deployment Server from a workstation or server, double-click the **Add/Remove Programs** icon in the Control Panel. Select **SOTI MobiControl** from the list, and then click the **Remove** button.

Microsoft SQL Server 2005 or SQL Server 2008 Express Edition

To uninstall the Microsoft SQL Server from a workstation or server, double-click the **Add/Remove Programs** icon in Control Panel. Select **Microsoft SQL Server** from the list, and then select the **Remove** button.

NOTE:

Database files will not be automatically deleted. You must manually delete the files using the File Explorer. If you installed MSDE with MobiControl, these files are stored in `C:\Program Files\SOTI\MobiControl\MSSQL`.

MobiControl Device Agent

Windows Mobile

To uninstall the MobiControl Device Agent from a Windows Mobile device, double-click the **Remove Programs** icon on the **System Settings** tab. Select **SOTI MobiControl** from the list, and then click the **Remove** button.

NOTE:

The uninstaller for the agent does not remove all installed files from the device. This is to ensure the device can be easily re-introduced to the MobiControl system when installing a new version of MobiControl. In order to completely remove the MobiControl Agent from the device, you must delete the files and folders listed below. It is then recommended to soft-reset the device to verify the uninstallation completed successfully.

In the persistent storage folder (set during install time), remove the file `pdb.ini`, and the folder `PdbPkg`.
In the root directory of the device, remove the files `PkInst.log`, `PkCtrlSv.log`, and the folder `PdbInfo`.

iOS Devices

To uninstall the MobiControl Device Agent from iOS devices, press and hold the MobiControl app icon until it shakes. Press the x icon that appears on top of the app.

After you removed the MobiControl app, you should remove any profiles associated with it. To do this, go to the Settings app. Once inside the Settings app, select the General tab. Scroll down to the bottom of the General section and select Profiles. Remove all profiles that are associated with MobiControl.

Android Devices

To remove the MobiControl Device Agent from Android devices (both generic and Android Plus), you must deactivate MobiControl as the device administrator. To do this, go into Settings, Security, then Device Administrators. Once in the Device Administrators section, select MobiControl and deactivate it.

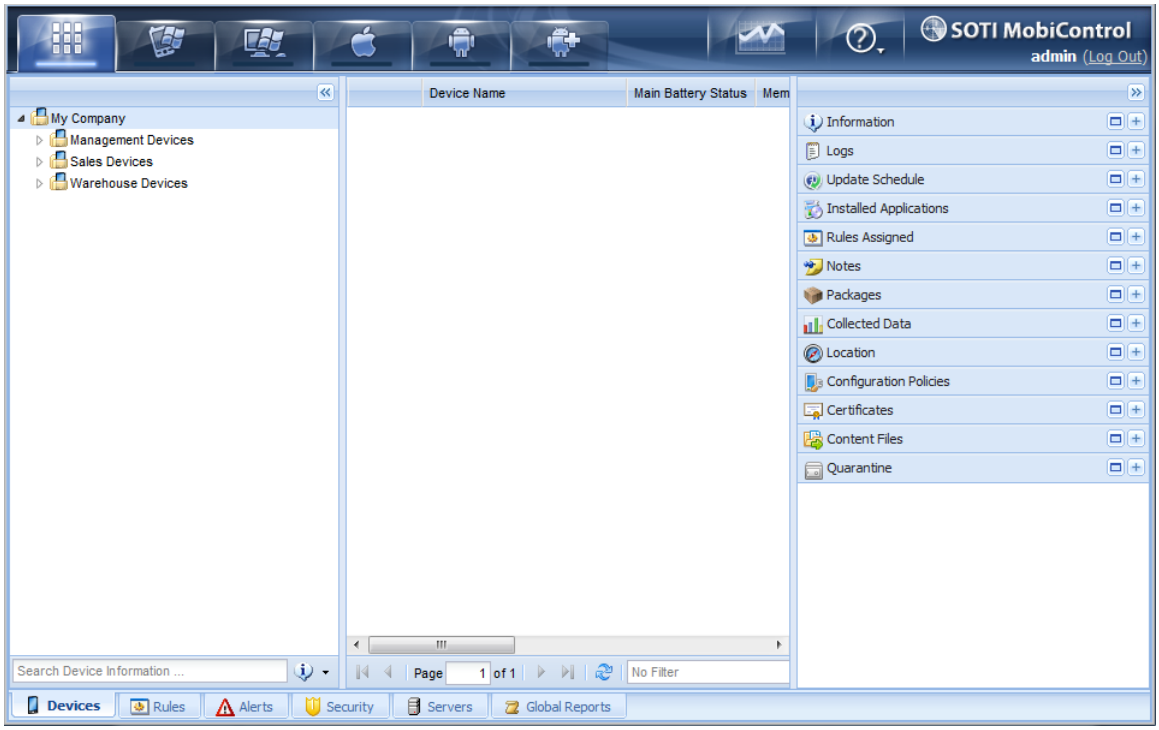
After you deactivated MobiControl, you can then remove the MobiControl app as a regular Android app.

MobiControl Web Console

The MobiControl Web Console allows you to provide Management Console access to your mobile support team using a thin management console available anywhere where Internet Explorer is installed.

The Web Console is an online Management Console providing you with the ability to support your mobile devices from anywhere in the world. You can do everything from locate your devices to remote control, and even send scripts.

The MobiControl Web Console is installed to https://localhost/MobiControl



From the MobiControl Web Console you can:

- Remote Control/View
- Send Scripts and Messages
- Locate and Track Devices
- View Logs, Device Info, Packages, Assigned Rules and Installed Programs
- Make Notes
- View Deployment Server Information
- Generate Reports

NOTE:

Web Remote Control uses Microsoft ActiveX Controls, if you are unable to remote control a device, please make sure this feature is not specifically denied within your Internet Explorer settings.

Device Status Icon

The MobiControl Web Console allows you to identify the different devices and their states via the device icon. The table below references the different icons and their states

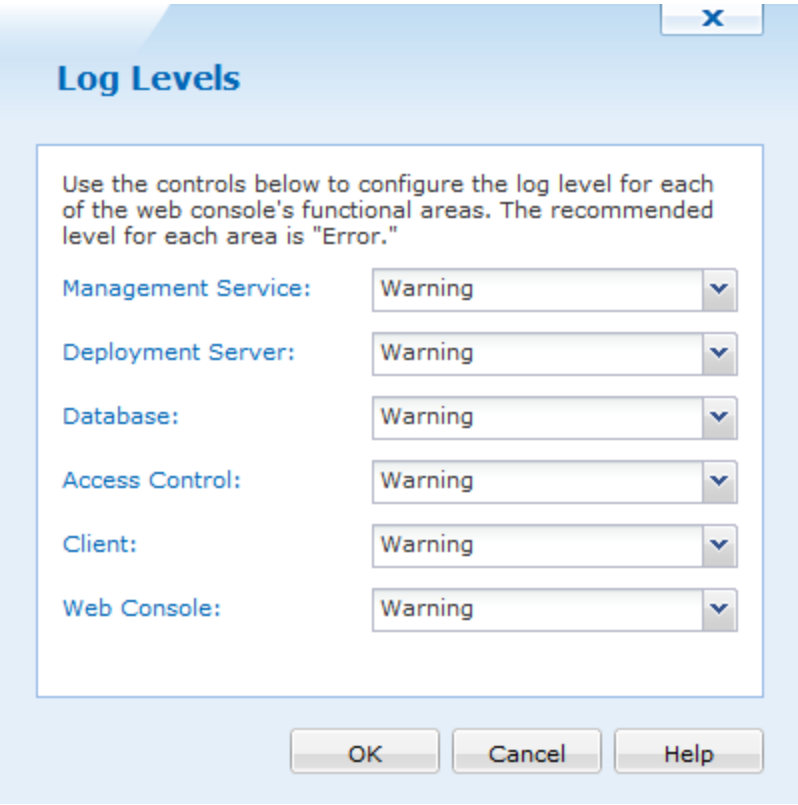
Device	Description	Icon
Windows CE / Windows Mobile device	Online	
	Offline	
	Learning	
Windows Desktop device	Online	
	Offline	
Apple iOS	Online	
	Offline	
	No Device Agent	
	Error - Profiles not installed	
Google Android	Online	
	Offline	
	Error - No Administrator rights	

Logging

The web console has the ability to set logging levels and to view the log file generated.

Log Levels

To set the log levels, click the question mark on the top right hand corner, and select **Log Levels**. The logging levels can be set for the Management Service, Deployment Server, Database, access control, client or Web Console. These files are stored on the computer where these services are installed on.



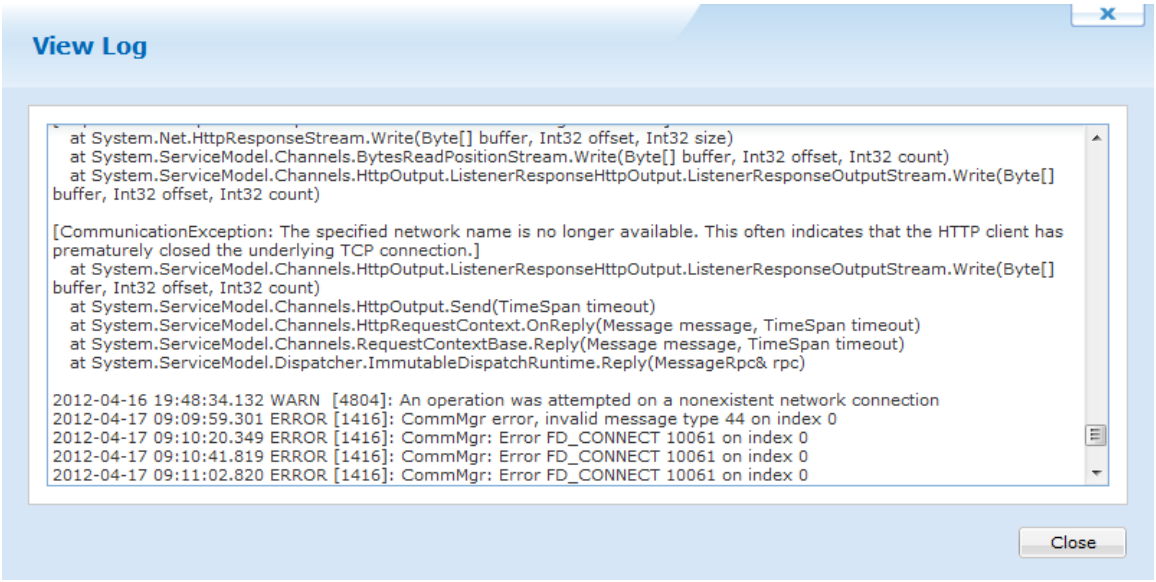
MobiControl Log Levels

Log Level	Description
Off	Setting the log level to Off turns off any logging for the associated section.
Error	Setting the log level to Error allows only error messages to be written to the log file
Warning	Setting the log level to Warning allows only warning messages to be written to the log file
Information	Setting the log level to Information allows only

Log Level	Description
	information messages to be written to the log file
Verbose	The Verbose setting enables Error, Warning and Information to be written to the log file at the same time.

View Log File

To view the log file in the Web Console, click the question mark on the top right hand corner, and select **View Log Levels.**



MobiControl log file

All Devices Tab

The Devices view (tab) is the main view into the status of the devices in the MobiControl system.

Device Tree

The device tree provides a structured view of the devices in the system. The group structure is easily defined by the user by creating new groups and dragging and dropping devices between groups. Please see the "Device Groups" topic on page 124 for detailed information on groups and virtual groups.

Commonly-reported device information can be easily referenced in the device tree window by right-clicking in any open space in the device tree window and selecting the information that you would like to see displayed.

Devices are added to the system by defining an add device rule and creating a MobiControl Device Agent that is installed on the device. Please see the "Adding Windows Mobile Devices" topic on page 747 for a detailed explanation of how to add devices to MobiControl.

Info Panel

The Info panel provides detailed status information about the group or device that is selected in the device tree. When a group is selected, the displayed information includes the number of subgroups and how many unique, online, offline, or disabled devices are in the group. For devices, the displayed information includes device ID, IP address, battery and memory status. In addition, custom data retrieved from your devices may also be displayed. Please see the "Windows Mobile Custom Data" topic on page 700 for detailed information about configuring custom data retrieval.

The content displayed in this panel is stored in the MobiControl database. This information is refreshed when a device establishes a new connection to the MobiControl Deployment Server, and when you click **Refresh** or press F5 on this tab.

Logs Panel

The Logs panel provides a listing of the events occurring in the MobiControl system. This listing is filtered based on the group or device that is selected in the device tree. If only one device is selected, only the events related to that device are displayed. If a group is selected, events for the group and all the devices that belong to that group are displayed.

You have the option to show or hide logging, adjust the maximum number of logs displayed, and the frequency with which the Manager should refresh the log view.

Update Schedule Panel

The Update Schedule panel lists the dates and times when the device is programmed to query the MobiControl system to check for updates. By default, a device will also check for updates whenever it connects to the MobiControl system. Please see the "Windows Mobile Device Update Schedule" topic on page 722 for more information.

Installed Applications Panel

The Programs panel lists the applications that are installed on the device that is selected in the device tree.

Rules Assigned Panel

The Rules Assigned panel lists the deployment and file sync rules assigned to the group or device that is selected in the device tree. Rules are inherited from parent groups; a rule will apply to a device if it belongs to group to which the rule has been assigned.

The assignment of rules to groups provides a flexible and convenient means for easily configuring devices. For example, once you have set up your rules for software or data distribution, you can automatically provision your devices by simply adding them to the appropriate group within the device tree. Please see the "Web Rules Tab" topic on page 575 for information on creating deployment rules and file sync rules.

Notes Panel

The Notes panel lists the notes that are associated with the selected device. If a group is selected in the device tree, all the notes for the devices that belong to the group are listed. Notes are a convenient way to maintain information about the device such as trouble tickets. Please see the "Device Notes" topic on page 1384 for information on creating device notes.

Packages Panel

The Packages panel lists the packages that are configured on the device that is selected in the device tree. The assignment of packages is directly based on the assigned rules. This panel provides a status column which indicates the state of the package for that device. For example, the status "Pending" indicates that the package has been queued and its installation on the device is pending.

You can force the re-installation of a package on a given device by right-clicking on the package in the Package Panel and selecting **Force Package Reinstall on Next Schedule** or **Force Package Reinstall Now.**

Collected Data Panel

The Data Collection Panel allows you to view the collected historical data for a set of devices. By creating a Data Collection Rule you will be able to specify which items to collect data from, how often to collect them, and when to upload the collected data to the server. Please see the Creating Data Collection Rules page for information on creating Data Collection.

Location Panel

The Location Panel gives the ability to locate, track and gather information on the movement of your GPS enabled devices, no matter where they are in the world which is powered by Microsoft's Bing maps technology. Whether you need to confirm the current location of a particular field-worker, track the progress of an important shipment or collect historical information on the movement of a group of devices or vehicles in order to analyze performance, MobiControl's Location Services can help. Please see the Location Services page for more information.

Configuration Policies Panel

The Configuration Policies panel lists all policies that are currently configured on the device. It also lists where these policies are inherited from. This allows us to have a quick look to see what configurations are currently on devices.

Certificates Panel

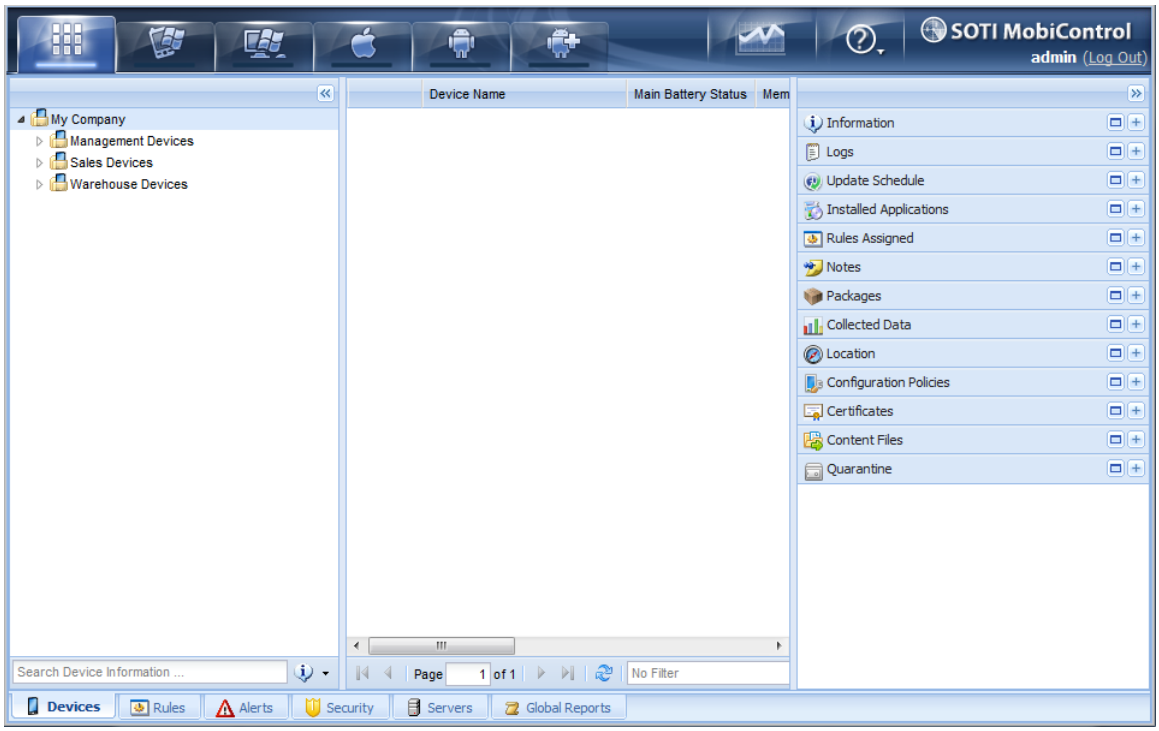
The Certificates Panel lists all certificates that MobiControl sent to devices. Certificates can range from email to WiFi authentication.

Content Files Panel

The Content Files panel lists all files that devices are currently able to access. The panel will also list if a file has been downloaded or pushed to the device. This panel is only available for iOS and Android devices.

Quarantine Panel

The Quarantine Panel will list all applications and files that the MobiControl Antivirus policy found. This allows us to quickly see how many applications or files have been detected. The Quarantine Panel is only available for Android devices.



MobiControl Devices Tab Devices view (tab)

Virtual Device Group

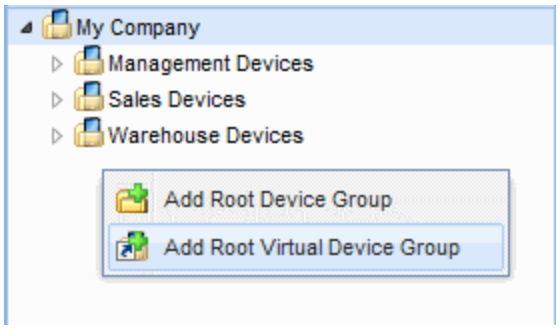
A virtual group is a special type of group that allows you to assign deployment rules or file sync rules to a set of devices, even though the devices may actually belong to different groups in the device tree. This is useful in cases where you want a sub-set of devices to be configured with rules that are typically only assigned to mutually exclusive groups.

Devices are placed into a virtual group by dragging and dropping them into the virtual group. MobiControl automatically creates a shortcut in the virtual group for the device(s). You can easily remove a device from a virtual group by deleting the devices entry in the virtual group. This will not remove the actual device from the MobiControlsystem. It will only remove the shortcut.

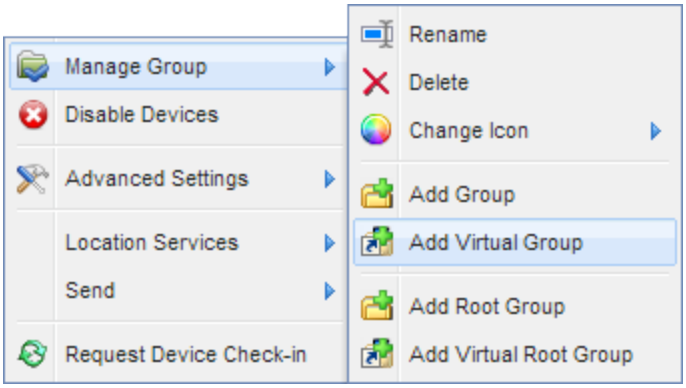
One of the key differences between a regular group and a virtual group is that device configuration settings (remote control settings, update schedule, lockdown and Deployment Server priority) can only be specified for a regular group. The ability to locate or track devices with Location Services at the group level is not available for virtual groups.

Virtual Group Editor

To add a Virtual group in MobiControl, make sure that you are in the Devices view (tab). While in the Devices view (tab) right click any white space in the device group view. You can add a virtual group in either the root of the device tree or under a device group.



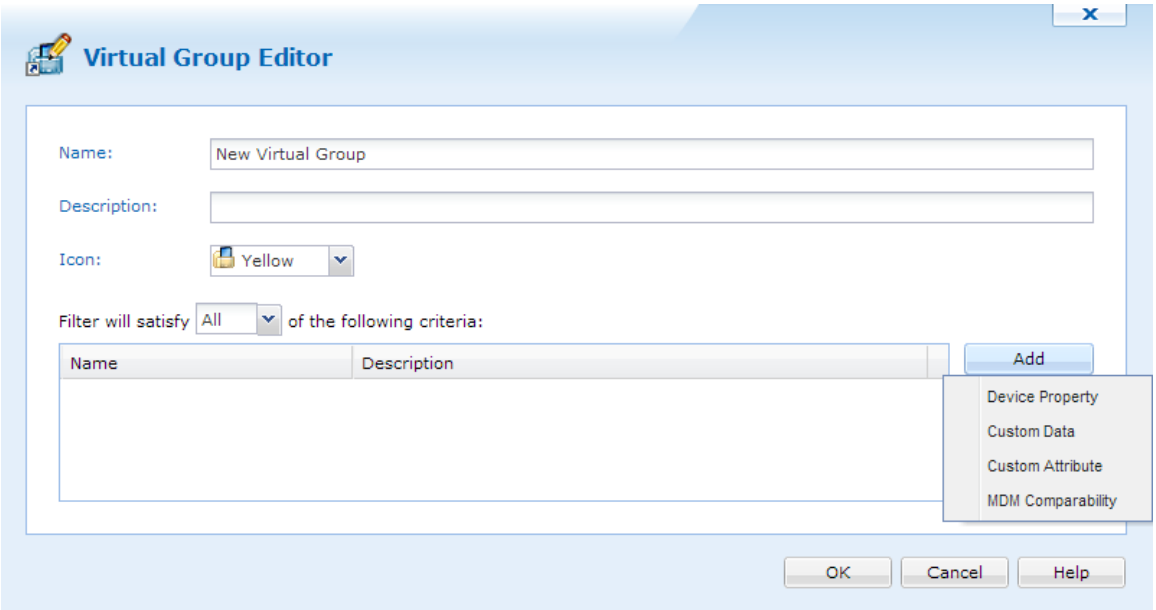
Adding a Virtual Device Group to the root of the Device Tree



Adding a Virtual Device Group to a device group

When you add a Virtual group the Virtual groupEditor appears. Within the Virtual group you are able to name the Virtual group, add a description and change the icon of the folder.

You are also able to create filters that automatically create shortcuts to devices that meet the criteria. Below shows the Virtual groupEditor:



The Virtual Group Editor

NOTE:

When you create a filter in a Virtual Device group, you are not allowed to manually move devices in or out from the group because this is done automatically. You can only move devices to and from Virtual Device groups if no filter is created.

Filter Entry Editor

The Filter Entry Editor allows you to create specific criteria that automatically moves provisioned devices into the Virtual group. There are 4 types of filters that you are able to configure: Device Property, Custom Data, Custom Attribute and MDM Comparability.

Clicking each of the filters adds an entry to the Virtual Group editor.

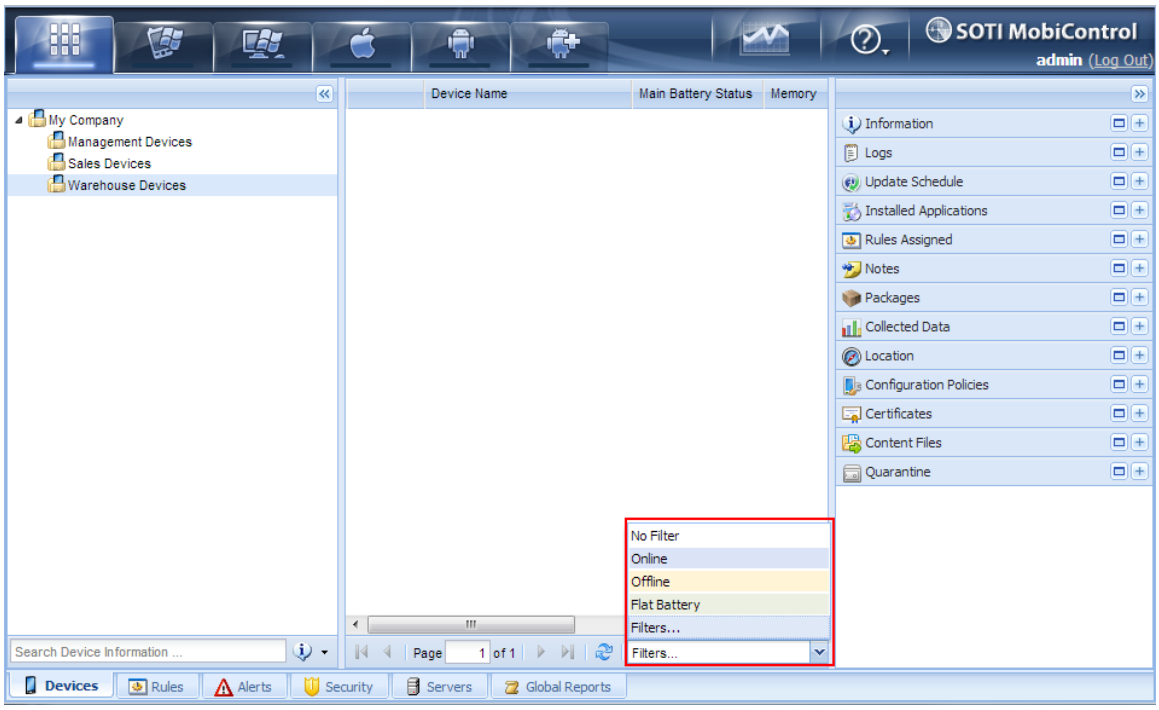
Filter	Description
Device Property	The device property filter lists all available properties that devices report to MobiControl. These include agent version, last connection time and many others.
Custom Data	The custom data filter lists available custom data fields that have been created for devices. This is only available for Windows Mobile, Windows Desktop and Android devices.
Custom Attribute	The custom attribute filter lists the available custom attributes that have been created. Please see the "Custom Attributes" topic on page 1343 for more information.
MDM Comparability	The MDM comparability filter will allow us to

Filter	Description
	filter devices based on their MDM version. This is only available for Android devices, regular Android devices will always have the generic MDM version.

Filter Manager

The MobiControl web console allows us to filter which devices you see on each Device Tab. This allows us to quickly see devices that fulfil the filter criteria.

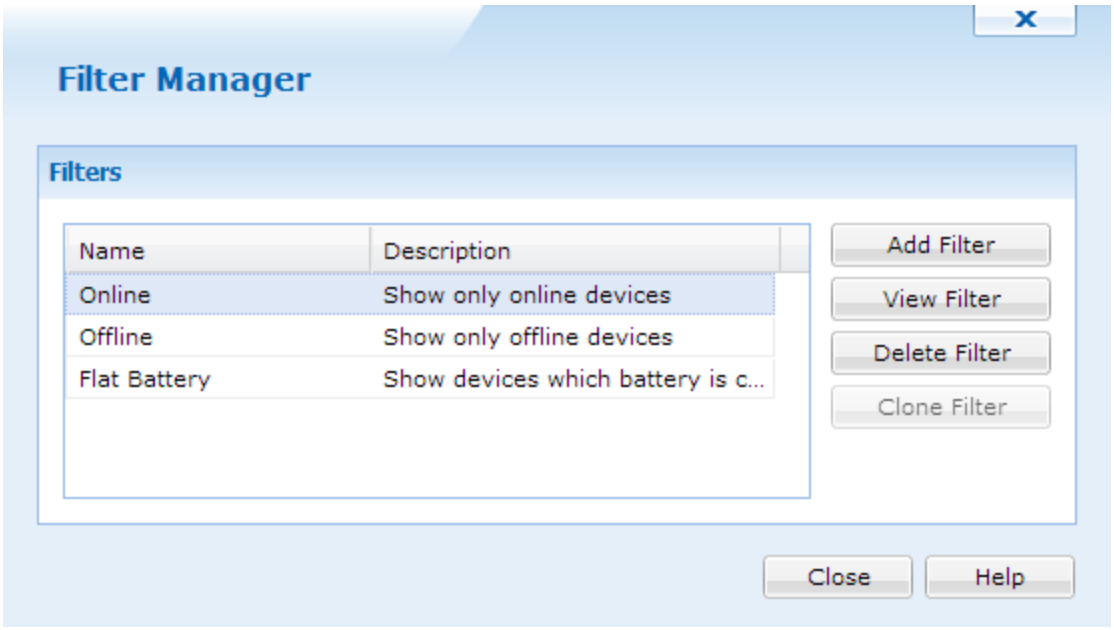
Default filters include, devices that are online, offline and devices that have a flat battery. Clicking **Filters...** will allow us to create custom filters based off device properties, custom data, custom attributes, or MDM comparability.



MobiControlWeb Console Filter

Filter Manager

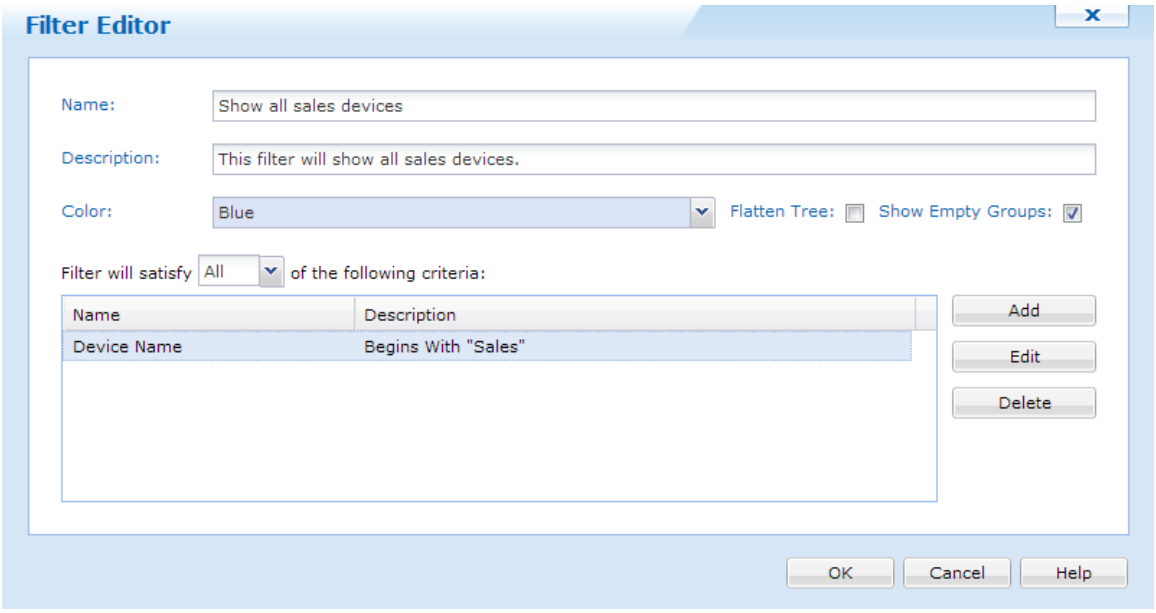
When we select the **Filters...** option it brings up the Filter Manager. Here we are able to create a new filter, edit a previously created filter, delete and clone a filter.



Filter manager

Add Filter

The add filter option allows us to create a new filter based on criteria we set. In the filter editor we are able to set the name, the description and the color of what the web console will look like.



New Filter Creation

Field	Description
Name	The name of this filter
Description	The description that will be given to the filter
Color	The background color of the web console when this filter is selected.
Flatten Tree	Selecting this will show all devices in the web console without having to go through each of the groups.
Show Empty groups	This will show groups that contain no devices.

Edit Filter

The Filter Manager also has an option to view or edit a filter. The three default filters; Online, Offline, Flat Battery, can only be viewed. For any other created filters you are allowed to edit them.

Delete Filter

You are also able to delete filters that you have created in the Filter Manager. Please note, once you have deleted a filter there is no way to retrieve it back. The only way to get it back is to recreate it from scratch.

Clone Filter

The Clone Filter button allows you to copy a filter that you have created. Note that you cannot clone any of the default filters.

When you Clone a filter, all settings will be copied and the name will be different. This feature is useful for when you want to add additional filters to a previously created Filter, without losing the original one.

Filter Entry Editor

The Filter Entry Editor allows you to create specific criteria that automatically moves provisioned devices into the Virtual group. There are 4 types of filters that you are able to configure: Device Property, Custom Data, Custom Attribute and MDM Comparability.

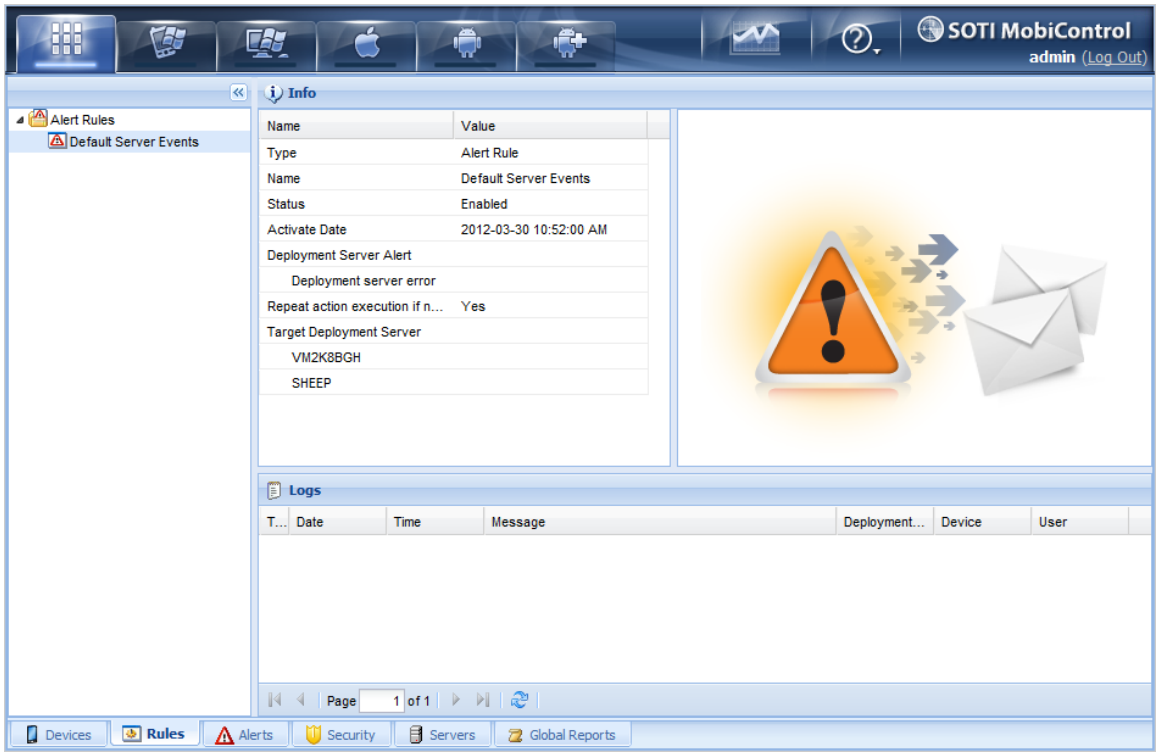
Clicking each of the filters adds an entry to the Virtual Group editor.

Filter	Description
Device Property	The device property filter lists all available properties that devices report to MobiControl. These include agent version, last connection time and many others.
Custom Data	The custom data filter lists available custom data fields that have been created for devices. This is only available for Windows Mobile, Windows Desktop and Android devices.
Custom Attribute	The custom attribute filter lists the available custom attributes that have been created. Please see the "Custom Attributes" topic on page 1343 for more information.
MDM Comparability	The MDM comparability filter will allow us to filter devices based on their MDM version. This is only available for Android devices,

Filter	Description
	regular Android devices will always have the generic MDM version.

All Devices Rules Tab

MobiControl uses rules to simplify the tasks of device management and configuration. See Below for a description of each rule available on the All Devices Rule Tab.



MobiControl Rules Tab

Alert Rules

1. Create an Alert Rule

   An Alert Rule allows Administrators and Users to be notified when events of interest arise on the system. Please see the "Windows Mobile Alerts" topic below for detailed information about creating an Alert Rule.

2. Check the Alert Rule execution status.

   Once the Alert Rule has been created, you may want to run a report to see what alerts have been generated. You can do this by looking at the Alert Rule Summary report in the Reports view (tab). Please see the "Generate Reports" topic on page 623 for more detail about reports.

Alert Rules

Alert Rules allow Administrators to be notified when events of interest arise on the system. This notification system allows Administrators to quickly and effortlessly communicate an event message to large groups of people via email, and notifies users via the MobiControl Manager Alert tab. For every type of scenario, whether it is a Rule Change or a Device Error, the system will rapidly deliver your message to a designated audience.

NOTE:

The Deployment Server must be online in order for Alerts to be generated and sent out.

The MobiControl Web Console allows you to create Alerts based on the Devices Operating System (OS). Some Alerts are specific to the OS Tab that has been selected . For detailed information on the Alerts Available please see below.

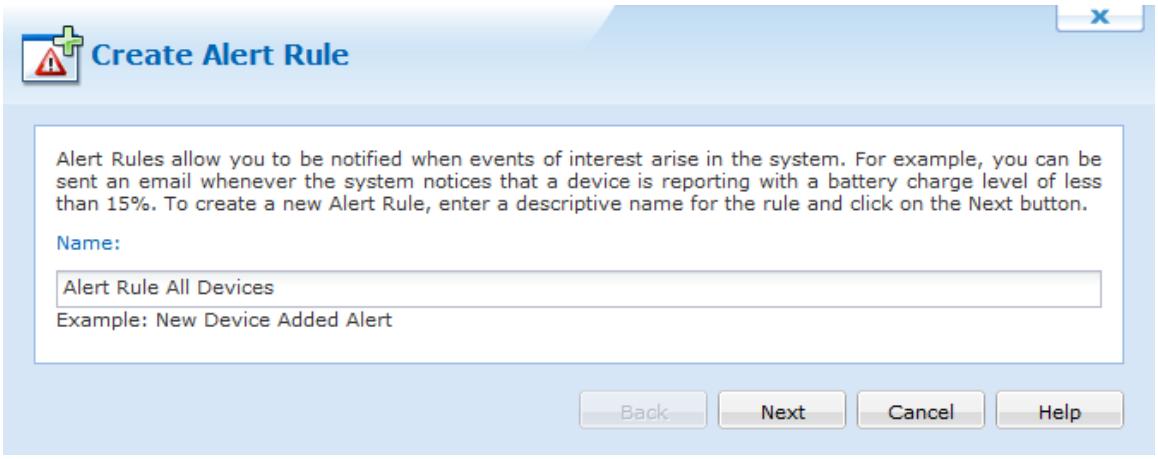
Type	Description
Deployment Server Event	Trigger alerts based on an assortment of Deployment Server events.
System Event	Trigger alerts based on an assortment of system events.

The steps below describe how the Create Alert Rule Wizard can be used to create an Alert using the MobiControl Web Console:

Start the wizard.

Select the All OS's Tab, then select the Rules tab, then Right click on the **Alert Rule** folder, and select **Create Alert Rule**. The first page of the Create Alert Rule Wizard will be displayed.

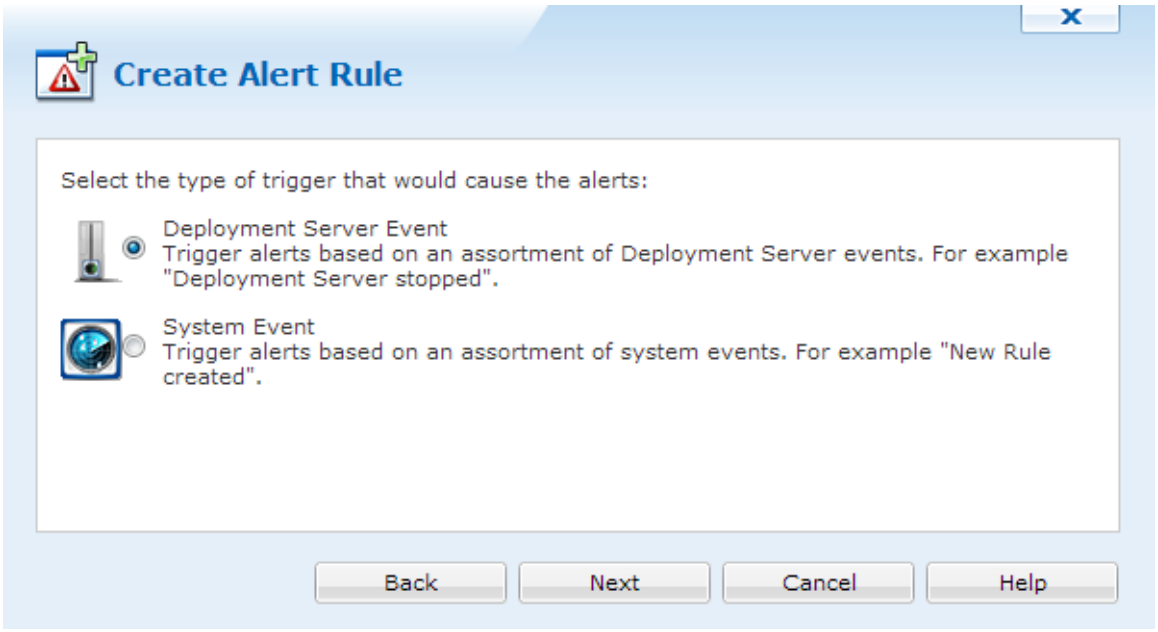
Enter a descriptive name for the Alert Rule you are creating and click **Next.**



First page of the Alert Rule Wizard

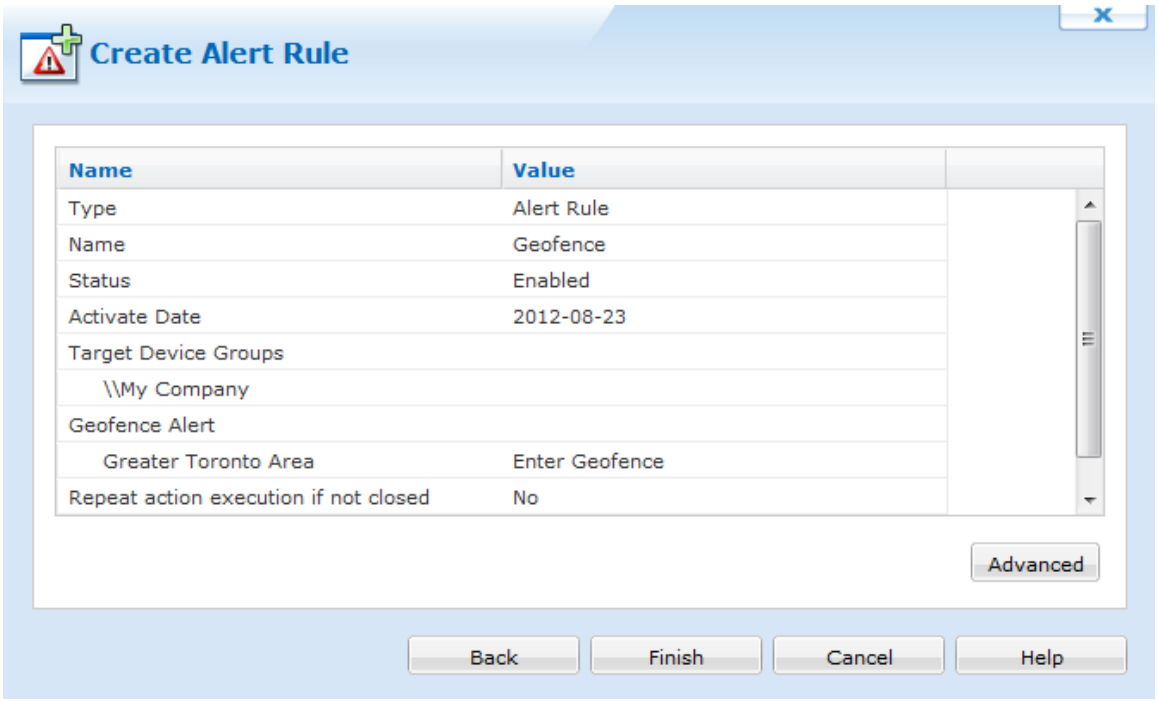
1.

2. Select the Alert Rule Type.



Select the Alert Rule Type and click Next. After Clicking Next you will be asked to specify the Alert Options for the selected Alert Type. Select the type of alert below for more information on the Alert Options available.

Review the summarized information.



3. Click **Finish** to complete the wizard.

SMTP Notification Profile

When you configure an alert, you have the ability to get notified by sending an email to a user or users indicating the particular event. A **Notification Profile** allows you to configure the sending email server settings as well as the contents of the message.

From the Manage Profiles dialog, you have the ability to select an existing profile, create a new profile, edit or delete an already existing profile.

If no email notification profile exists, you'll need to specify a Profile Name, the SMTP Host, Port, and give the option of different levels of Authentication within the Create Notification Profile dialog. You have the option of having an Anonymous, basic, or NTLM authentication and the ability to enable the use of SSL.

The Sender dialog allows you to specify details of the email address that will be sending the notification. You must also specify a name for that sender which gets displayed in the From field. Optionally, you have the ability to setup a Priority for the email where the available options are Low, Medium and High.

Select the Recipients that should be notified when the particular alert event is triggered. When you click the Add button, you have the ability to setup recipients that would be in the To field, CC field and BCC field as well.

The **Message** dialog allows you to specify both the Subject and the Message. Variables can be added to both the Subject and the Message as shown in the screen shot above. The entire list of variables that can be used are described below:

The Schedule dialog allows you to specify when the alerts will be fired and sent to the recipients.

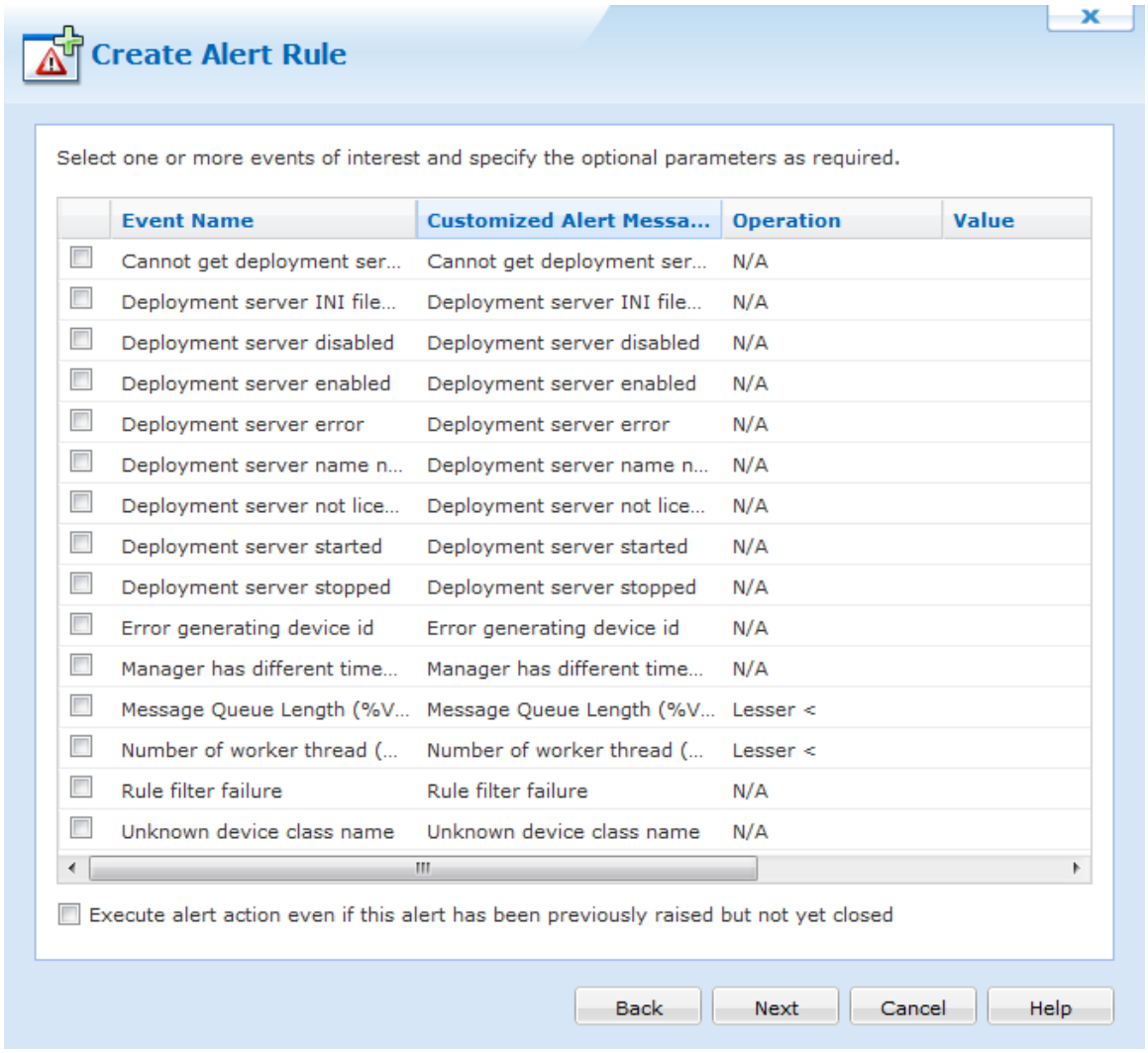
Variable	Description
%%ALERT%	Displays the Alert name that was specified when the alert was created.
%SOURCE%	Display the Deployment Server name in the case it is a Deployment Server alert. Displays the "MobiControl System" in case it is a System alert. Displays the Device name in case it is a Custom Data alert. Displays the Device name in case it is a Device alert. Displays the Device name in case it is a Geofence alert.
%LOCATION%	Displays the Deployment Server name in the case it is a Deployment Server alert. Displays the "MobiControl System" in case it is a System alert. Displays the location in case it is a Custom Data alert. Displays the location in case it is a Device alert. Displays the location in case it is a Geofence alert.
%DATE%	Displays the date the alert was generated.
%TIME%	Displays the time the alert was generated.

The Create Notification Profile - Summary Information page summarizes the settings configured on the previous pages of the wizard. If you are satisfied with the configured settings, click on the Finish button to create the Create Notification Profile, otherwise use the Back button to go to previous screens and make adjustments. The Test button will send a test email to the recipients to ensure the settings are correct.

After completing the Notification Profile Wizard, click Finish and continue the Alert Rule Wizard here.

Deployment Server Event

A Deployment Server Event is an alert trigger based on an assortment of Deployment Server Events. See below for a full list.



Deployment Server Event Notification Selection Window

The Operation and Value fields allows to filter out Alerts based on specific values or value ranges. The Operation field specifies at which point an alert will be created for the data value you have specified. Severity is set to Minor by default and can be altered.

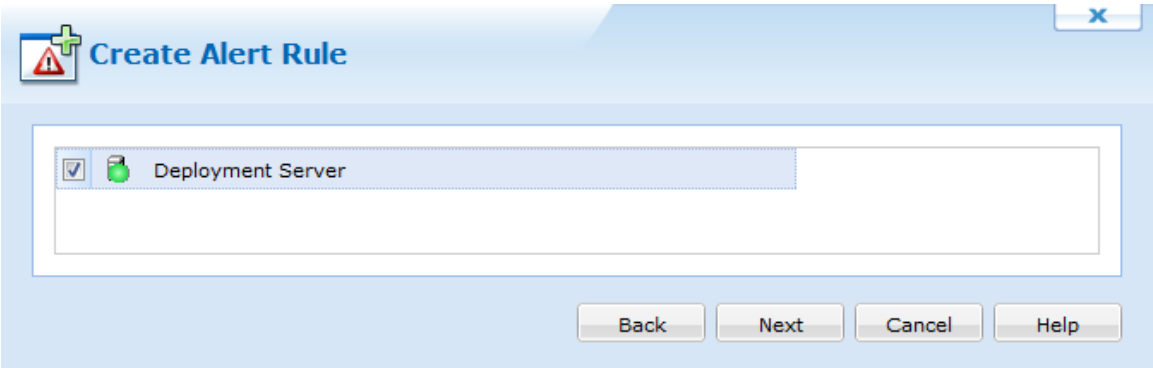
The below table shows all available default Deployment Server events:

Log Event	**Description**
Cannot get Deployment Server IP Address	Cannot get Deployment Server IP Address
Deployment server started	Deployment server started
Deployment server stopped	Deployment server stopped
Deployment server disabled	Deployment server disabled
Deployment server enabled	Deployment server enabled

Log Event	Description
Deployment server not licensed	Deployment server not licensed
Deployment server INI file not found	Deployment server INI file not found
Deployment server name not defined	Deployment server name not defined
Cannot get deployment server IP address	Cannot get deployment server IP address
Error generating device id	Error generating device id
Deployment server error	Deployment server error
Manager has different time with deployment server	Manager has different time with deployment server
Unknown device class name	Unknown device class name
Message Queue Length	Message Queue Length
Number of worker threads	Number of worker threads
Rule Filter failure	Rule Filter failure

Select Deployment Server.

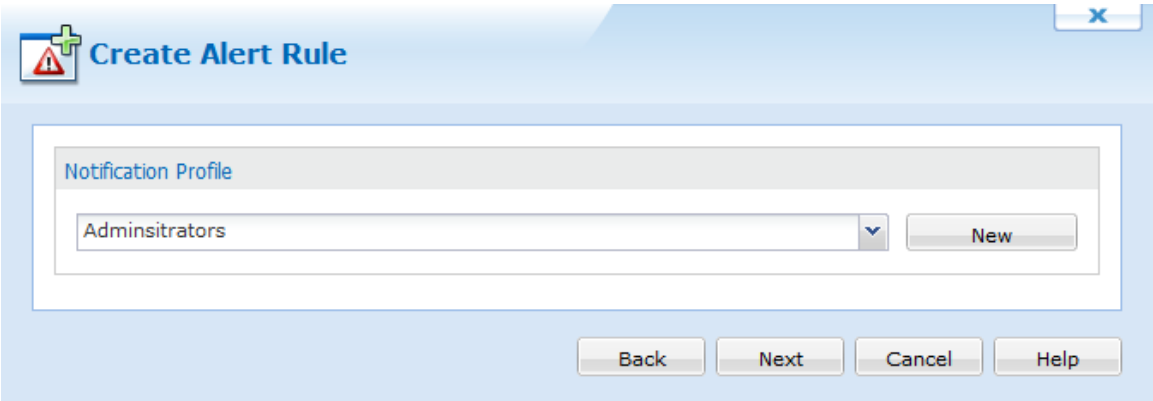
Select the Deployment Server(s) to which the rule will be applied. Once you have completed this section, click the **Next** button.



After selecting your target Deployment Server(s), click Next

Notification Profile Settings

Once the Alert Rule is selected, you must select your Notification Profile.



Select an existing notification profile, or click New to create a new Notification Profile. For assistance with notification profiles click here. Once you have selected your notification profile click Next.

Click next to continue the Alert Rule Wizard here.

System Event

A System Event is an alert triggered based on an assortment of system events. See below for a full list.

System Event Notification Selection Window

Severity is set to Minor by default and can be altered.
The below table shows all available default System events:

Log Event	Alert Message (Customisable)
Site name changed	Site name changed
Log was truncated automatically by the Deployment Server	Log was truncated automatically by the Deployment Server
Manager has different time with deployment server	Manager has different time with deployment server
Log was truncated manually by the user	Log was truncated manually by the user
Database was shrunk	Database was shrunk
Number of configured device has reach licensed number	Number of configured device has reach licensed number
Invalid device site name	Invalid device site name
Error starting communications engine	Error starting communications engine
Attempting to upgrade database	Attempting to upgrade database

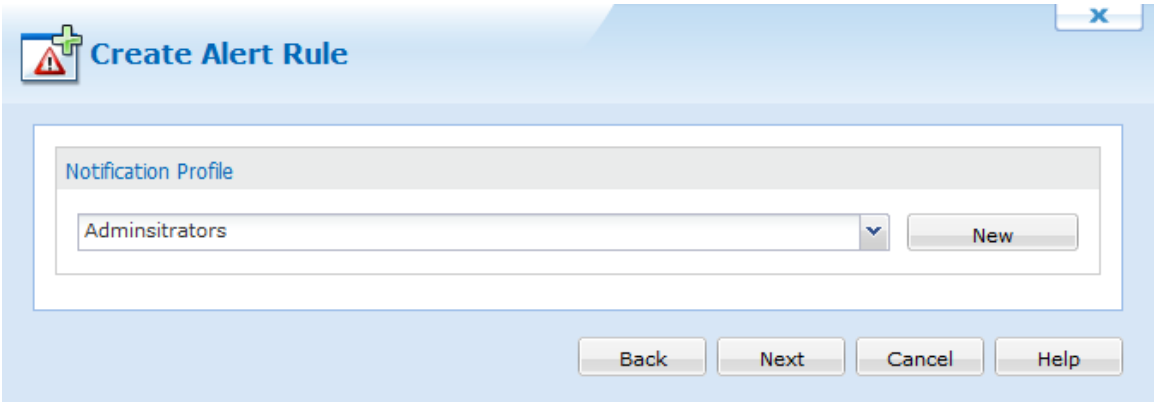
Log Event	Alert Message (Customisable)
Database upgrade completed	Database upgrade completed
Error finding rule	Error finding rule
Error adding device	Error adding device
General system error	General system error
Communication error	Communication error
Rule Created	Rule '%RULENAME%' Created
Rule Enabled	Rule '%RULENAME%' Enabled
Rule Disabled	Rule '%RULENAME%' Disabled
Rule Renamed	Rule '%RULENAME%' Renamed
Rule Changed	Rule '%RULENAME%' Changed
Rule Deleted	Rule '%RULENAME%' Deleted

The following list of variables are only available within the Customized Alert Message field:

Type	Description
%RULENAME%	The name of the rule
%PACKAGENAME%	The name of the package

Notification Profile Settings

Once the Alert Rule is selected, you must select your Notification Profile.

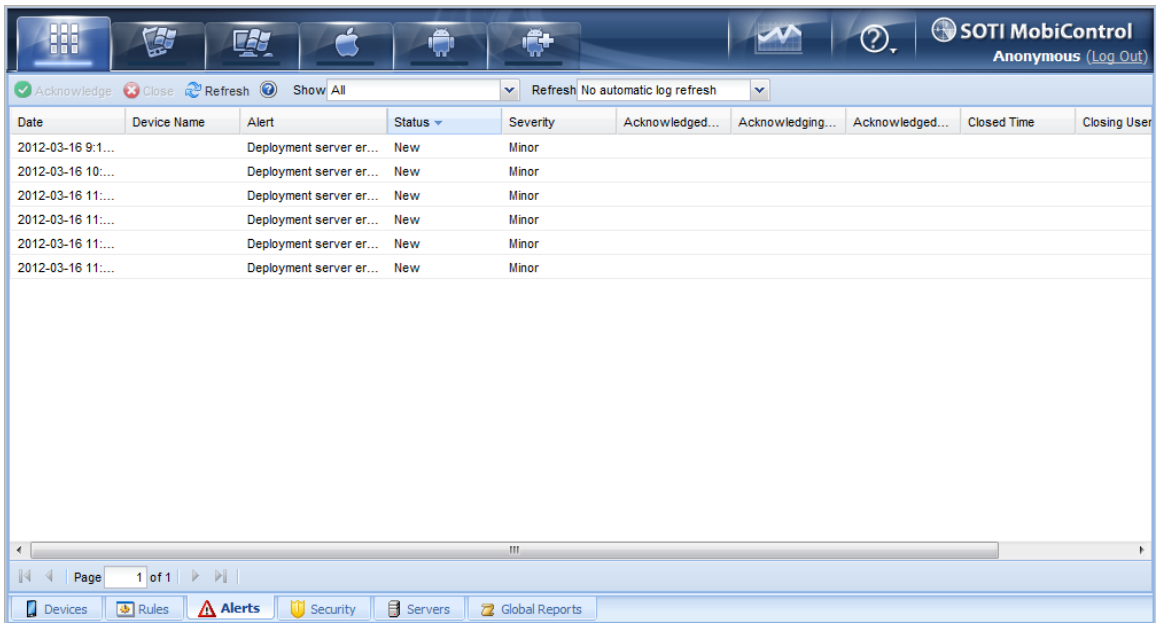


Select an existing notification profile, or click New to create a new Notification Profile. For assistance with notification profiles click here. Once you have selected your notification profile click Next.

Click Next and continue the Alert Rule Wizard here.

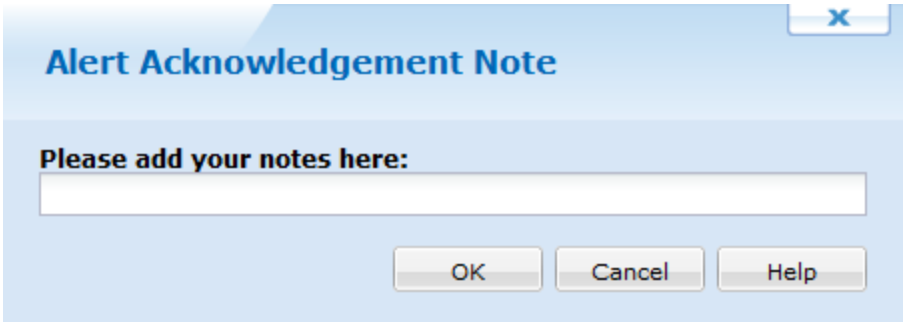
Alert Manager Tab

Once you have successfully created an Alert Rule the MobiControl Manager Alerts Manager window will start populating Alerts that have been generated by the rules created.

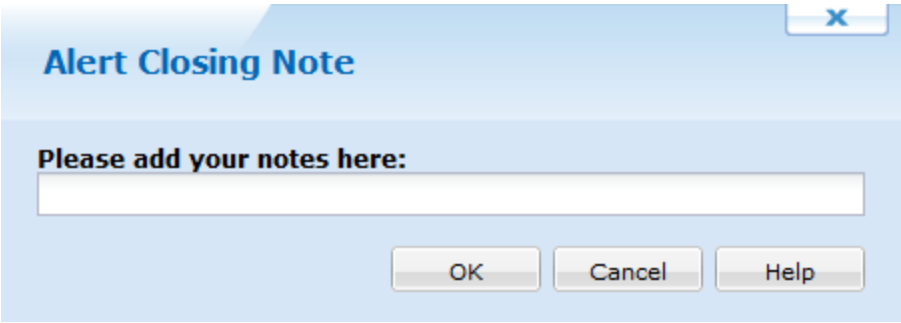


The Alerts Manager window will show information regarding your alerts. Alerts can be Acknowledged here by selecting the alert and clicking Acknowledge. Also Alerts can be closed from this window.

To Acknowledge an Alert or Close an Alert, right click on the Alert in the list and select Close or Acknowledge. Alternatively you can select the Alert and click the Close or Acknowledge button. When Closing or Acknowledging an Alert you can enter a note about the alert. The note is then available in the Alert Manager.



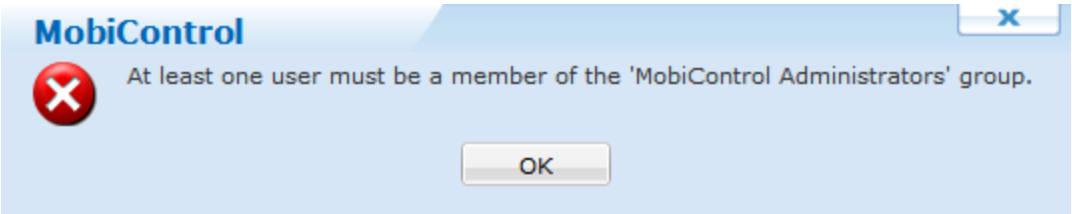
Acknowledge an Alert



Close an Alert

Security Tab

The **Security Tab** gives you the ability to view and edit the applied Console Security Settings, provided your user account has access rights to view this screen. If you have not created a user and added them to the **MobiControl Administrators** group the following error will appear:



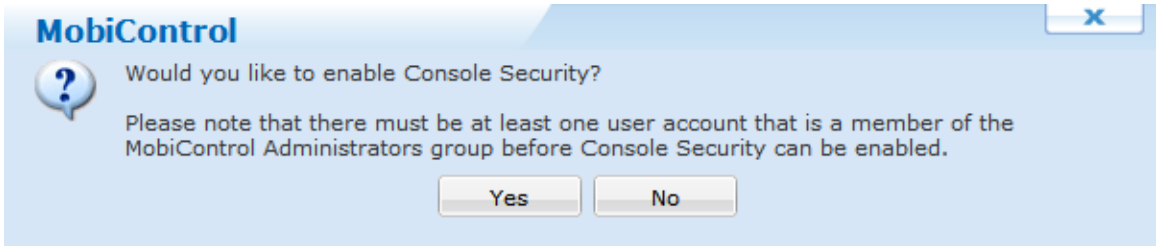
To resolve this issue create a user and add them to the **MobiControl Administrators** group prior to enabling security.

Console Security

The following screen will be displayed if **Console Security** has not been enabled.

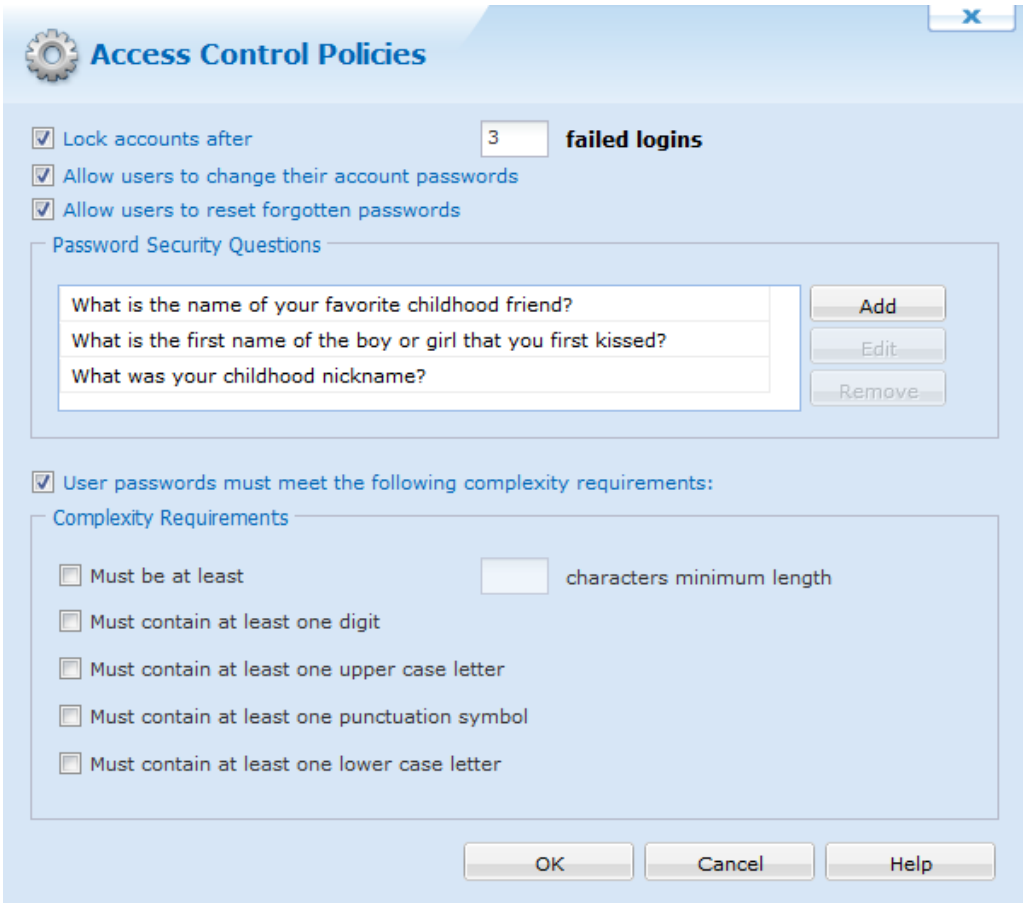
To Enable **Console Security** via the Management Console visit the Manager Console User Security page.

To enable **Console Security** from within the Web Console click the **MobiControl Console Security** button. The following pop up will be displayed



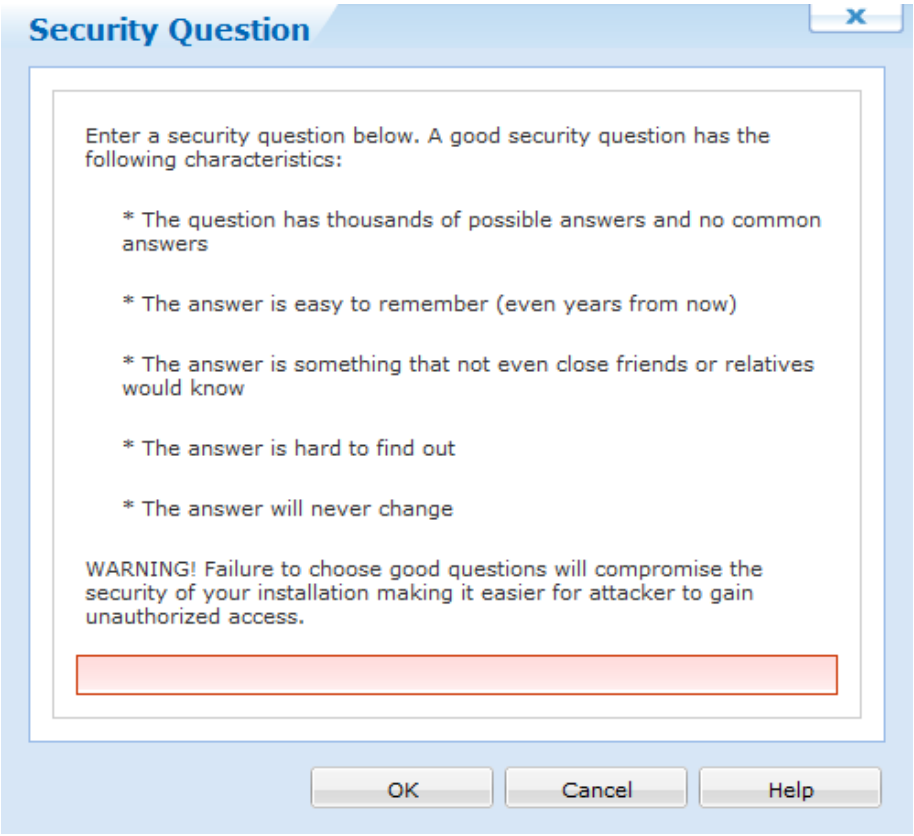
Once **Console Security** has been enabled, the Console Security screen will change to the following:

The Configure MobiControl Access Policy allows you to set complexity requirements and allows you to let users reset forgotten passwords.



Access Control Policies

You can add, edit or remove any of the Password Security Questions that are in this window. To add a new security question, click the **Add** button. A pop up window will appear and give you suggestions to creating a strong security question. The next time a user logs into MobiControl, it will prompt the user to choose 3 questions and provide an answer to each one. If the user cancels this dialog, it will be prompted again the next time the user logs in.



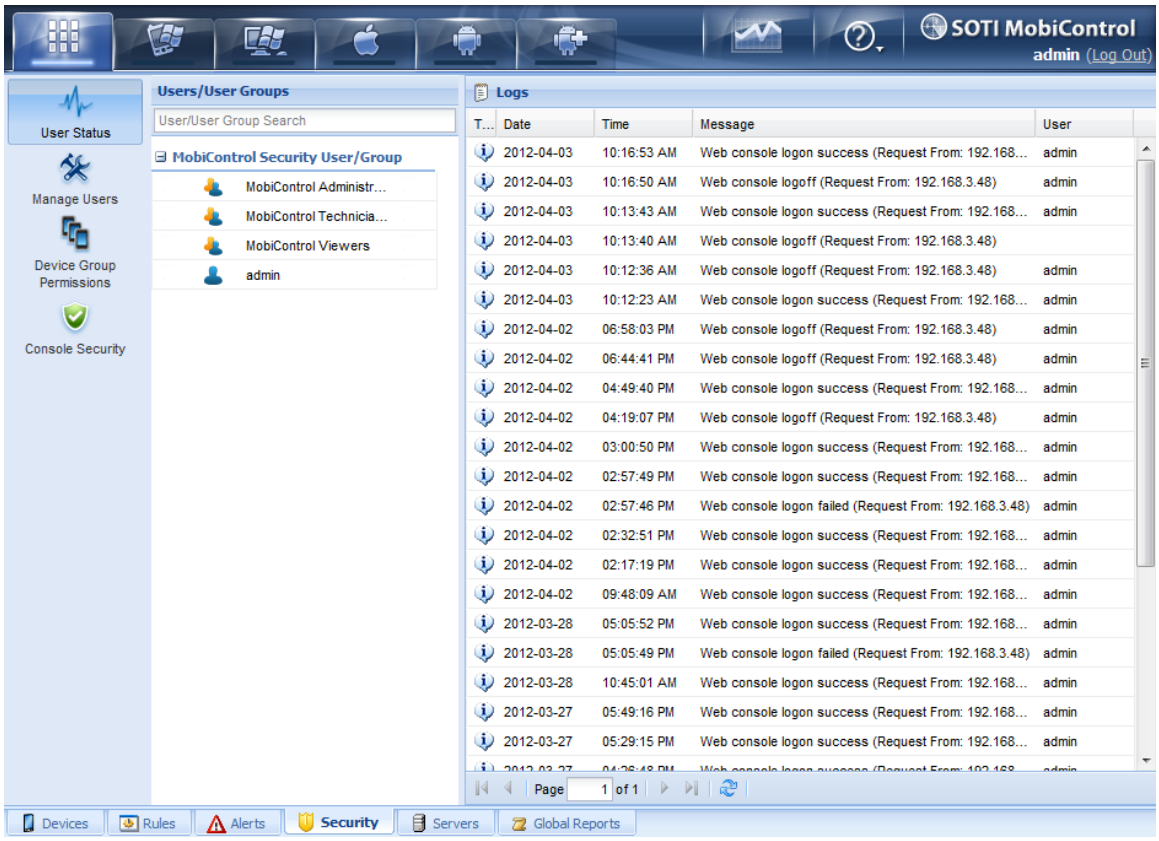
Security Question dialog

Active Directory Configuration

You can also toggle Active Directory Security on and off by clicking the **Active Directory Security** button. When you first turn on **Active Directory Security** a new window will appear asking you to insert your LDAP connection Settings. This is the LDAP Connections Manager. Please see the "LDAP Connections Manager" topic on page 616 for more details.

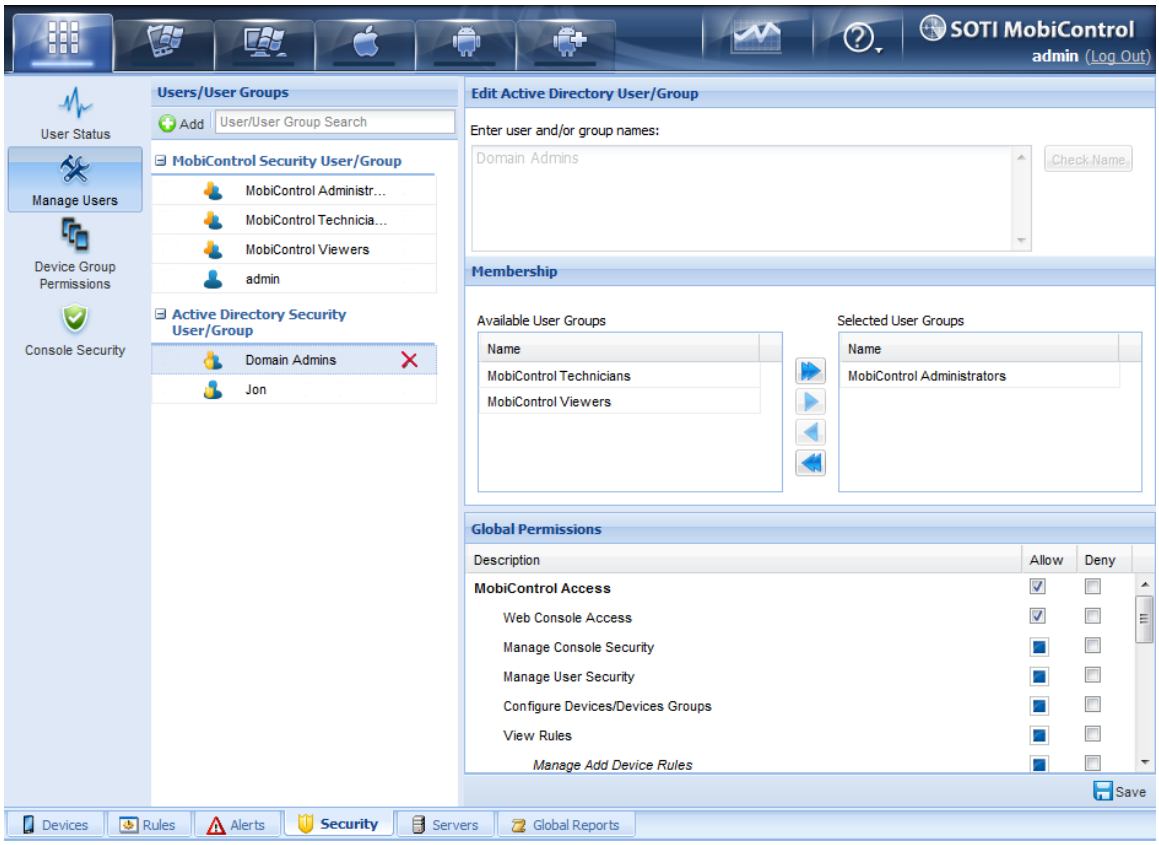
To Disable **Console Security** from within the Web Console click the **MobiControl Console Security** button. The following pop up will be displayed

User Status



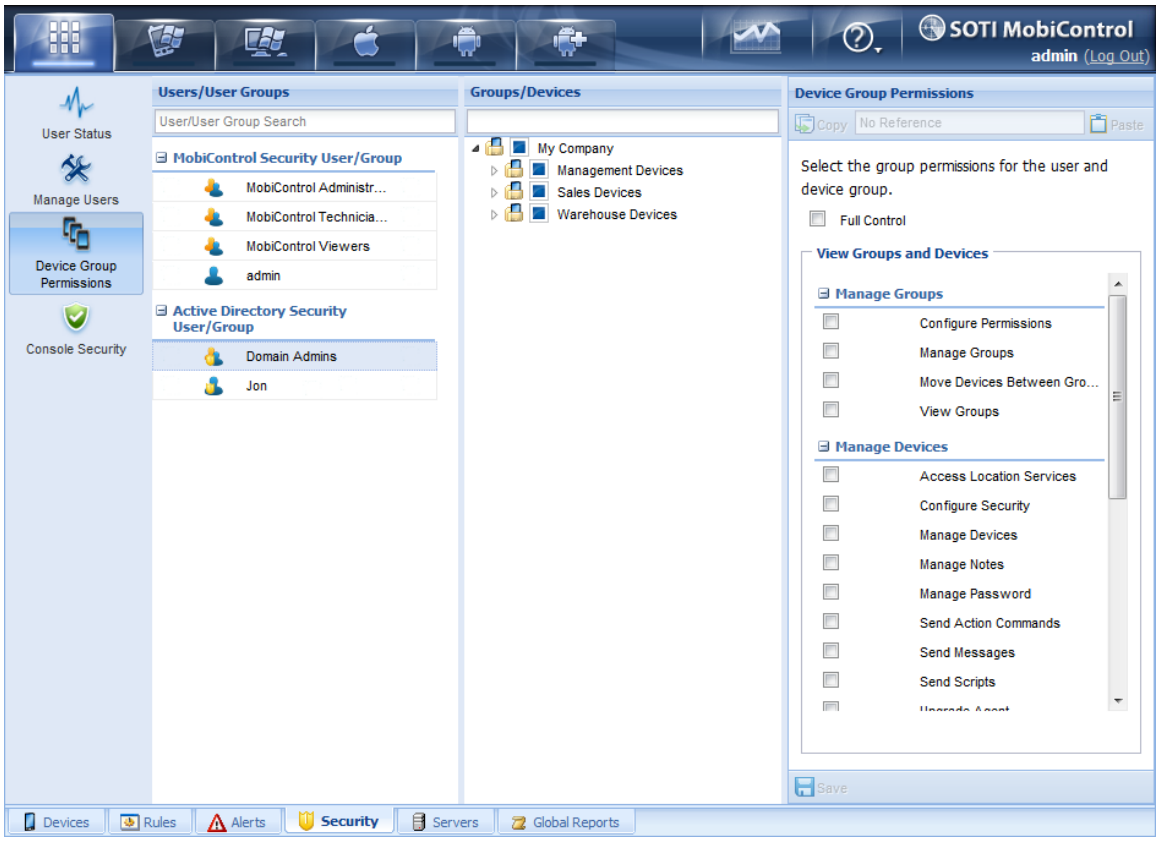
The **User Status** tab will provide you with detailed activity logs for both Users and Groups. Simply click on the desired Group or User and the logs will update. Clicking on the tab itself will display all user logs.

Manage User



From the **Manage Users** tab you can add both Basic and Domain Users and Groups as well as adjust their Basic Group Membership. The Global Permissions tab - general system permissions can be set to both Users and Groups. For assistance with these settings please visit the Manager Console User Security page.

Device Group Permissions



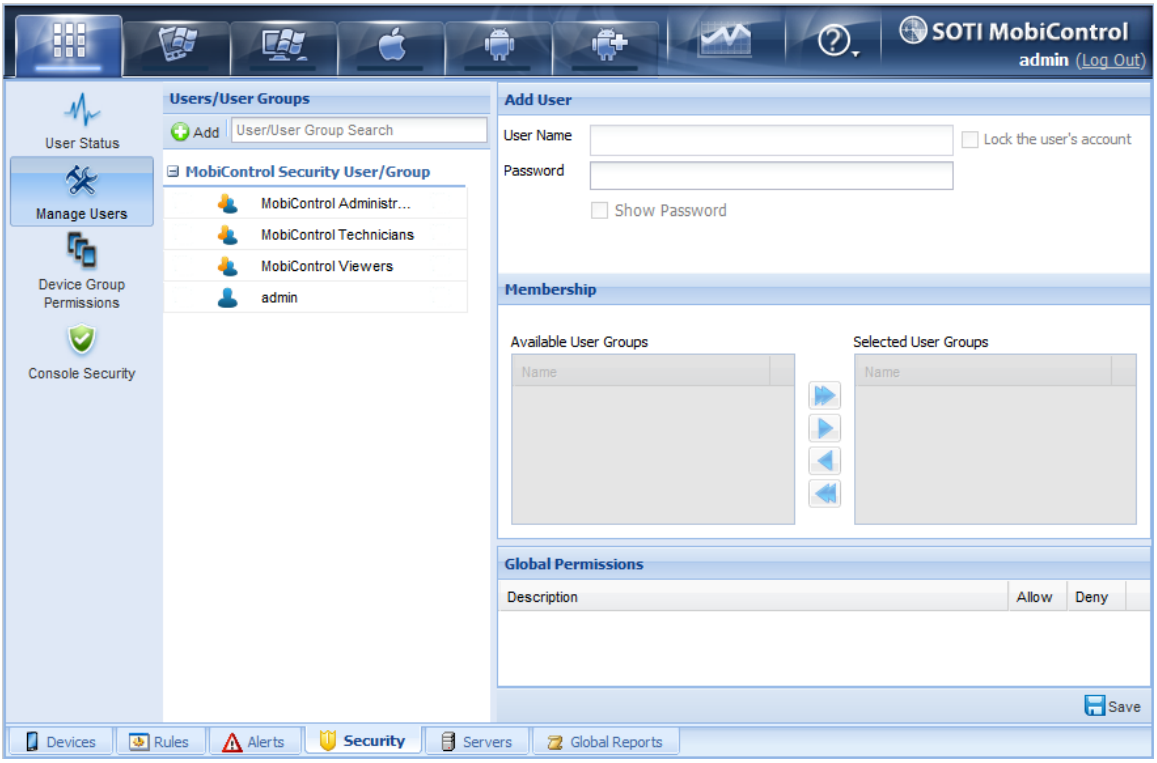
The **Device Group Permissions** tab allows you to apply more granular permissions based on the Device Tree Structure. For assistance with these settings, please see the Device Group Permissions page

Web Console Manage Users

IT administrators in security conscious organizations have roles-based security model(s) implemented to restrict the access to various applications and operations for personnel. The roles often reflect current organizational structures and business groups hierarchy.

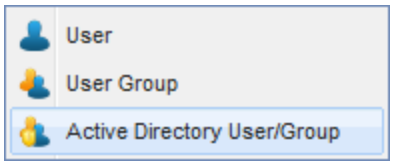
When using a powerful, feature-rich mobile device management solution like MobiControl, it may be desirable to limit access to MobiControl's functionality for some individuals or groups of users. For example, for a multi-tier support and help desk team, an organization may want to limit the access of tier-one help desk personnel to the MobiControl Web Console while added functionality and features might be available for tier-two personnel.

With the MobiControl Web Console, we are able to create new users and user groups. We are also able to bind to active directory to create accounts based on Active Directory credentials.



Manage Users

When the Add button is clicked in the manage users panel, a menu appears asking if we want to create a user, a user group or an Active Directory User/Group.Creating a user and a user group is independent of Active Directory and uses MobiControl's own security engine to keep passwords secure.



Add user, user group or Active Directory User/group

NOTE:

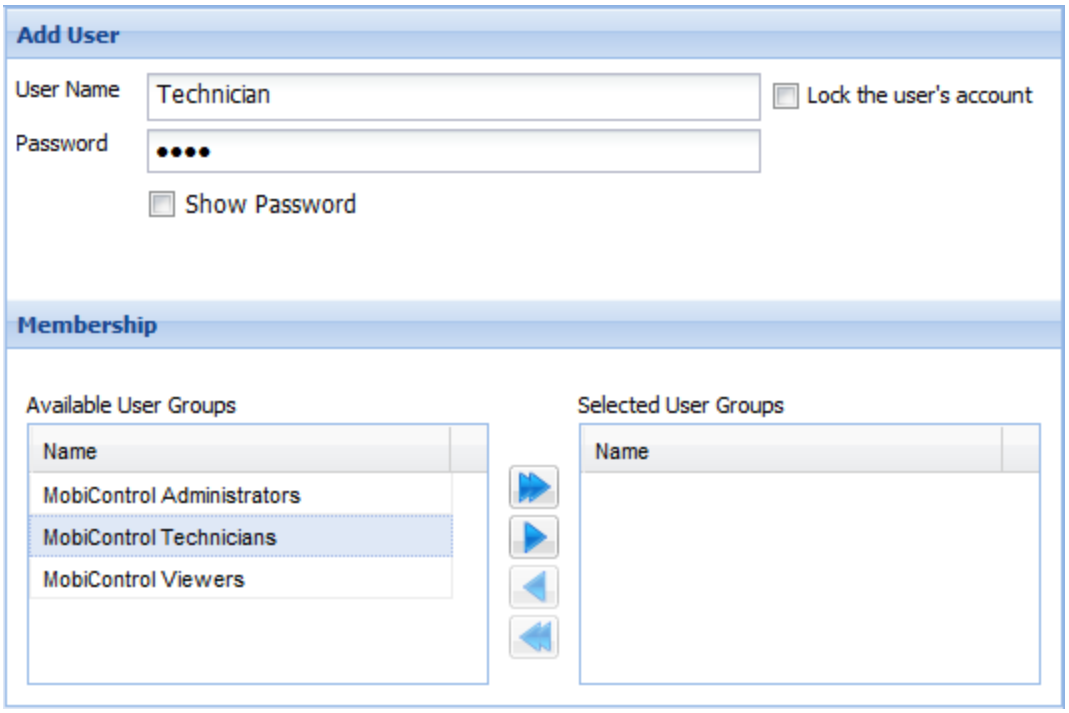
Before activating web console security, a MobiControl administration account must be created.

Users

Creating new users for the MobiControl web console allows only authorized users to access it.

When the **User** option is select from the Add menu, the right panel will change to the Add User interface. From here, we can create the name and password for the new user account. We can also assign this user to a user group. MobiControl comes with 3 default user groups: MobiControl Administrators, MobiControl Technicians and MobiControl Viewers. New user groups can be created from the User Group interface.

To add the user to the user group, select a group and click  .



Create New Users

After we're done, click the 

button in the bottom right hand corner.

NOTE:

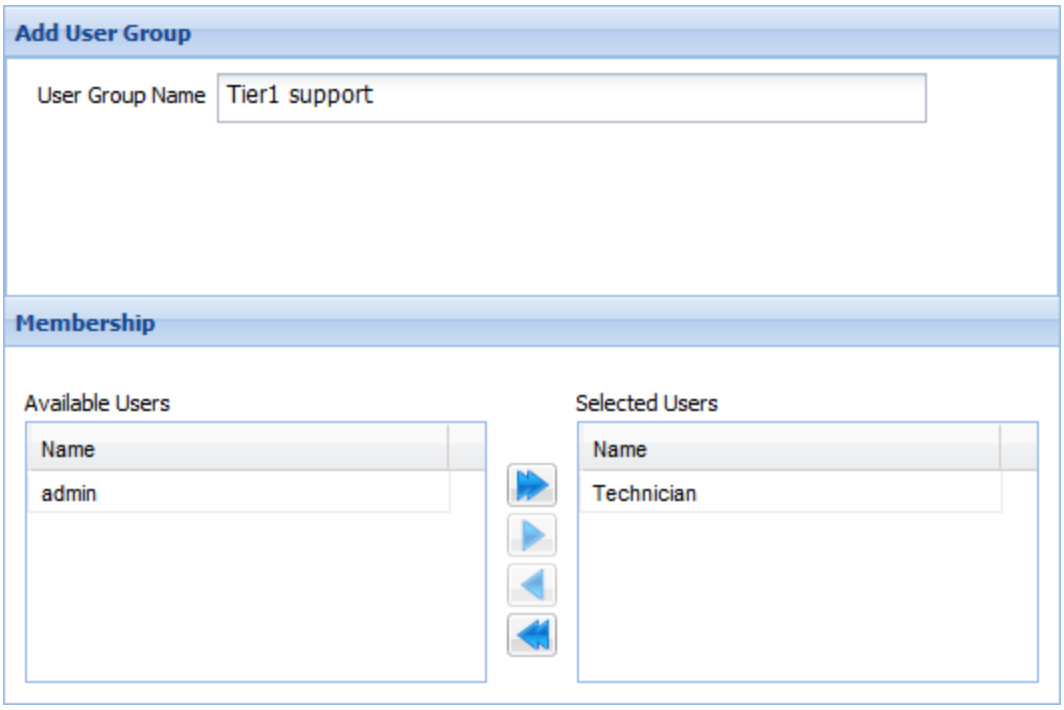
If a user has locked their account, uncheck the Lock the user's account option. This is only available for MobiControl user accounts, and not LDAP accounts.

User Groups

With user groups we are able to organize user accounts based on the Global permissions.

To create a user group, select **User Group** from the Add menu. The right panel will change to the Add User Group interface. Here we can name this user group.

We are also able to select which users are included in this group. To move users into this group, select a user and click  .



Create New User Groups

NOTE:

Users can be placed into more than one user group. If a Global Permission from one group conflicts with another group, the allow option will automatically be inherited.

After we're done, click the Save button in the bottom right hand corner.

Global Permissions

Global Permissions allows for the configuration of functionality in the MobiControl Web Console. For example, if a certain user group shouldn't be able to view device rules, just click deny in the View Rules section. Global Permissions can be modified on user accounts and user groups.

If allow or deny is not selected, the default value is set to deny.

Global Permission	Description
MobiControl Access	Allow or deny access to the MobiControl Manager. If allow is selected, every option below it will automatically be allowed. If deny is selected, every option below it will automatically be denied.
Web Console Access	Allow or deny access to the MobiControl Web Console
Manage Console Security	Allow or deny users to turn off Web Console security
Manage User Security	Allow or deny users to manage users
Configure Devices/Device groups	Allow or deny users to access the devices tab under each

Global Permission	Description
	device section
View Rules	Allow or deny users to view the rules tab. If allow is selected, Manage Add Device, Deployment, File Sync, Device Relocation, Data Collection, Alert and Application Catalog rules below it will automatically be allowed. If deny is selected, they will automatically be denied.
Manage Add Device Rules	Allow or deny users to manage Add Device rules
Manage Deployment Rules	Allow or deny users to manage Deployment rules
Manage File Sync Rules	Allow or deny users to manage File Sync rules
Manage Device Relocation Rules	Allow or deny users to manage Device Relocation rules
Manage Data Collection Rules	Allow or deny users to manage Data Collection rules
Manage Alert Rules	Allow or deny users to manage Alert rules
Manage Application Catalog Rules	Allow or deny users to manage Application Catalog rules
Configure Packages	Allow or deny users to access the packages tab under each device section
Configure Deployment Servers	Allow or deny users to access the servers tab
Manage Console Global Settings	Allow or deny users to change Global Settings for MobiControl. This includes changing the APNS certificate and log truncation.
Change MobiControl Registration Code	Allow or deny users to change the MobiControl registration code.
Manage System and Device Alerts	Allow or deny the users to view and access alerts
Generate and Print Reports	Allow or deny users to access the reports tab under each device section
Import Reports	Allow or deny users to import new reports
View Dashboard	Allow or deny users to view the Web Console dashboard

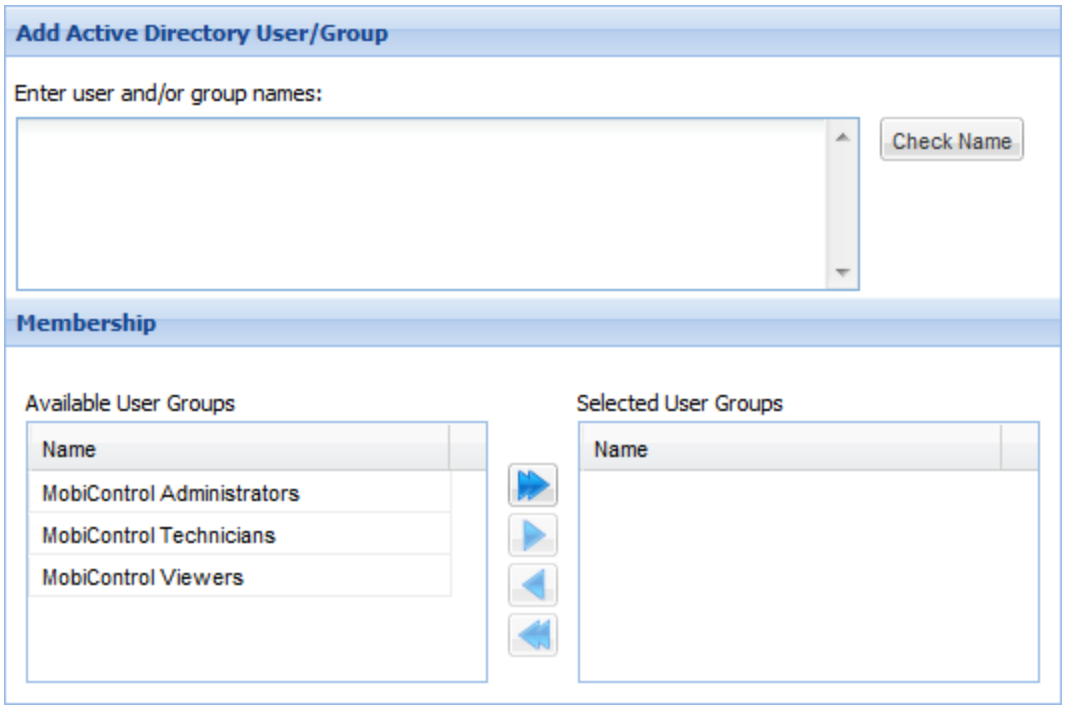
Active Directory User/Group

Using Active Directory accounts is efficient to users because they would enter the username and password they log into their Windows Workstation with, meaning, one less password to remember. To ensure that Active Directory user accounts can be binded, please make sure that Active Directory Security is enabled in console security. Please see the "Console Security" topic on page 590 for more information on how to enable Active Directory security.

When Active Directory User/group is selected, the right panel will change to Add Active Directory User/Group. Here, **enter the display name of the user/group to be added and not the User/Group ID.** Click Check Name to find the user/group.

If an Active Directory group is added, then all users who are included into that group have access to the MobiControl Web Console.

You can also assign Active Directory user/groups to MobiControl Security Groups.



Create New MobiControl Active Directory Accounts

After we're done, click the Save button in the bottom right hand corner.

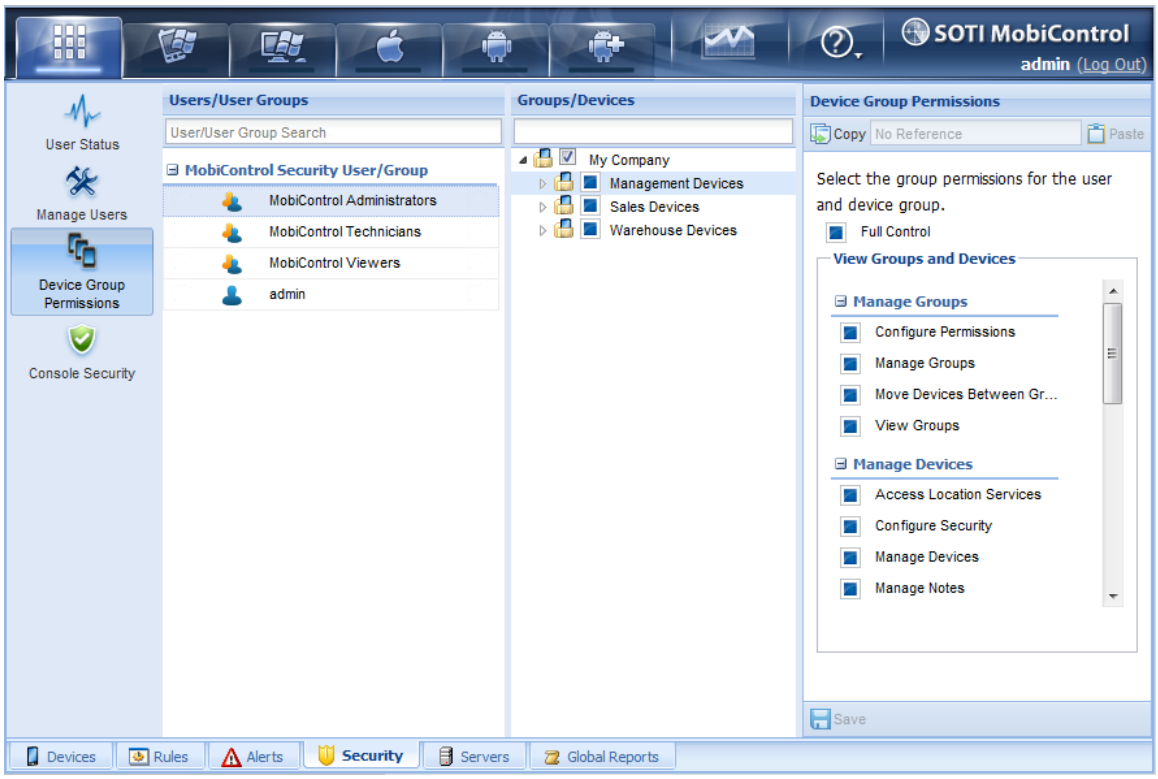
Removing users

If a user account or group is not required anymore, click the user account/group and click ✕.

Web Console Device Group Permissions

Device group permissions allow for the segregation of MobiControl management privileges based on the device tree structure. For example, a support team operating out of California may be responsible for supporting all the devices in the western states, while another team out of New York is responsible for controlling all the devices in the eastern states. Using device group permissions, the members of the two respective teams can be granted varying levels of access to the devices in their own region (i.e. full access), and those in other regions (e.g. no access).

To enable group permissions, you must first enable the MobiControl Web Console user security. (Please see the "Console Security" topic on page 586.) Once the Web Console user security is enabled, select **Device group permissions**.

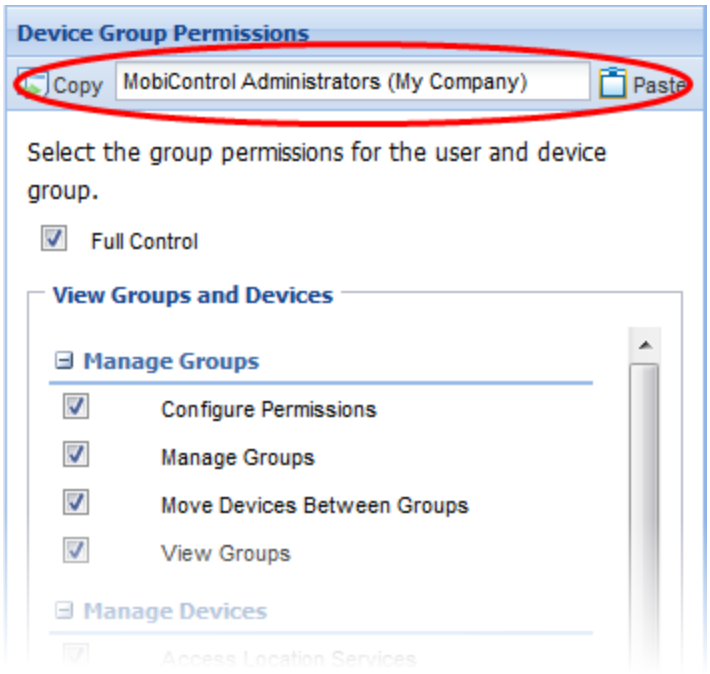


Selecting "Device Group Permissions" in the MobiControl Web Console

From the **Device Group Permissions**section on the right side, user access and permissions can be customized. For instance, if a particular user needs to access everything, **Full Control** should be selected. Alternatively, if the user should only to be able to remote control the device, then select only that option. These security settings are applied to the device groups in theMobiControl Web Console and define what users can do at the device level.

The permissions in the group permissions page can be set at the group level, as well as the individual user level. The permissions will take the most restrictive settings.

MobiControl includes a copy feature when configuring device group permissions. With this, administrators can copy a group's configuration and paste it to another group. To do this, select a group to be copied, and click copy. Once copy has been clicked, the name of the MobiControl security user/group is shown as well as the group. After, select another group and click paste. All configurations from the copied group are now pasted into the new one.



Web Console copy and paste

After all group permissions have been set, click Save at the bottom of the device group permissions section.

Device Group Permissions

If **Full Control** is selected, then every permission is automatically selected.

Manage Groups

Access Right	Description
Configure Permissions	Allow user/group to configure group permissions
Manage Groups	Allow user/group to right click device groups
Move Devices Between Groups	Allow user/group to move devices between two groups
View Groups	Allow user/group to view device groups

Manage Devices

Access Right	Description
Access Location Services	Allow user/group to locate and track devices
Configure Security	Allow user/group to configure device security (Lockdown, authentication)
Manage Devices	Allow user/group to right click devices

Access Right	Description
Manage Notes	Allow user/group to create and manage notes for devices
Manage Password	Allow user/group to reset device passwords
Send Action Commands	Allow user/group to send action commands (reset device, etc)
Send Messages	Allow user/group to send messages to devices
Send Scripts	Allow user/group to send scripts to devices
Upgrade Agent	Allow user/group to enable device upgrade

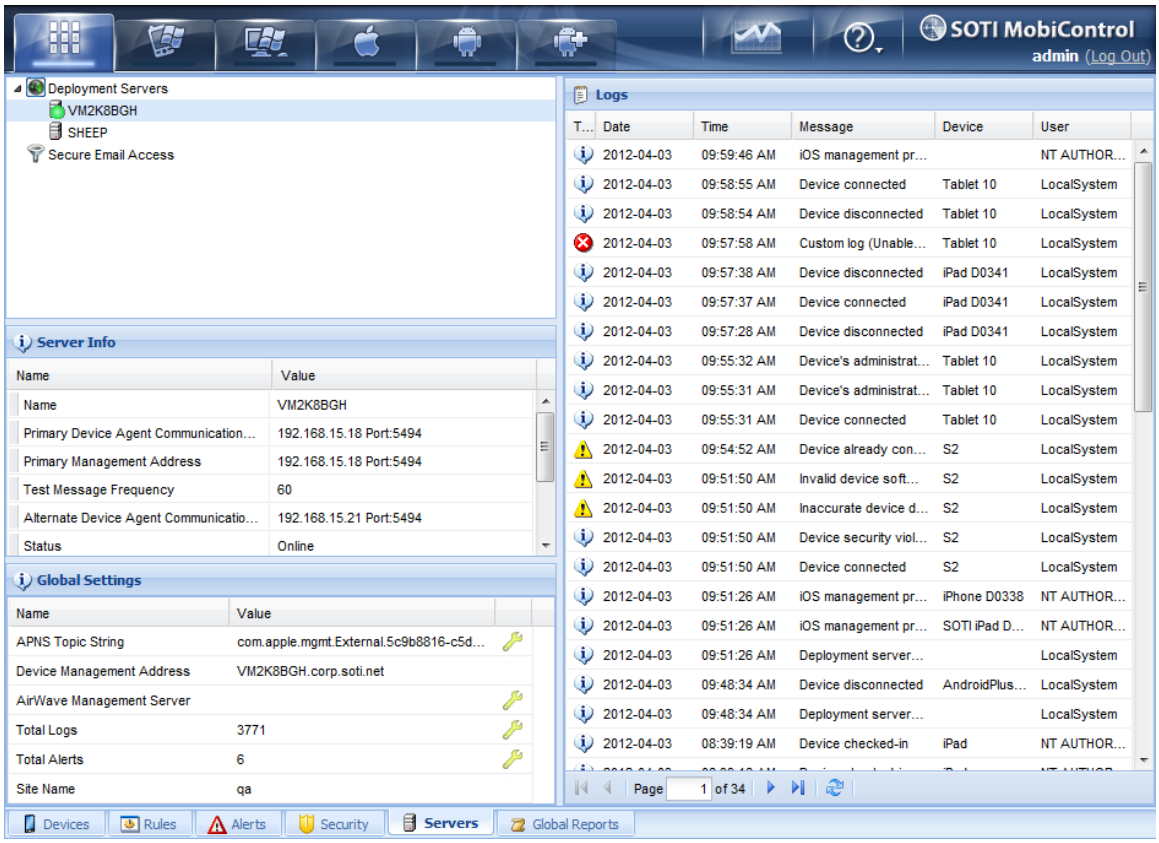
Remote Control Devices

Access Right	Description
Control Without Notification	Allow user/group to remote control devices without letting device operators know
Edit Tasks and Services	Allow user/group to stop device tasks
Remote Control Devices	Allow user/group to remote control devices
Remote Control Scripting	Allow user/group to use scripts
Run Command Prompt	Allow user/group to open the command prompt
Send Keyboard/Mouse Input	Allow user/group to send keyboard and mouse control to the device
Update Files	Allow user/group to save changes to device files
Update Registry	Allow user/group to save changes to the device registry
View Files	Allow user/group to view device files
View Registry	Allow user/group to view the device registry
View System Info	Allow user/group to view device system information (RAM, CPU usage)
View Tasks and Services Info	Allow user/group to view what applications are currently running on the device

Servers Tab

The Deployment Servers view (tab) in MobiControl Web Console lists all MobiControl Deployment Servers installed, the online devices connected to the servers and the Secure Email Access . Users can remotely configure and manage Deployment Servers using the Deployment Servers view (tab).

Please see the "Deployment Server Overview" topic on page 382 for general concepts about MobiControl Deployment Servers.



Field Name	Description
Server Info	Displays the Server Information of the selected Deployment Server
Logs	Displays the logs of the selected Deployment Server
Global Settings	Displays the external communication settings for Android and iOS devices.

Global Settings

Change APNS Certificate

If you need to change your APNS certificate you may do so by clicking the **Change APNS Certificate** button located inside the **Global Settings** section of the Web Console.

LDAP Connections

LDAP Connections brings up the LDAP Connections Manager. Here we can configure multiple LDAP connections to use through out MobiControl. Please see the "LDAP Connections Manager" topic on page 616 for more information about this manager.

Aruba AirWave Management Server

MobiControl allows integration with Aruba AirWave v7.2x. For more information on Aruba AirWave please visit www.arubanetworks.com.

Item	Description
Server Name	Friendly name of the AirWave server
URL	URL of the AirWave Management Service
Username	Username used to access the AirWave Management Service
Password	Password used to access the AirWave Management Service.

Total Logs

Total Logs displays the total amount of logs of the MobiControl Deployment. Clicking the icon opens the Log Maintenance options. Click here for more information about Log Maintenance.

Total Alerts

Total Alerts displays the total amount of Alerts. Clicking the icon opens Alerts Truncation options. Click here for more information bout Alerts Truncation.

Certificate Authorities

Configuring Certificate Authorities, allows MobiControl to issue certificates on behalf of users. MobiControl can utilize ADCS, Entrust and any Generic SCEP server. Please see the Certificate Authorities page for more information.

Terms and Conditions Manager

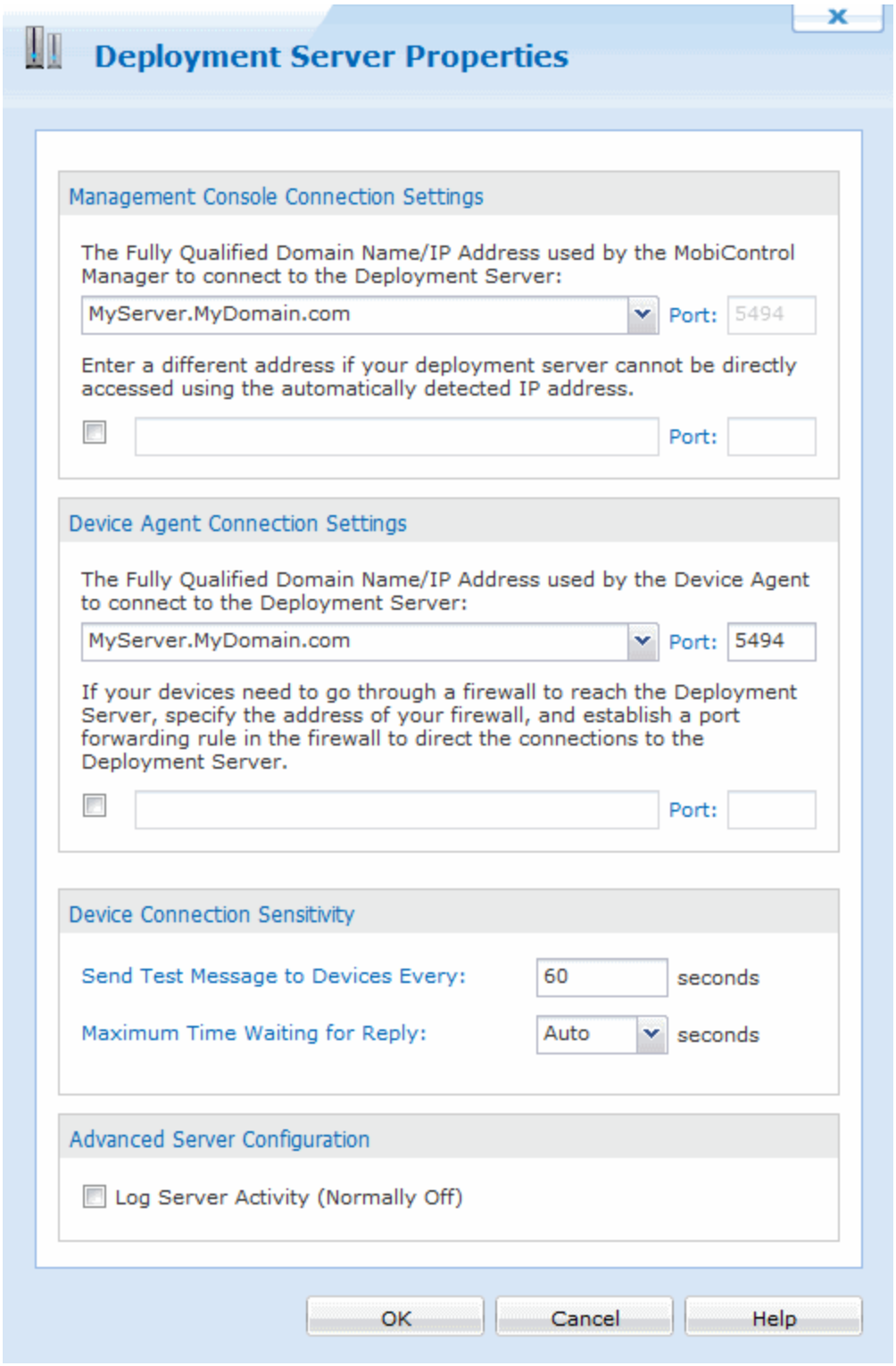
The Terms and Conditions Manager allows us to modify or create new Terms and Conditions to use in Add Device Rules. Please see the "Terms and Conditions" topic on page 619 for more information.

Manage Custom Attributes

Manage Custom Attributes allows us to modify or create new attributes used across devices and device groups. Please see the "Custom Attributes" topic on page 1343 for more information.

Server Properties

To set Deployment Server properties, select the icon for a particular Deployment Server in the Deployment Servers view (tab) and select the **Server Properties** option from the **Deployment Server** menu. The **Deployment Server Properties** dialog box will be displayed.



Deployment Server Properties dialog box

Server configuration and device connection sensitivity settings can also be changed through the Deployment Server system tray applet. Please see the "Deployment Server Configuration" topic on page 386. The table below describes each field of the **Deployment Server Properties** dialog box:

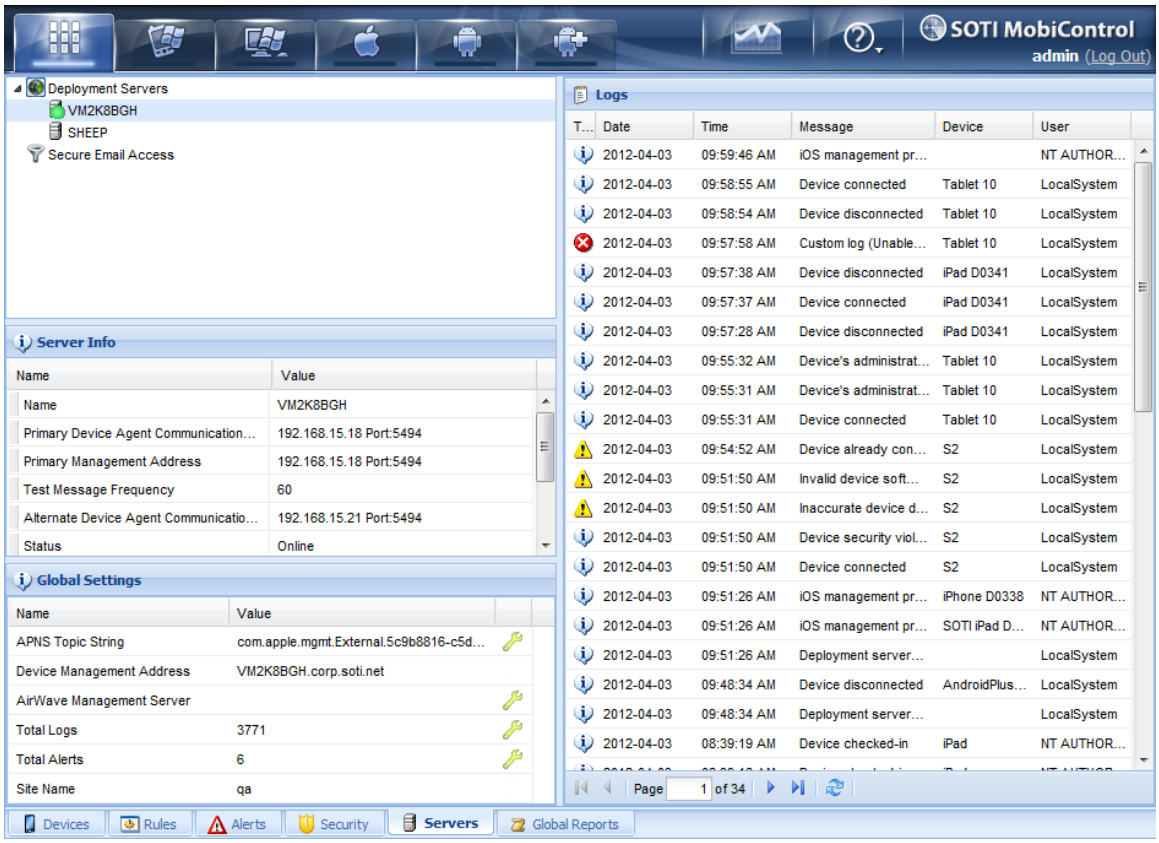
<table>
<tr><th>Field Name</th><th>Description</th></tr>
<tr><td>Management Console Connection Settings</td><td>This is the IP address or hostname used by the management console to connect to the Deployment Server to receive real-time updates. The Deployment Server automatically reads the default IP address assigned to the host computer upon which it is running. If you wish to change this IP address, select Override automatically detected IP address. You may also specify an alternate server address in situations where the device will need to use a different IP address when connecting to a certain IP network. This option is also useful when you need to move the from one host computer to another.</td></tr>
<tr><td>Device Agent Communication Settings</td><td>This is the Fully Qualified Domain Name (ie Hostname)/IP address used by devices to connect to the Deployment Server to receive updates and facilitate remote control.
By default, this address is the same as the management address. In situations where mobile devices need to go through a firewall or proxy server the devices may need to use external addresses for Deployment Servers that get mapped by the firewall or proxy server to the private network address.
NOTE:
We recommend you to specify a DNS resolvable hostname instead of a static IP address as the DNS resolvable hostname is less likely to change.
When MobiControl Device Agent software is generated, the server address for device communication is injected into the generated Device Agents. If you need to change the external IP address, you need to do this before you generate a Device Agent for new devices. For devices that are already connected to the Deployment Server, these settings are refreshed on the devices when they reconnect to the server.
You may also specify an alternate server address in situations where the device will need to use a different IP address when connecting to a certain IP network. This option is also useful when you need to move the MobiControl Deployment Server from one host computer to another.
When external addresses are configured, MobiControl Device Agents will try to connect to the Deployment Server using one of the addresses. If multiple addresses are configured, the set Deployment Server priorities will be used to determine which Deployment Server an agent should try to connect to. Please see the "Deployment Server Priority" topic on page 167 for information on Deployment Server priority configuration.
Devices connecting through a proxy
If the Device requires proxy access to the Internet in order for the device agents to connect to the Deployment Server you can use the following settings in the Device Agent Connection Field:
www Proxy:
http://<Username>:<Password>@<Proxy Server>:<Proxy Port>/<DS Address>:<DS Port>

Socks Firewall/Proxy:
socks://<Username>:<Password>@<Proxy Server>:<Proxy Port>/<DS Address>:<DS Port></td></tr>
</table>

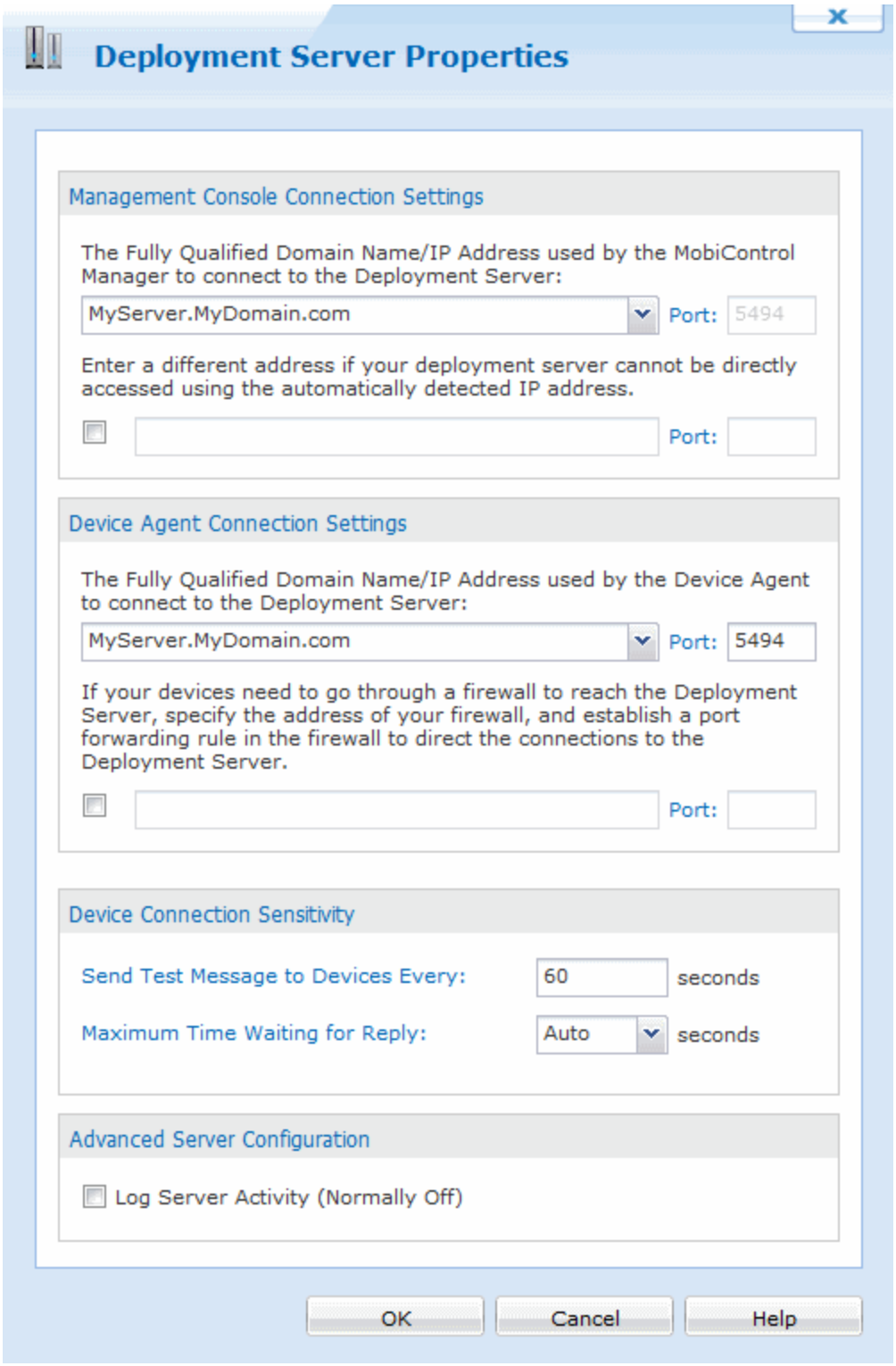
Field Name	Description
	or socks://<Proxy Server>:<Proxy Port>/<DS Address>:<DS Port>
Send Test Message to Device Every	This setting is used to control how often the Deployment Server is to send test message to device. MobiControl Deployment Servers send test messages (approximately 32 bytes) to devices periodically and then wait for the device to send the message back. If a Deployment Server does not receive a test message back within a specified time, it concludes that the connection is not functioning properly, and closes the connection to the device. For slow connections or situations where you are being charged based on your amount of data you send through the network (e.g. some cellular data plans) we recommend that you set the Deployment Server's **Send Test Message to Devices Every** setting to at least 180 seconds.
Maximum Time Waiting for Reply	This setting is used to control how long the Deployment Server will wait for the reply from the device.
Log Server Activity (Normally Off)	If this box is checked, the Deployment Server will start verbose logging. This may result in slowing down the response time problems, and working with SOTI support staff. Select the **View Log** button to display the debug log for the Deployment Server. This log provides useful information when diagnosing potential problems with technical support.

Server Properties

The Deployment Servers view (tab) in MobiControl Manager lists all MobiControl Deployment Servers installed, the online devices connected to the servers as well as properties for the servers. Users can remotely configure and manage Deployment Servers using the Deployment Servers view (tab).



To set Deployment Server properties, select the icon for a particular Deployment Server in the Deployment Servers view (tab) and select the **Server Properties** option from the **Deployment Server** menu. The **Deployment Server Properties** dialog box will be displayed.



Deployment Server Properties dialog box

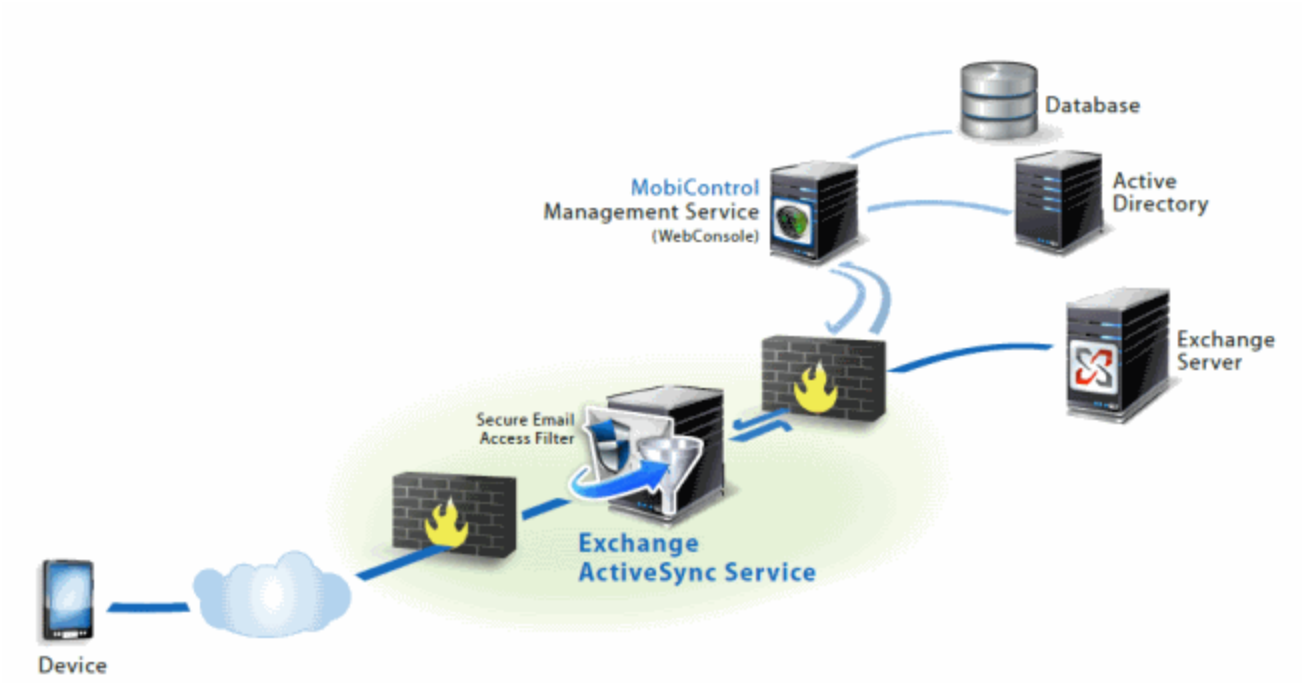
Server configuration and device connection sensitivity settings can also be changed through the Deployment Server system tray applet. Please see the "Deployment Server Configuration" topic on page 386. The table below describes each field of the **Deployment Server Properties** dialog box:

Field Name	Description
Management Console Connection Settings	This is the IP address or hostname used by the management console to connect to the Deployment Server to receive real-time updates. The Deployment Server automatically reads the default IP address assigned to the host computer upon which it is running. If you wish to change this IP address, select **Override automatically detected IP address.** You may also specify an alternate server address in situations where the device will need to use a different IP address when connecting to a certain IP network. This option is also useful when you need to move the from one host computer to another.
Device Agent Communication Settings	This is the Fully Qualified Domain Name (ie Hostname)/IP address used by devices to connect to the Deployment Server to receive updates and facilitate remote control. By default, this address is the same as the management address. In situations where mobile devices need to go through a firewall or proxy server the devices may need to use external addresses for Deployment Servers that get mapped by the firewall or proxy server to the private network address. **NOTE:** We recommend you to specify a DNS resolvable hostname instead of a static IP address as the DNS resolvable hostname is less likely to change. When MobiControl Device Agent software is generated, the server address for device communication is injected into the generated Device Agents. If you need to change the external IP address, you need to do this before you generate a Device Agent for new devices. For devices that are already connected to the Deployment Server, these settings are refreshed on the devices when they reconnect to the server. You may also specify an alternate server address in situations where the device will need to use a different IP address when connecting to a certain IP network. This option is also useful when you need to move the MobiControl Deployment Server from one host computer to another. When external addresses are configured, MobiControl Device Agents will try to connect to the Deployment Server using one of the addresses. If multiple addresses are configured, the set Deployment Server priorities will be used to determine which Deployment Server an agent should try to connect to. Please see the "Deployment Server Priority" topic on page 167 for information on Deployment Server priority configuration. Devices connecting through a proxy If the Device requires proxy access to the Internet in order for the device agents to connect to the Deployment Server you can use the following settings in the Device Agent Connection Field: **www Proxy:** http://<Username>:<Password>@<Proxy Server>:<Proxy Port>/<DS Address>:<DS Port> **Socks Firewall/Proxy:** socks://<Username>:<Password>@<Proxy Server>:<Proxy Port>/<DS Address>:<DS Port>

Field Name	Description
	or socks://<Proxy Server>:<Proxy Port>/<DS Address>:<DS Port>
Send Test Message to Device Every	This setting is used to control how often the Deployment Server is to send test message to device. MobiControl Deployment Servers send test messages (approximately 32 bytes) to devices periodically and then wait for the device to send the message back. If a Deployment Server does not receive a test message back within a specified time, it concludes that the connection is not functioning properly, and closes the connection to the device. For slow connections or situations where you are being charged based on your amount of data you send through the network (e.g. some cellular data plans) we recommend that you set the Deployment Server's **Send Test Message to Devices Every** setting to at least 180 seconds.
Maximum Time Waiting for Reply	This setting is used to control how long the Deployment Server will wait for the reply from the device.
Log Server Activity (Normally Off)	If this box is checked, the Deployment Server will start verbose logging. This may result in slowing down the response time problems, and working with SOTI support staff. Select the **View Log** button to display the debug log for the Deployment Server. This log provides useful information when diagnosing potential problems with technical support.

Secure Email Access

MobiControl's Secure Email Access filter provides the ability to restrict access to the enterprise Exchange environment. The Secure Email Access filter will intercept Exchange ActiveSync requests and only allow legitimate traffic through to the Exchange server.

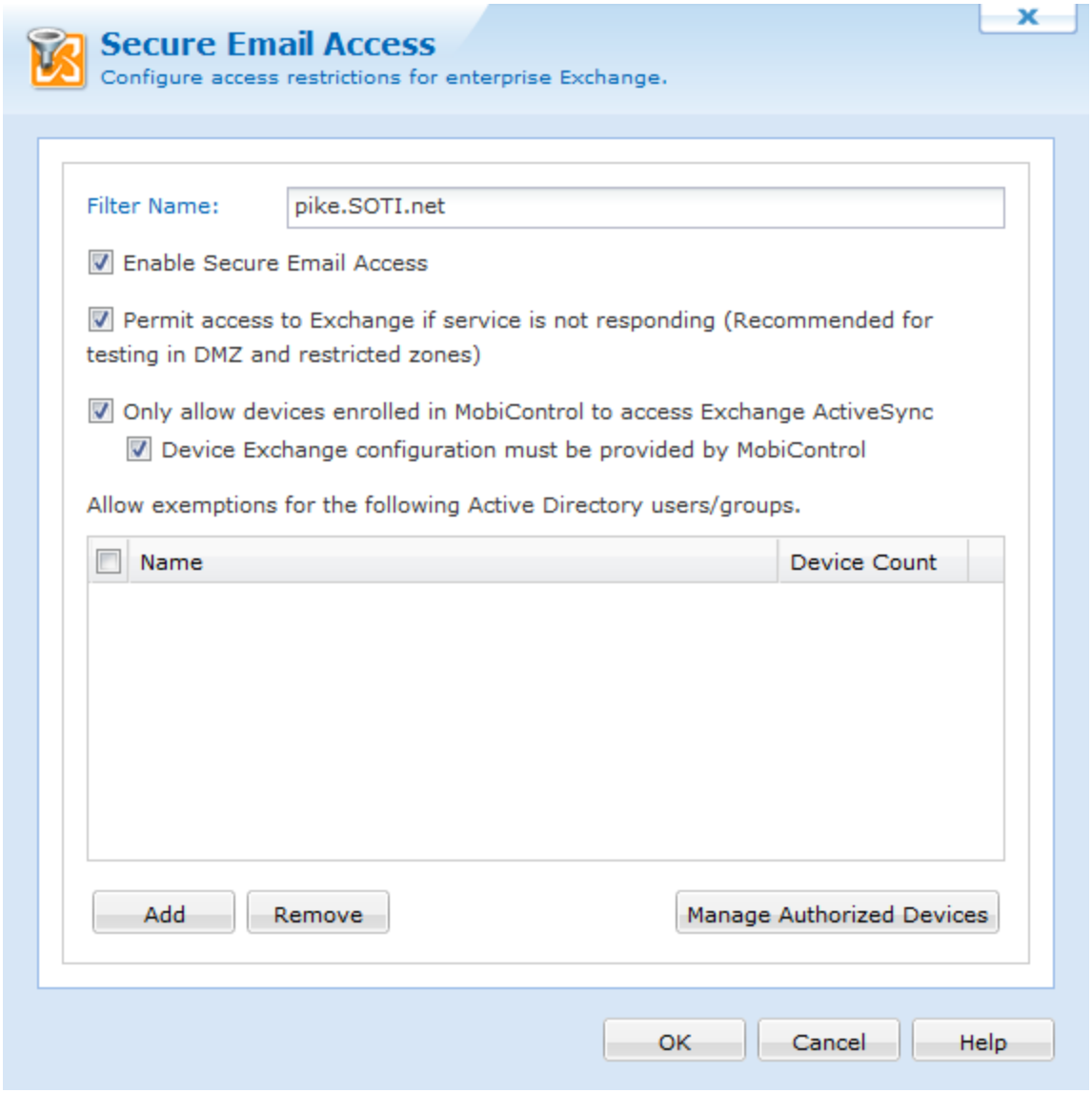


To install the Secure Email Access filter please Skin/Formats/CrossReferencePrintFormat(See "Secure Email Access Install The Secure Email Access Filter allows you to achieve greater control with devices receiving email from your Exchange Service. When the filter is installed, you can block access to Exchange on certain devices as well as other controls. To successfully install the Exchange ActiveSync Filter, the MobiControl Root CA must be installed on the server that is publishing the Exchange ActiveSync Service. Below shows how to install the filter on your Exchange Server. Prerequisite StepsInstall MobiControl's Secure Email Access filter(Optional) 3rd party Exchange ActiveSync Filter Configuration Prerequisite StepsThe prerequisite steps show how to install the MobiControl Root CA on the Exchange Server. Go to the MobiControl Administration Utility and go to Certificates. The MobiControlAdministration Utility (MCAU)Click the Export button at beside the MobiControl Root Certificate label. Export the MobiControlRoot CertificateSave the exported certificate in a directory that is easy to remember. Next we need to go to the server with the Exchange ActiveSync Service.Open the Microsoft Management Console (MMC) by opening up the run command and typing mmc. Open the Microsoft Management Console. In MMC, click File then Add/Remove Snap In...Adding Snap-insSelect the Certificates snap-in and click Add >. Adding the Certificates Snap-inA new window will appear asking to select an account. Select the Computer account and click Next. Select the Computer Account. On the next screen select Local Computer and click Finish. Select ComputerAfter clicking Finish, click OK in the Add or remove Snap-ins window. Expand the Certificates (Local Computer) tree on the left side and go to Trusted Root Certification Authorities, then Certificates. Right click the Certificates folder and go to All Tasks then Import.Importing a new CA Follow the steps in the Certificate Import Wizard leaving all settings default. After the wizard has finished you will see the MobiControl Root CA in your Trusted Root Certification Authorities. The MobiControl Root CAInstall MobiControl's Secure Email Access filterMobiControl's Secure Email Access Filter must be installed on the server that is publishing the Exchange ActiveSync service. Typically this is the same computer that is hosting OWA (Outlook Web Access). From the server where the Secure Email Access filter will be installed, open Internet Explorer and browse to the MobiControl Web ConsoleLog in to the Web Console as an Administrator based account that has the "Configure Deployment Servers" permissionSelect the All Devices tab at the top of the MobiControl Web Console and then select the Servers tab located along the bottom of the Web ConsoleRight click on the Secure Email Access filter listed under the Deployment Server, and select Install Exchange ActiveSync FilterSave and then run the ExchangeActiveSyncFilter.exe program. This will place the needed files onto

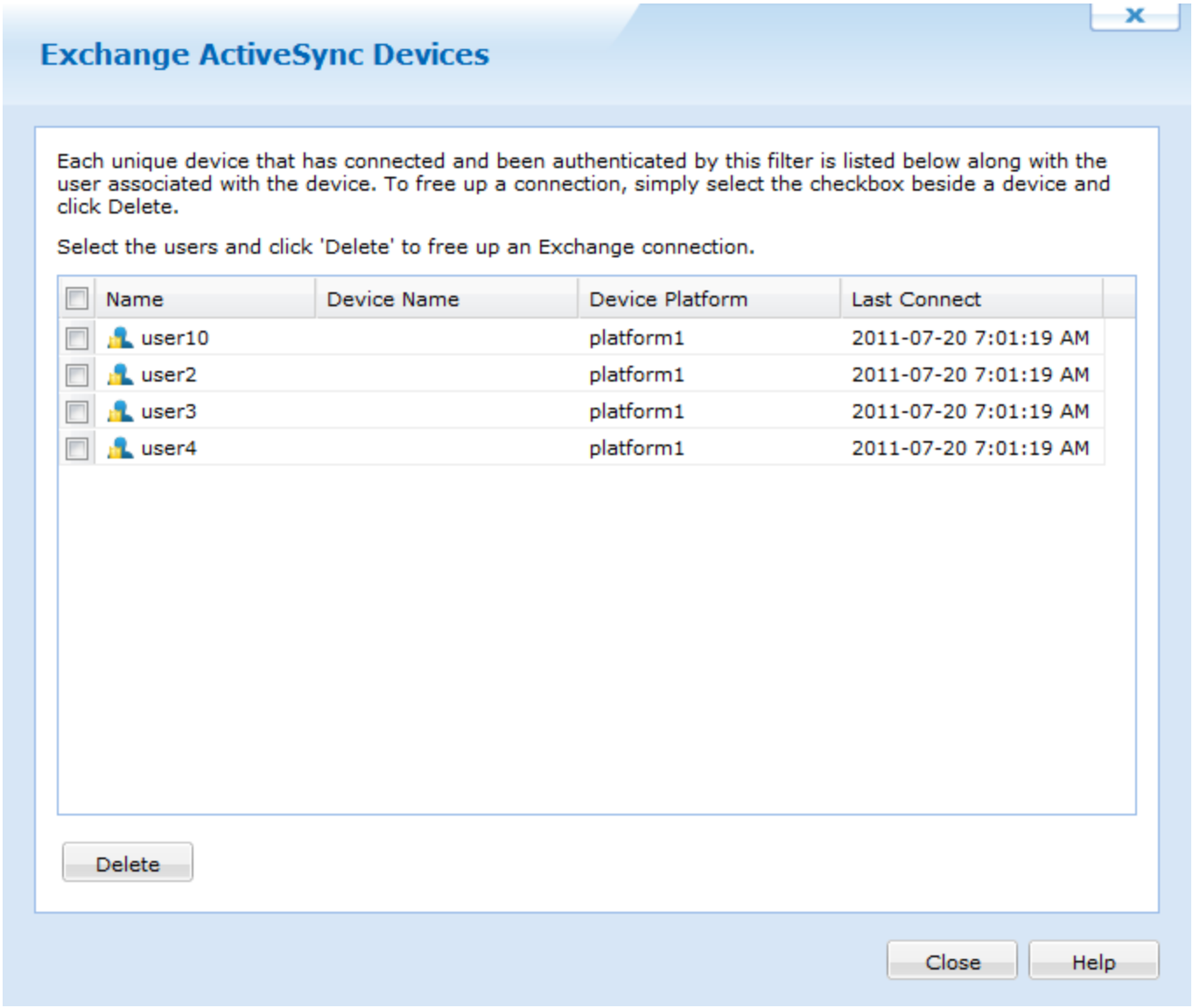
the server. Note: Depending on your Internet Explorer settings, you may be prompted to allow file downloads from the web pageOpen IIS manager and select the web site that is publishing Exchange ActiveSync Select ISAPI filters and select Add from the list of actionsEnter MobiControl Secure Email Access as the filter name For the Executable, If the Exchange ActiveSync site is running in a 32-bit application pool, select \Program Files\SOTI\XAS\mcxas.dll or, if the Exchange ActiveSync site is running in a 64-bit application pool, select \Program files\SOTI\XAS\mcxas64.dllSelect OK to save the filterIn the resulting list of filters, ensure that the MobiControl Secure Email Access filter is listed above the Microsoft Exchange ActiveSync filter. If this is not the case, select View Order List from the available actions, highlight MobiControl Secure Email Access and select Move Up to place it at the top Note: MobiControl's Secure Email Access required communication between the server that is publishing Exchange ActiveSync where the filter is installed, to the MobiControl Web Console. This communication happens over SSL on port 443.3rd party Exchange ActiveSync Filter ConfigurationBefore you begin, the following components must be installed/enabled.1. IIS 7 with ASP.NET role service enabled.2. URL Rewrite Module installed (version 2.0 is required)3. Application Request Routing version 2.5 (Link)The URL Rewrite Module and Application Request Routing version 2.5 are both installed at the same time. After installation, please follow these steps:Open the IIS managerSelect the server in the tree view on the left hand side and then click on the Application Request Routing feature.Application Request RoutingOn the right menu, click Server Proxy Settings in the Proxy SectionServer Proxy SettingsCheck the Enable Proxy check box. Leave the default values for all the other settings on this page. Click Apply on the right side to commit the change.Enable ProxyNext step is to add the HTTP_ACCEPT_ENCODING server variable and Inbound and Outbound rules. To do this, please go to the left hand panel and select the Default Web Site and then select URL Rewrite. URL rewriteIn the URL Rewrite page, select View Server Variables on the right hand side. View Server VariablesClick the Add... link on the right side of the page to add the HTTP_ACCEPT_ ENCODING variable. Click OK then Back to Rules. Adding a server variableClick the Add Rule(s)... link on the right side to add Inbound and Outbound rules. Add rule(s)...When creating the Inbound and Outbound rules, select Blank Rule under the respected heading and click OK.Adding a Blank Inbound or Outbound ruleOn the page shown below, the following fields need to have values entered (Please ensure that you enter your appropriate owa address):NameReverseProxyInboundRule1Pattern^(.*)Rewrite URLhttps://owa.myDomain.com/{R:1} Inbound Rule creation pageAfter the values have been entered, the server variable needs to be added. To do this, expand the Server Variables panel. Click Add and choose HTTP_ACCEPT_ENCODING from the drop down menu. Under value, enter 0, then click OK. Set Server VariableAfter entering all required values, click Apply.Apply Inbound RuleCreate a new blank rule to create an Outbound Rule. Please see below for what values to set on this page: Outbound rule pageUnder precondition, you will need to create a new condition. To do this, select <Create New Precondition...>. When the pop up window appears, click Add... to add a pattern:Add PreconditionAfter entering all required values, Click OK then click Apply.Apply Outbound RuleAfter the rules have been created, click the IIS server, and restart. To confirm that everything has been configured properly, go to C:\inetpub\wwwroot and open the web.config file in notepad. Your file should look similar to this: <?xml version="1.0" encoding="UTF-8"?> <configuration> <system.webServer> <rewrite> <rules> <rule name="ReverseProxyInboundRule1"> <match url="^(.*)" /> <serverVariables> <set name="HTTP_ ACCEPT_ENCODING" value="0" /> </serverVariables> <action type="Rewrite" url="https://owa.soti.net/ {R:1}" /> </rule> </rules> <outboundRules> <rule name="ReverseProxyOutboundRule1" preCondition="ResponseIsHtml1"> <match filterByTags="A, Form, Img" pattern="^http (s)?://owa.soti.net/(.*)" /> <action type="Rewrite" value="http{R:1}://owa.soti.net/{R:2}" /> </rule> <preConditions> <remove name="ResponseIsHtml1" /> <preCondition name="ResponseIsHtml1"> <add input="{RESPONSE_CONTENT_TYPE}" pattern="^text/html" /> </preCondition> </preConditions> </outboundRules> </rewrite> </system.webServer> </configuration>" on page 1) page.

MobiControl allows you to configure which devices are allowed to communicate with the Exchange server. Once the filter is installed and enabled, you can block access for any device that is not enrolled in MobiControl. This means that the device must be listed in MobiControl’s device tree or it will not be allowed to communicate with Exchange.

Further, any device that has Exchange settings that were not set by MobiControl can be blocked ensuring that only devices with the correct Exchange ActiveSync configuration are allowed to sync against the enterprise Exchange server.



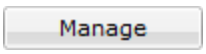
Under certain circumstances, you may need to provide an exception to the Secure Email Access filter and allow select users to sync devices that have not been configured or enrolled into MobiControl to connect with Exchange ActiveSync. To do this, simply add the username along with the number of devices they are allowed to connect to Exchange in the exceptions window. MobiControl will automatically allow the connection until the unique device count is exceeded.



A full list of devices that have passed security and been allowed to connect to the Exchange server can be seen under the Manage Authorized Devices button. This provides the ability to remove old devices and blocked devices.

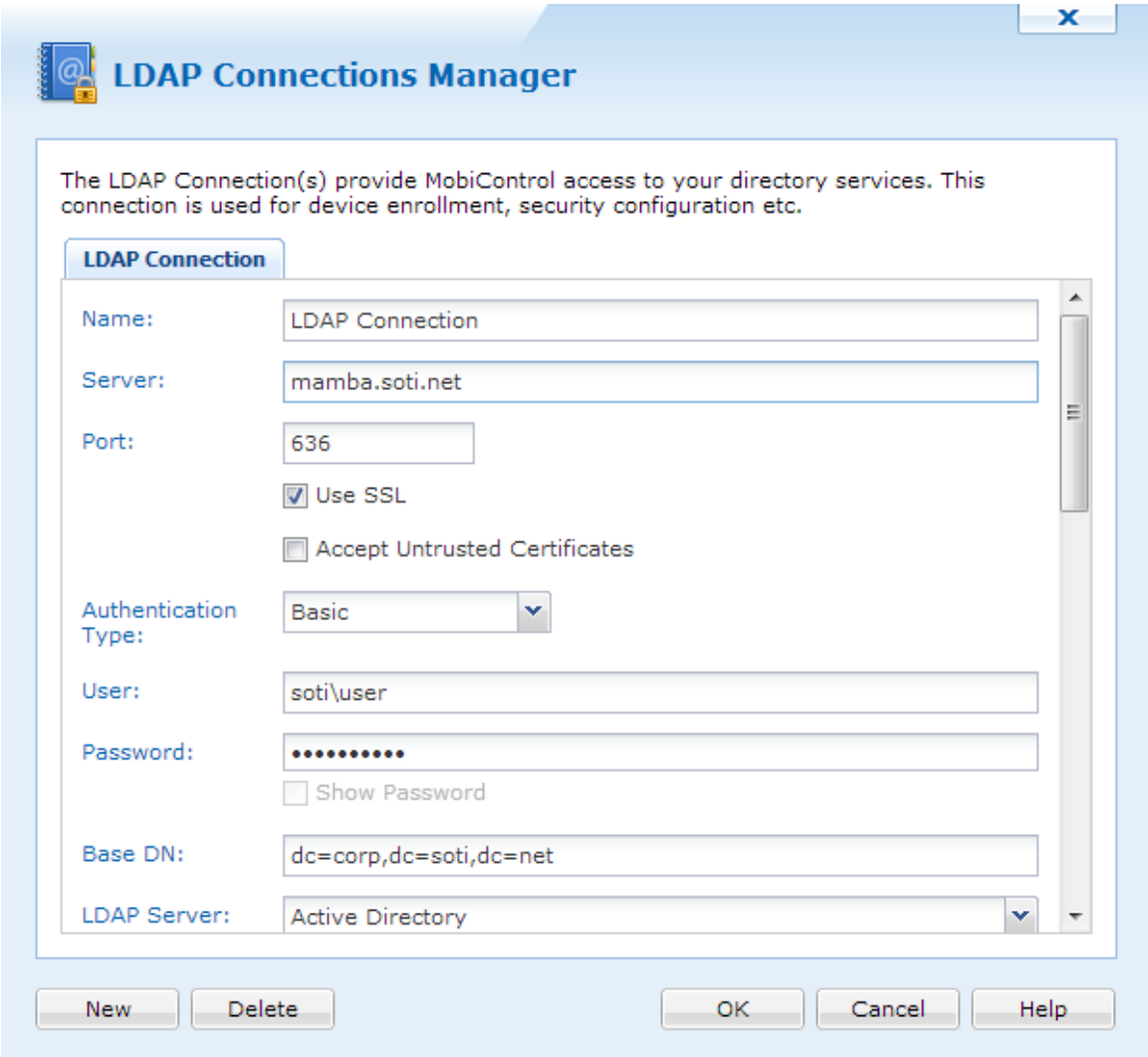
LDAP Connections Manager

The LDAP Connections Manager allows us to create custom connections to Active Directory, Open Directory, Domino, and other LDAP servers. We can create multiple connections so that we can have different connections for different sections of MobiControl. These sections include the Web Console security, Windows Mobile authentication, and Add Device Rules for iOS and Android.

There are multiple ways to reach the LDAP Connections Manager. One would be from an Add Device Rule, the next would be from the Console security, and anywhere else we can select a LDAP connection. Clicking 

in any of these sections will bring the manager up.

The other way is to go to the All Devices Tab, then clicking the bottom Servers tab. Once there, we can click the configuration button for LDAP Connections.



LDAP Connections Manager

If it's the first time opening up the LDAP Connections Manager, a new form will show. Here we can enter the connection settings for the LDAP server.

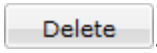
Section	Description
Name	LDAP Connection name, for reference only
Server	LDAP Server's hostname or its IP address
Port	LDAP Server connection port, default is 386, in case of using SSL, the port is 636. The port can be any value if it matches server's settings
Use SSL	If checked off, MobiControl secures the LDAP communication over a Secure Sockets Layer (SSL) tunnel
Accept Untrusted Certificates	This option allows SSL connections to use Untrusted Certification which in most cases is a self-

Section	Description
	signed CA root certificate. It's not recommended to enable this in a production environment.
Authentication Type	This option defines how to make a connection to the server and it should match to the server's settings. It should be one of the three: Anonymous, Basic, Negotiate **Anonymous:** Indicates that the connection should be made without passing credentials **Basic:** Indicates that basic authentication should be used on the connection **Negotiate:**Indicates that Microsoft Negotiate authentication should be used on the connection.
User	The user name used for binding to the connection when the authentication Type is Basic or Negotiate
Password	The password of the binding user
Base DN (Distinguished Name)	The top level of the LDAP directory tree is the base, referred to as the "base DN". This option is to define the highest level of the LDAP search scope. a.k.a. RootContainer
LDAP Server	This defines the LDAP server type. We can select Active Directory, Open Directory, Domino, or other. The server type will decide what default search attributes will be used.

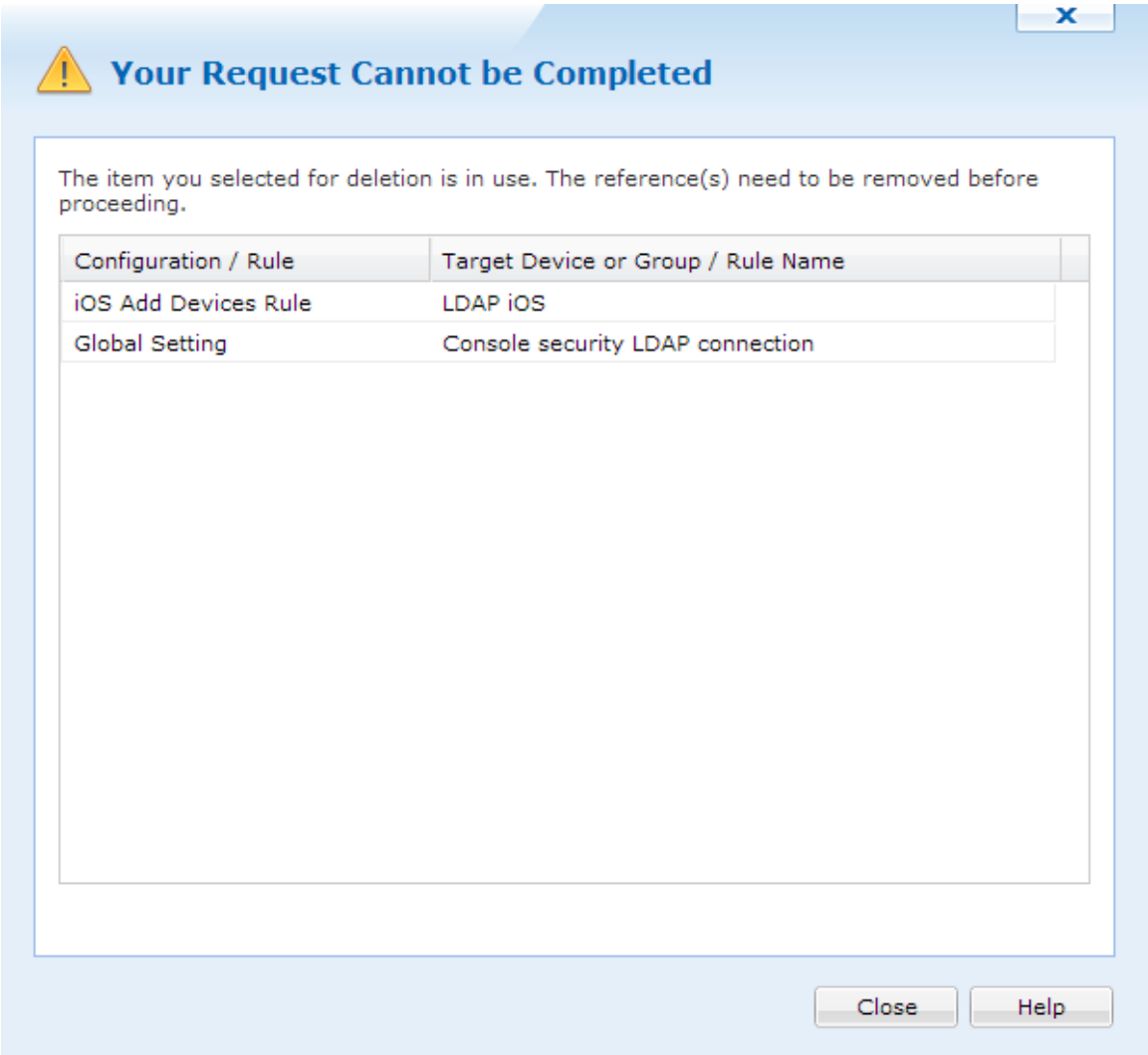
After setting up the connection for the LDAP server, we can configure the search attributes.

Click each title below to expand a list of search attributes:

- **General Attributes**
- **Group Attributes**
- **User Attributes**

If a LDAP connection is not needed anymore, click 

. If a LDAP connection is used in anywhere, clicking Delete will result in the error below:



LDAP Connection Delete Warning

MobiControl will show all configurations / rules where this connection is used in. It will also say the name of the target device or group / rule name. To successfully delete the connection, we would have to go through the list to make sure that this connection is not used anymore.

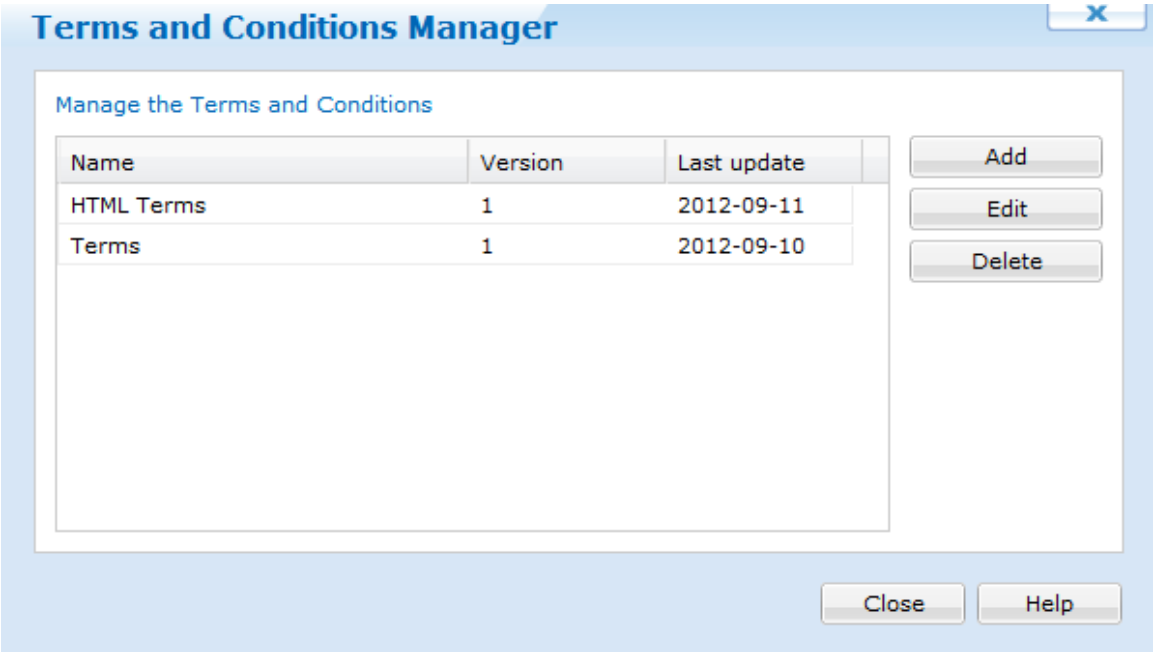
After all configurations are done, click OK to save and close the LDAP Connections Manager.

Terms and Conditions

The terms and conditions page allows us to send terms and conditions to devices. Users must accept these terms before they are able to enroll their device to MobiControl. If they do not accept the terms and conditions, the device will not connect.

There are two ways to manage terms and conditions. One is when creating a new Add device rule, and the other is from the servers tab on the Web Console.

When we manage terms and conditions we will see the following manager:



Terms and Conditions Manager

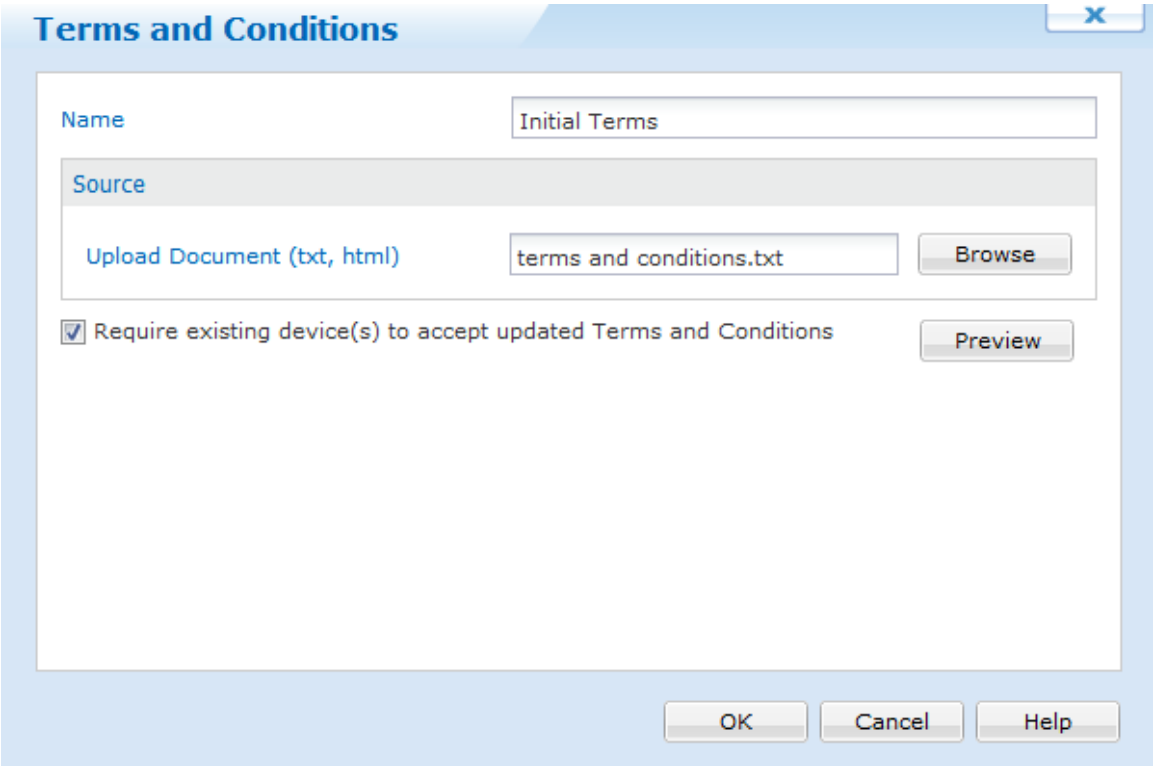
Here, we are able to add a entry with the 

button. When the add button is clicked, a prompt will display asking for the name and the source of the Terms and Conditions. MobiControl accepts either a plain text file (UNICODE) or a HTML file.
Clicking "Require existing devices(s) to accept the updated Terms and Conditions" ensures that devices that are already enrolled, accept the terms.

When uploading HTML files, MobiControl supports light weighted HTML. Here is the list of tags that we are able to use:

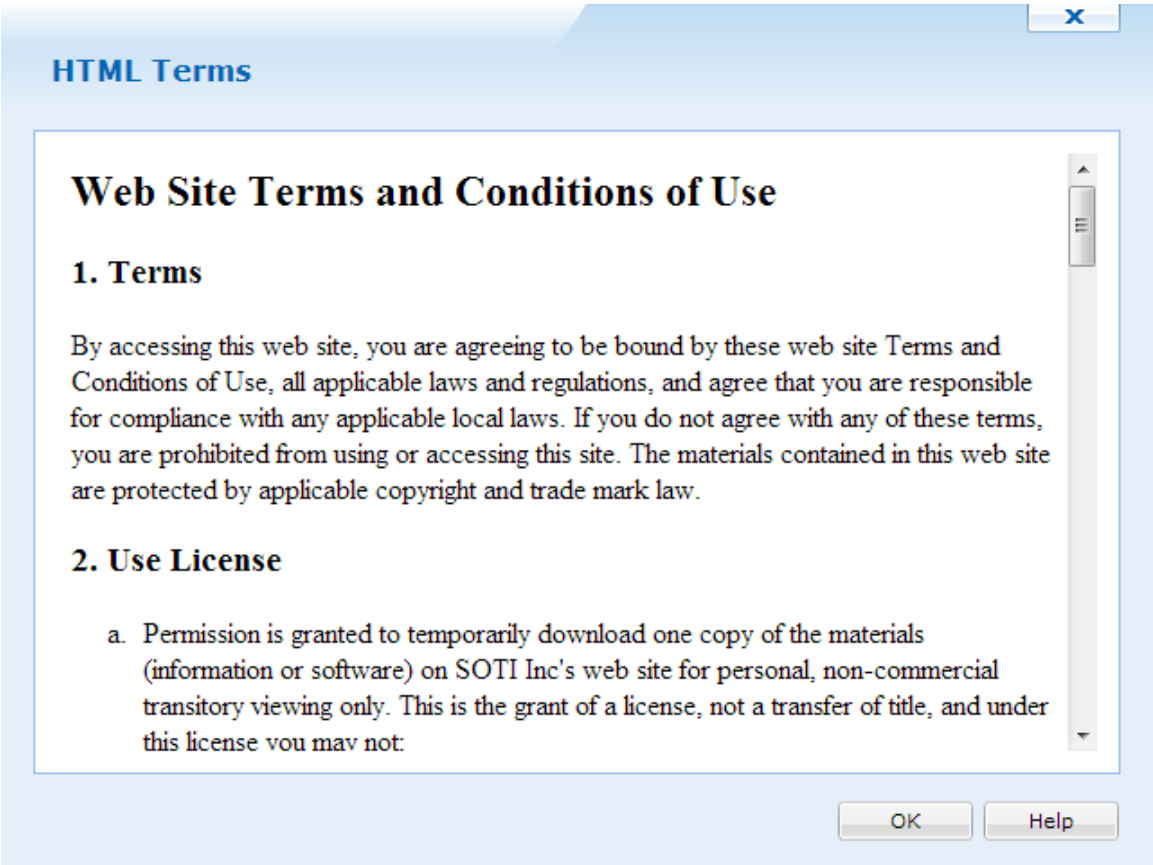
- <a> (supports attribute "href")
- <b>
- <big>
- <blockquote>
-
- <cite>
- <dfn>
-
-
- <font> (supports attributes "color" and "face")
- <i>
- <p>
- <small>
-
- <sub>

- <sup>
- <tt>
- <u>



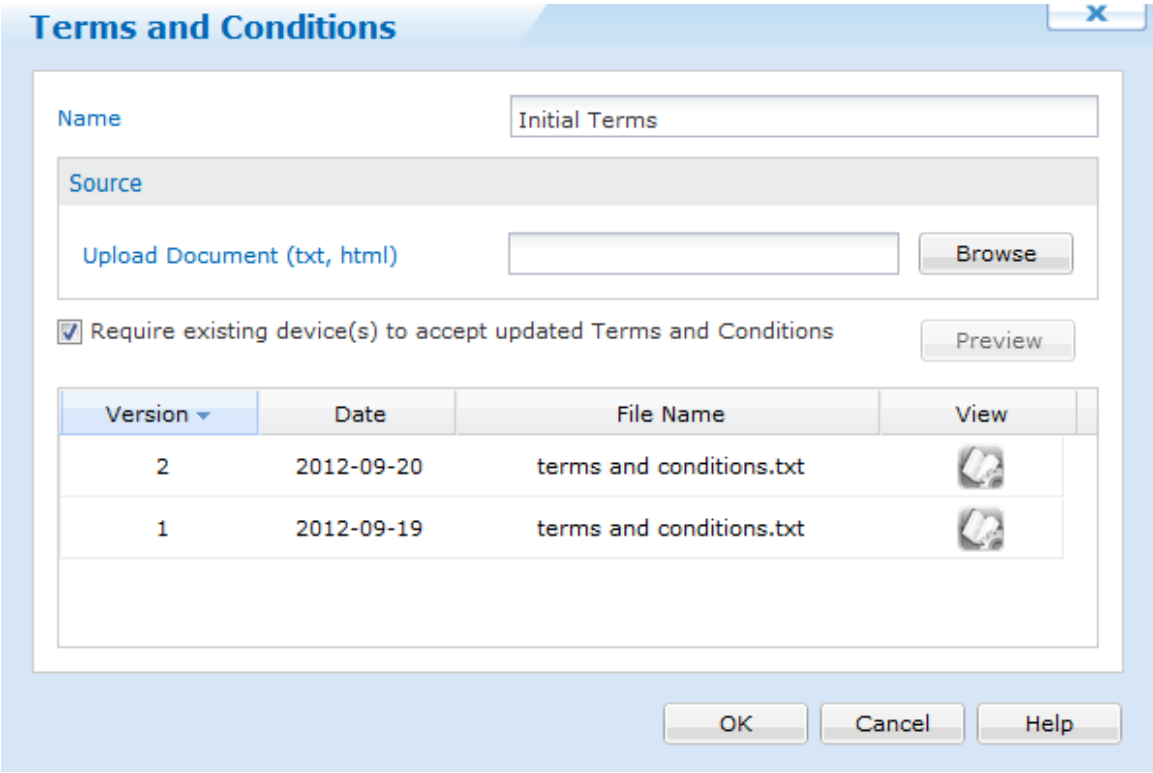
Adding new Terms and Conditions

Clicking Preview will allow us to see the terms and conditions.



Adding new Terms and Conditions

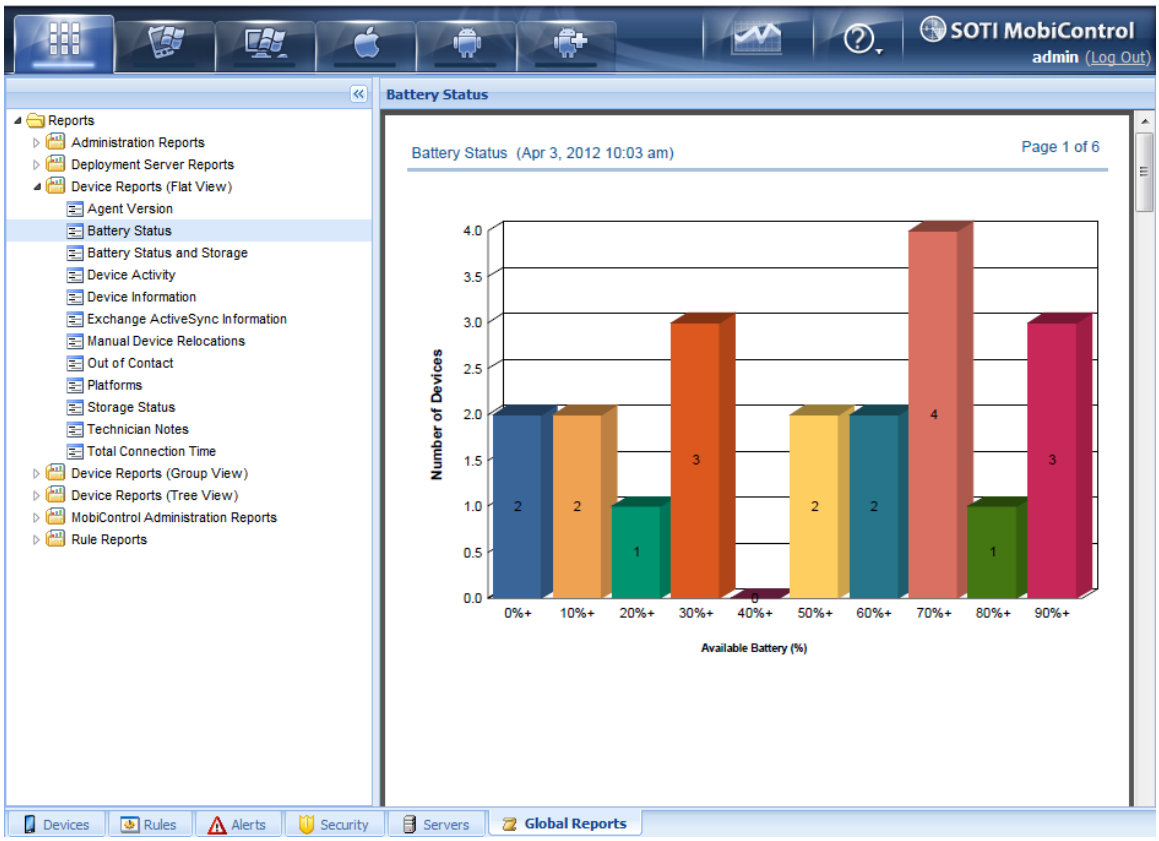
With the Edit button, we can upload an updated Terms and Condition file for that item. When this happens, the version number of the Terms and Condition is increased by 1.



Edit Terms and Conditions

Reports View

MobiControl includes an advanced reporting engine—Crystal Reports—that gives detailed information about all aspects of system operation. The product includes a set of canned reports that provide information about key areas of system operation. Reports can also be customized as well as new reports can be created and added to the system as needed.



MobiControl Manager Reports view (tab)

The MobiControl Web Console allows you to generate Reports based on the Devices Operating System (OS). Some Reports are specific to the OS Tab that has been selected. For detailed information on the Reports available please see the specific Reports that can be created below:

Report Types

The following reports are included with MobiControl:

- A **deployment server activity report** is a detailed report for deployment server activity over a specified time period.
- A **deployment rule report** is a detailed report of deployment rules and all devices.
- A **Battery and Storage Report** is a detailed report of the battery and storage of the selected devices.
- A **Cellular Signal Strength Data Report** is a detailed report of the cellular signal strength of the selected devices.
- A **deployment rule summary report** is about deployment rule exceptions, showing how many devices have executed the rule successfully, are pending, or have encountered an error.
- A **Deployment Server activity report** is a detailed report of Deployment Server activity over a specified time period.
- A **device activity report** provides information about the device activity during a specific time period.
- A **device custom data report** provides information about devices with the custom data values of selected custom data fields.
- A **device note report** provides information about the notes for your devices.
- A **device package report** provides information about packages installed on your device.
- A **device program report** provides information about all the programs installed on your devices.
- A **device relocation rule report** provides information about all the relocation rules for your devices.
- An **out of contact devices report** provides information about devices that have not connected to the system since the specified date.
- A **package deployment report** provides information about package deployment.
- A **Location Collected Data Report** is a detailed report of the location data collected for the devices.
- A **Connectivity Information Report** is a detailed report regarding device's connectivity.
- A **Device Tree Report** provides information about the device tree structure.
- A **Device Tree with Virtual Groups Report** provides information about the device tree structure along with the virtual groups.
- A **Log Information Report** provides information about the device logs.
- A **Phone Number Report** provides information about the phone number of devices.
- A **Alert Summary Report** provides summary of the alerts.
- A **deployment rule report** is a detailed report of deployment rules and all devices.
- A **Geofence Report** provides detailed report based on the Geofence.
- A **Uninstalled Mandatory Applications Report** provides information about the mandatory application not installed on the devices.
- And many more.

Generating a Report

1. In MobiControl Manager, select the Reports view (tab).
2. Select a report in the left pane of the Reports view (tab).
3. Click the **Generate Report** button.

4. For some reports, a window will appear requesting additional parameters (e.g. time period) that may be required.

Saving a Report

1. Generate a report.
2. On the report screen, click the **Export Report** button. (It is the first icon in the toolbar, beside the **Print Report** button.)
3. Select the desired file type. Available file types are:
    - Adobe PDF (`.pdf`)
    - Crystal Reports (`.rpt`)
    - HTML 3.2/4.0 (`.html`)
    - MS Excel 97-2000 (`.xls`) or Data only (`.xls`)
    - MS Word editable RTF (`.rtf`)
    - ODBC
    - Record-style (columns of values with or without spaces) (`.rec`)
    - Report definition (`.txt`)
    - Rich text format (`.rtf`)
    - Comma-separated values (`.csv`)
    - Tab-separated text (`.ttx`)
    - Text (`.txt`)
    - XML (`.xml`).
4. Select the location to which you want to export the report. The options available are:
    - Application
    - Disk file
    - Exchange folder
    - Lotus Domino
    - Lotus Domino Mail
    - MAPI (Messaging Application Programming Interface)

Printing a Report

1. Generate a report.
2. On the report screen, click the **Print Report** button. (It is the second icon in the toolbar, beside the **Export Report** button.)
3. The print menu will pop up. Select the desired printer and the report will be printed there.

Generating Custom Reports

It is possible to create custom report files on any available statistic you desire. The Deployment Server database is a standard SQL database and can be queried by writing a custom query. Also, it is possible to create additional reports that are built into MobiControl. For more details, please contact us.

Other Tools

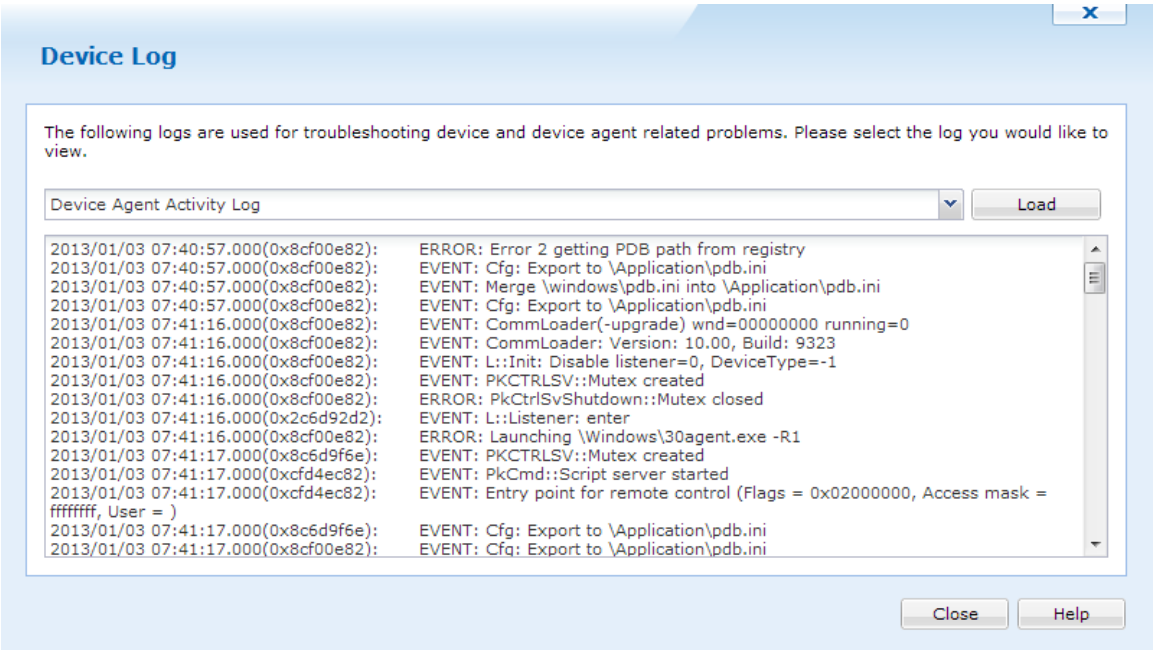
These other tools are available through the toolbar:

- The **Stop Loading** button stops the report generation process
- **Refresh** regenerates the report. If parameters were required to generate the original report (e.g. time period), a window will appear requesting the additional parameters
- The **Search Text** button searches the body of the report for a specified text string
- The **View Zoom** field allows the user to select view magnification, page width, and whole page views

Device Logs

If some devices are experiencing issues with MobiControl, we can view the log file of the device directly from the Web Console. This offers a convenient way to troubleshoot devices.

To do this, we right click any online Windows Mobile, Windows Desktop, or Android device, go to **Actions** and then **View Log File**.



Device Logs

When the device log window appears, we can select what kind of log we wish to view from the drop down menu. When the type of log is selected, click **Load** to show the log.

Windows Mobile devices can load the Device Agent Activity Log, Device Agent Installation Log and the Device Security Policy Log.

Windows Desktop devices can load the Device Agent Activity Log.

Android Devices can load the Device Agent Activity Log.

Location Services

MobiControl's Location Services provides the ability to locate and track mobile devices that are equipped with a GPS receiver that is internal or external to the unit. In order to locate a device, the GPS must be enabled and correctly configured on your device. The GPS determines the current location based on its position relative to orbiting satellites. In order for this to happen, the device requires a clear view of the sky. Determining location may not be possible if the device is inside buildings or has an obstructed view of the sky.

You can activate Location Services for a device in MobiControl by right- clicking on a device and selecting the **Location Services** option from the menu. The first time you select an option from the Location Services menu for a device, it will automatically use the next available license. If there are no more licenses available, you will be notified to contact SOTI for information on acquiring additional licenses for Location Services.

Please See the "Contact Us" page to contact us for more details on acquiring additional licensing.

NOTES:

- When using Location Services in MobiControl to track devices, Internet Explorer 7 or higher is required.
- The Current Format for Regional and Language Options on your PC MUST be compatible with Bing Maps. Click here for a list of supported Bing Map control settings.

Configure Windows Mobile / CE Devices

The **Windows Mobile / CE Device** tab enables you to access the devices connected to the deployment running a Windows mobile OS. All functions that affect this operating system are performed such as:

- Location Services
- Device Security
- Device Configuration
- Adding a Device
- Distributing software to a device
- Data collection functions
- Alerts

There are five views within the MobiControl web console. The views can be selected using the tabs at the bottom of the MobiControl Manager user interface.

- The **Devices view (tab)** allows users to view information about configured devices, for instance packages installed, device ID, and IP address. The Devices view (tab) also allows users to control and configure devices, for example, to remote control a device or to change a device's name.
- The **Rules view (tab)** allows users to view information about the configured rules. The Rules view (tab) also allows users to configure rules, for instance, create an add devices rule, a deployment rule, a file sync rule, an enable rule, or a disable rule.

- The **Packages view (tab)** allows users to view information about packages, for instance the packages currently configured or a list of devices onto which a certain package has been installed. The Packages view (tab) also allows users to configure package-related information, for example to add or delete packages.
- The **Reports view (tab)** provides users with a set of reports containing detailed information about the operation of the system. Provided reports include: deployment rule execution summary report, device configuration rule execution summary report, and device activity report.

The Windows Mobile / CE Device tab also allows you to reset passwords and block/unblock Exchange access on a group level. These options can be viewed when you right click a device group and go to **Action**.

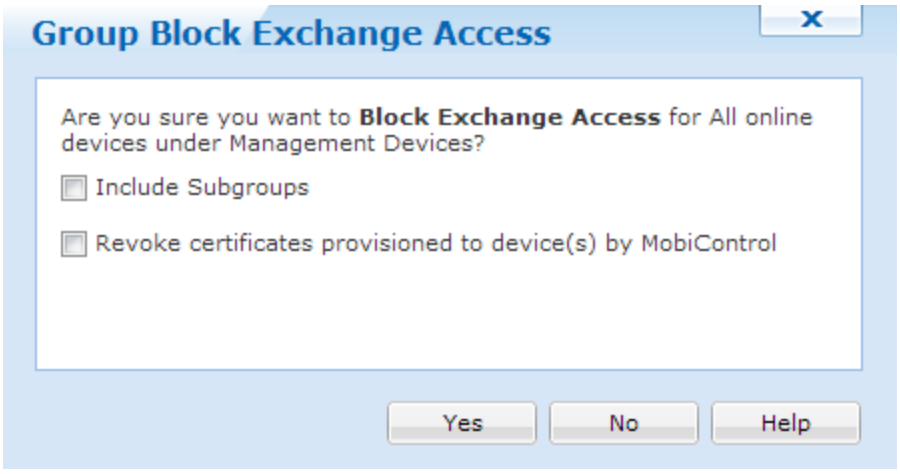
Reset Passcode

Reset Passcode allows you to reset the passcode for every device in the group. This can be useful when you move multiple devices into a specific group for resetting passcodes.

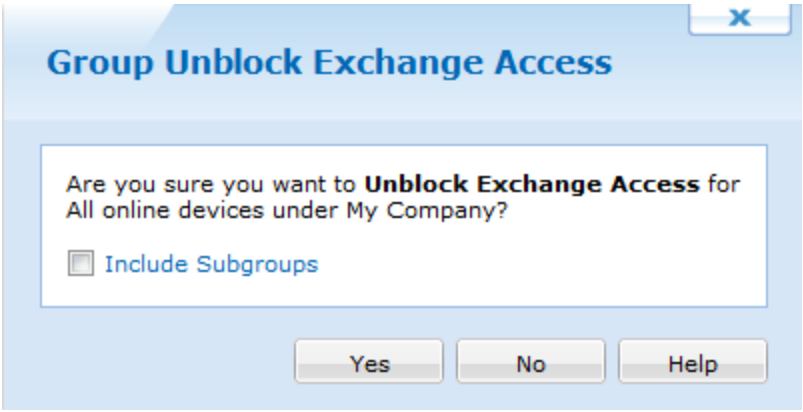
Group Reset Passcode

Block/Unblock Exchange Access

Using these options allow you to block and unblock Exchange access to every device in the group.



Blocking Exchange Access



Unblocking Exchange Access

Windows Mobile Devices Tab

The Devices view (tab) is the main view into the status of the devices in the MobiControl system.

Device Tree

The device tree provides a structured view of the devices in the system. The group structure is easily defined by the user by creating new groups and dragging and dropping devices between groups. Please see the "Device Groups" topic on page 124 for detailed information on groups and virtual groups.

Commonly-reported device information can be easily referenced in the device tree window by right-clicking in any open space in the device tree window and selecting the information that you would like to see displayed.

Devices are added to the system by defining an add device rule and creating a MobiControl Device Agent that is installed on the device. Please see the "Adding Windows Mobile Devices" topic on page 747 for a detailed explanation of how to add devices to MobiControl.

Info Panel

The Info panel provides detailed status information about the group or device that is selected in the device tree. When a group is selected, the displayed information includes the number of subgroups and how many unique, online, offline, or disabled devices are in the group. For devices, the displayed information includes device ID, IP address, battery and memory status. In addition, custom data retrieved from your devices may also be displayed. Please see the "Windows Mobile Custom Data" topic on page 700 for detailed information about configuring custom data retrieval.

The content displayed in this panel is stored in the MobiControl database. This information is refreshed when a device establishes a new connection to the MobiControl Deployment Server, and when you click **Refresh** or press F5 on this tab.

Logs Panel

The Logs panel provides a listing of the events occurring in the MobiControl system. This listing is filtered based on the group or device that is selected in the device tree. If only one device is selected, only the events related to that device are displayed. If a group is selected, events for the group and all the devices that belong to that group are displayed.

You have the option to show or hide logging, adjust the maximum number of logs displayed, and the frequency with which the Manager should refresh the log view.

Update Schedule Panel

The Update Schedule panel lists the dates and times when the device is programmed to query the MobiControl system to check for updates. By default, a device will also check for updates whenever it connects to the MobiControl system. Please see the "Windows Mobile Device Update Schedule" topic on page 722 for more information.

Installed Applications Panel

The Programs panel lists the applications that are installed on the device that is selected in the device tree.

Rules Assigned Panel

The Rules Assigned panel lists the deployment and file sync rules assigned to the group or device that is selected in the device tree. Rules are inherited from parent groups; a rule will apply to a device if it belongs to group to which the rule has been assigned.

The assignment of rules to groups provides a flexible and convenient means for easily configuring devices. For example, once you have set up your rules for software or data distribution, you can automatically provision your devices by simply adding them to the appropriate group within the device tree. Please see the "Web Rules Tab" topic on page 575 for information on creating deployment rules and file sync rules.

Notes Panel

The Notes panel lists the notes that are associated with the selected device. If a group is selected in the device tree, all the notes for the devices that belong to the group are listed. Notes are a convenient way to maintain information about the device such as trouble tickets. Please see the "Device Notes" topic on page 1384 for information on creating device notes.

Packages Panel

The Packages panel lists the packages that are configured on the device that is selected in the device tree. The assignment of packages is directly based on the assigned rules. This panel provides a status column which indicates the state of the package for that device. For example, the status "Pending" indicates that the package has been queued and its installation on the device is pending.

You can force the re-installation of a package on a given device by right-clicking on the package in the Package Panel and selecting **Force Package Reinstall on Next Schedule** or **Force Package Reinstall Now.**

Collected Data Panel

The Data Collection Panel allows you to view the collected historical data for a set of devices. By creating a Data Collection Rule you will be able to specify which items to collect data from, how often to collect them, and when to upload the collected data to the server. Please see the Creating Data Collection Rules page for information on creating Data Collection.

Location Panel

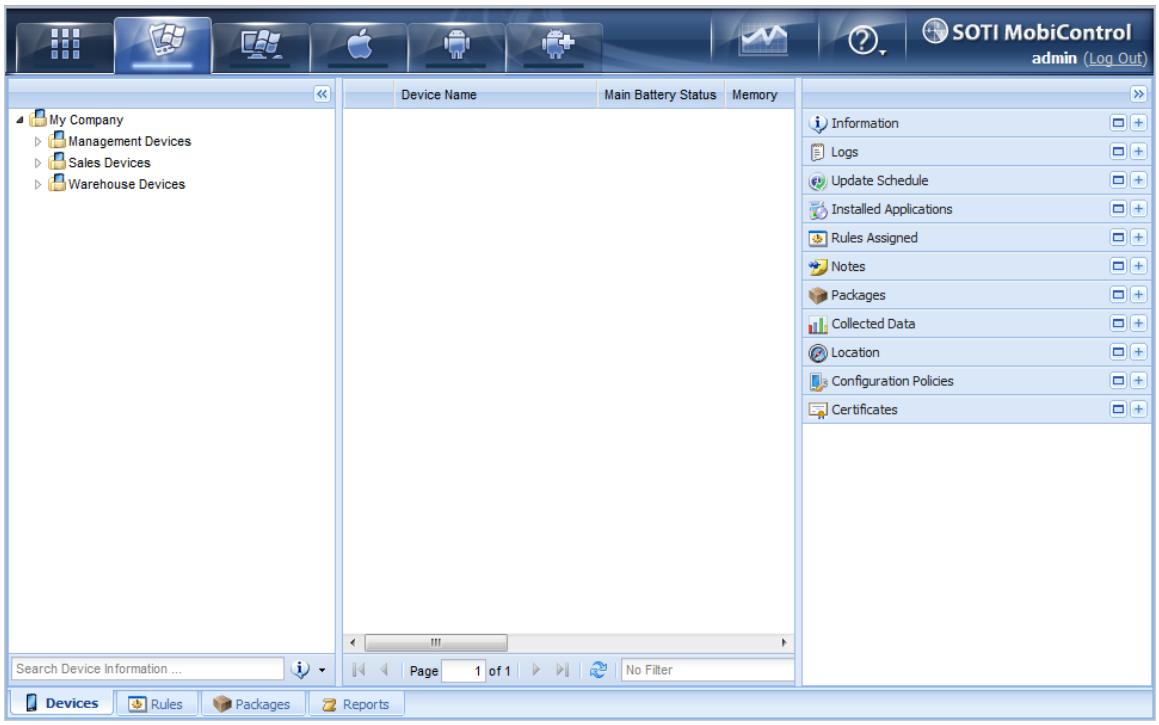
The Location Panel gives the ability to locate, track and gather information on the movement of your GPS enabled devices, no matter where they are in the world which is powered by Microsoft's Bing maps technology. Whether you need to confirm the current location of a particular field-worker, track the progress of an important shipment or collect historical information on the movement of a group of devices or vehicles in order to analyze performance, MobiControl's Location Services can help. Please see the Location Services page for more information.

Configuration Policies Panel

The Configuration Policies panel lists all policies that are currently configured on the device. It also lists where these policies are inherited from. This allows us to have a quick look to see what configurations are currently on devices.

Certificates Panel

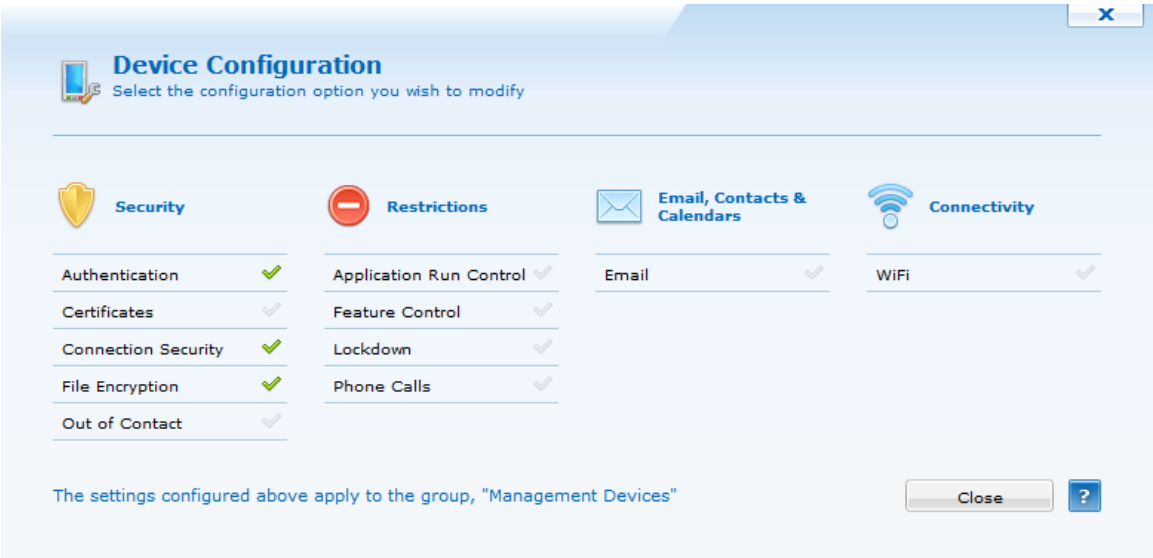
The Certificates Panel lists all certificates that MobiControl sent to devices. Certificates can range from email to WiFi authentication.



MobiControl Devices Tab Devices view (tab)

Windows Mobile Device Configuration

MobiControl offers several device security options ranging from password authentication, user interface lockdown (also known as "kiosk"), and the ability to configure the device to automatically react to security threats such as repeated failed login attempts, even if the device is out-of-contact or in an offline state.



MobiControl Device Configuration dialog box

MobiControl's device configuration provides powerful features for securing devices and mobile data, while maximizing usability and making security implementation easy, efficient and cost-effective. Salient features of MobiControl's device configuration include:

- Over-the-Air (OTA) security policy distribution
- Policies can be assigned at the individual device, group or global level
- Security managed for both online (connected) and offline (disconnected) devices
- Email and WiFi configuration

To access MobiControl's device configuration options, select the device or group of devices for which you want to configure security and then click **Device,** click **Device Configuration.**

Click each heading below to read a brief summary under each section:

Security

Restrictions

Email

Connectivity

NOTE:

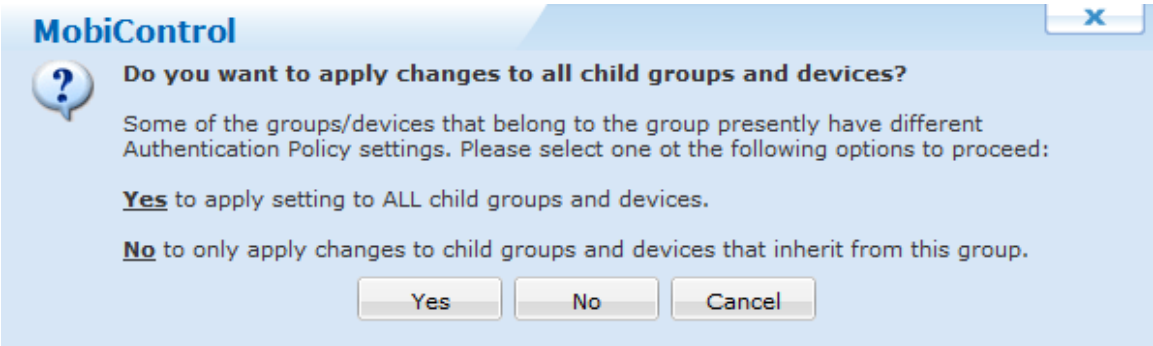
Due to a limitation in the way Windows CE 6.0 handles the pkfsh.log file - The following Device Security and Control Policies will not function properly:

- Application Run Control Policy
- Taskbar Lockdown
- Device Feature Control Policy
- File Encryption
- Phone Call Policy

Configuration Override Settings

Override settings allows you to create unique configuration settings at the current level which you have selected. This will override the settings that the device or group was previously inheriting from the parent group.

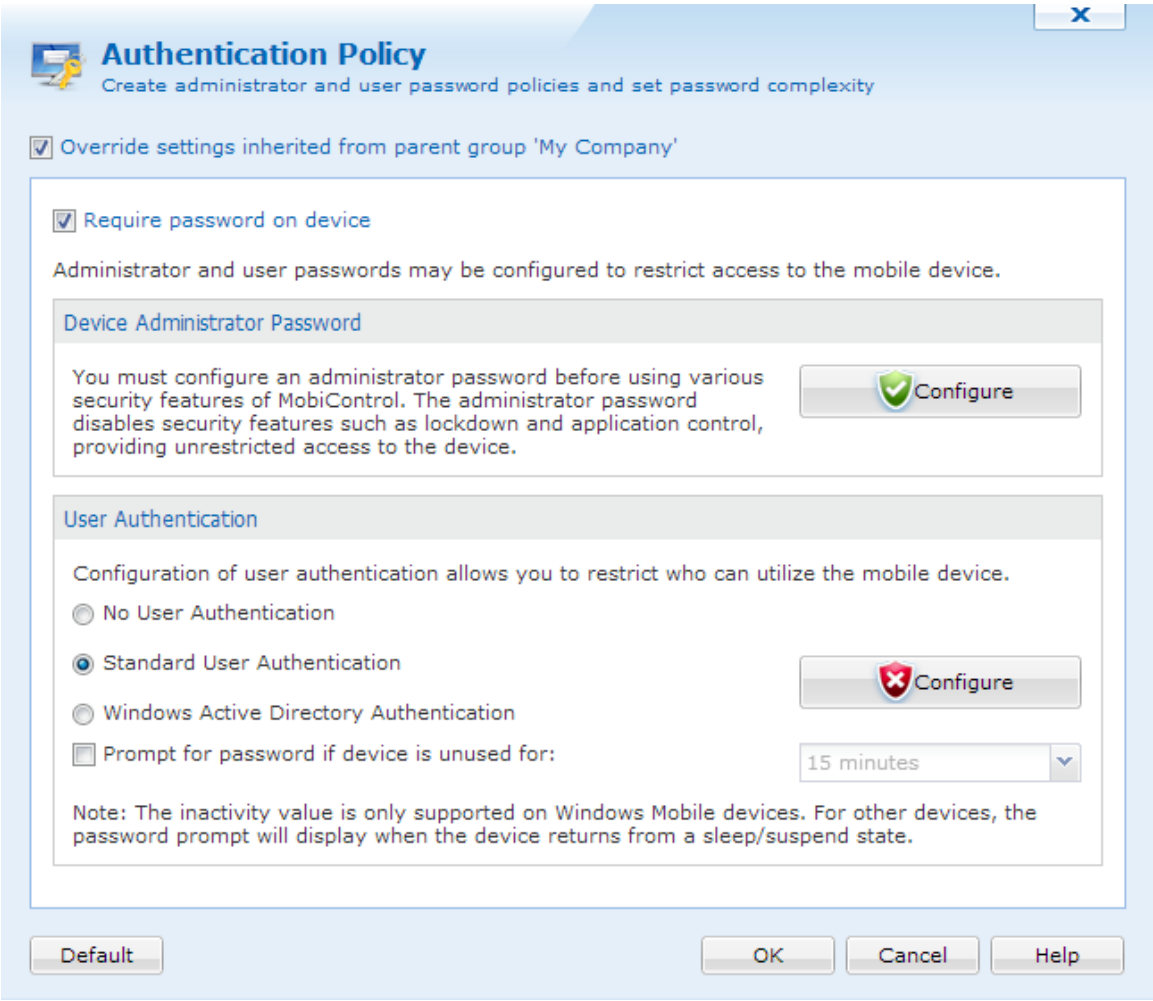
If the configuration settings are different at any sublevel (be it device or subgroup) then a confirmation prompt will allow you to choose whether the current setting(s) should be applied to all sub devices and groups or only the level that inherit configurations from this group.



Windows Mobile Authentication

The Authentication Policy option in the **MobiControl Security Center** dialog box allows administrators to set up device-side, password-based user authentication. This tab also allows administrators to create authentication actions, device-side scripts that execute when user authentication either succeeds or fails. For example, an administrator might create a script that locks the device for 30 minutes if authentication fails three times in a row.

To enable Authentication Security for a device or group of devices, select **Authentication Policy** from the MobiControl Security Center. (Please see the "Windows Mobile Device Configuration" topic on page 632.)



Device Authentication Configuration dialog box

For assistance with Override Settings Click Here.

Administrators can configure an administrator password and a user password. When the administrator password is entered, the device is unlocked so that the administrator has complete access to the device. When a user password is entered, the user will have access to only those programs that the administrator has configured. An administrator can allow users to run all programs or only specific programs. Please see the "Windows Mobile Device Lockdown" topic on page 667 and "Windows Mobile Application Run Control" topic on page 657 for more details.

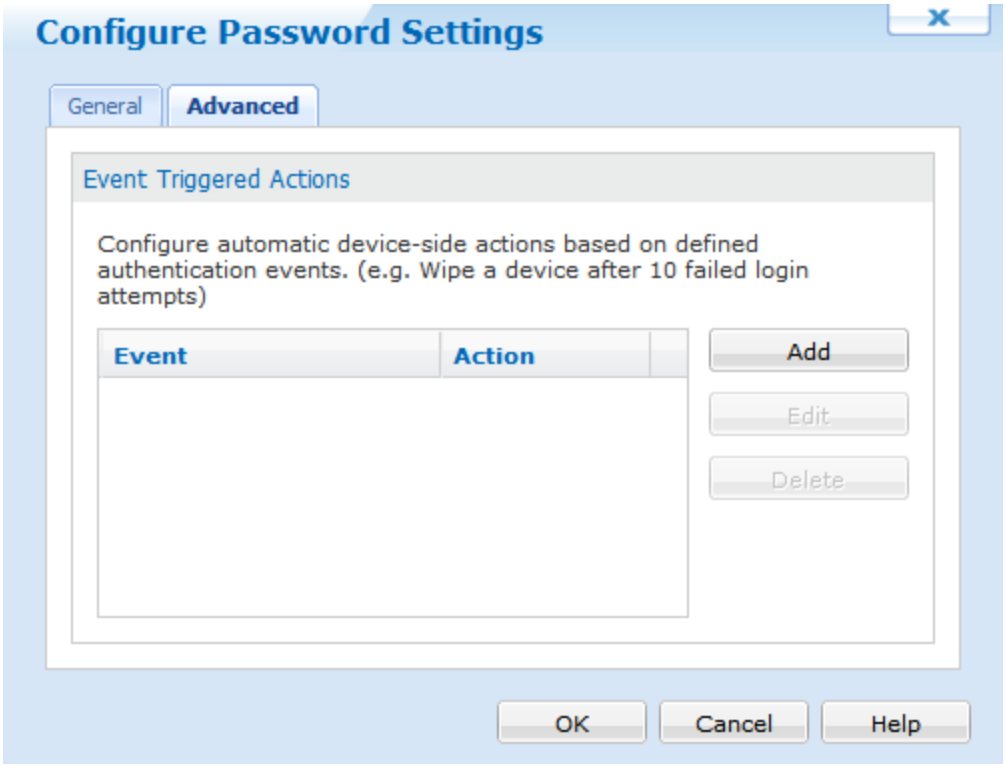
Administrator Password

To specify an administrator password, first ensure that the **Enable Password Authentication** box is checked, and then click the **Configure** button in the administrator password section. This will bring up the dialog box below. Enter the desired password in the two provided text boxes and click **OK**. The configuration of the Administrator password is a prerequisite for all the other security configurations. To get to this screen you must click on the **Options** button, then select **Administrator** and click **OK.**

Administrator Device Password prompt

General tab of the Configure Password Settings dialog box

Administrator Authentication Events and Actions



Advanced tab of the Configure Password Settings dialog box

You can specify actions for administrator events. For example, you may wish to wipe all the data on the device if there are 10 consecutive failed log-in attempts. To create, edit, or remove an action, click on the **Advanced** tab of the **Configure Password Settings** dialog box. To add an action, click the **Add** button. MobiControl will prompt you for the event that will trigger the new action. This event can be either a successful login or a certain number of failed attempts. After you have made your selection, click **OK** to bring up the **Action Configuration** dialog box. Please see the Windows Mobile Configuring Event Scripts page for more details. To edit an existing action, select the action from the list and click **Edit.** This will bring up a small menu that lets you choose whether to edit the event that triggers the action or the action itself. To delete an action, select it from the list and click **Delete.**

User Password and Policy

To specify a user password, first ensure that the **Enable Password Authentication** box is checked, and then click the **Configure** button in the user password section. You must specify an administrator password before you can specify a user password. MobiControl provides a dialog box similar to that used for administrator passwords. The **User Password** dialog box also allows you to specify a password policy.

When you have configured a password or chosen Active Directory-based authentication, MobiControl will queue up the delivery of packages and settings targeted to the device, and only install the packages and settings once the user has been authenticated.

A user password policy specifies whether or not users can change their passwords and what minimum complexity requirements those passwords must meet (if any). Complexity requirements can include minimum length and uppercase, lowercase, numeric, and special character requirements.

There are four options with regard to user authentication:

User Device Passwo

Field Name	Description
No Authentication	No user authentication is set. Any user can access the mobile device without any authentication.
Standard User Authentication	The administrator must specify a password for the user to enter to access the mobile device. This password is unique to MobiControl and can be controlled only with MobiControl.
Windows Active Directory Authentication	MobiControl now enforces Active Directory authentication for the users on their mobile devices. The end-user must enter their Active Directory credentials when trying to logon to the device. If the administrator changes their Active Directory profile, the changes are propagated down to the mobile device with MobiControl.
Prompt for password if device is unused for	This option can be used with both Standard and Windows Active Directory Authentication. When this option is enabled, if the mobile device is unused for the specified period of time, then the user will be prompted to enter the password again and authenticate their identity. The time value only works with Windows Mobile 5 (or greater) devices. On all other platforms, enabling this setting will cause the device to prompt for a password after device emerges from sleep mode. **NOTE:** It is necessary for the device to be soft reset (i.e. powered off and back on) for the change to take effect.

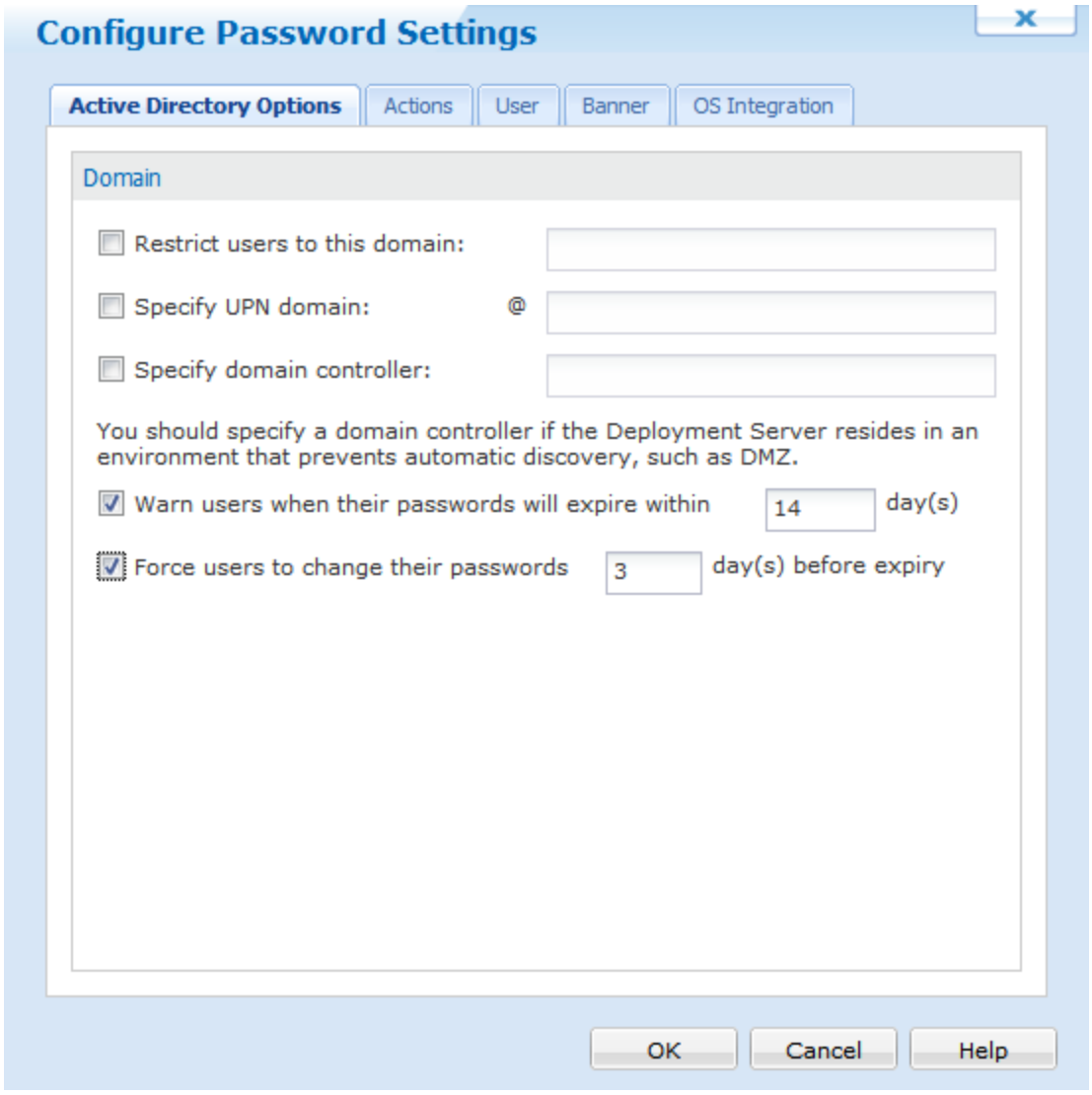
User Password Settings

When Standard Authentication is selected, a password is specified for the user and complexity requirements for the user password is enforced, if the user password does not meet the complexity requirements, MobiControl will prompt you to change the user password within MobiControl Manager.

User Password Settings dialog box

Windows Active Directory Authentication

When you choose Windows Active Directory-based authentication, the MobiControl Agent will directly authenticate the user's credentials with the Active Directory server associated with the configured domain. The Active Directory Server requires SSL security to be enabled, and ports 636 and 443 to be open between the Deployment Server and Active Directory Server. If your organization is using a non-standard port to communicate over SSL with your Active Directory Server, then a colon " : " must be used to indicate the port being used in the **Specify domain controller** field (i.e. `Mydomain.com:1234`). If no other connections are available, the MobiControl agent will attempt to initiate a data connection if one has already been configured.



Configure Active Directory Settings dialog box

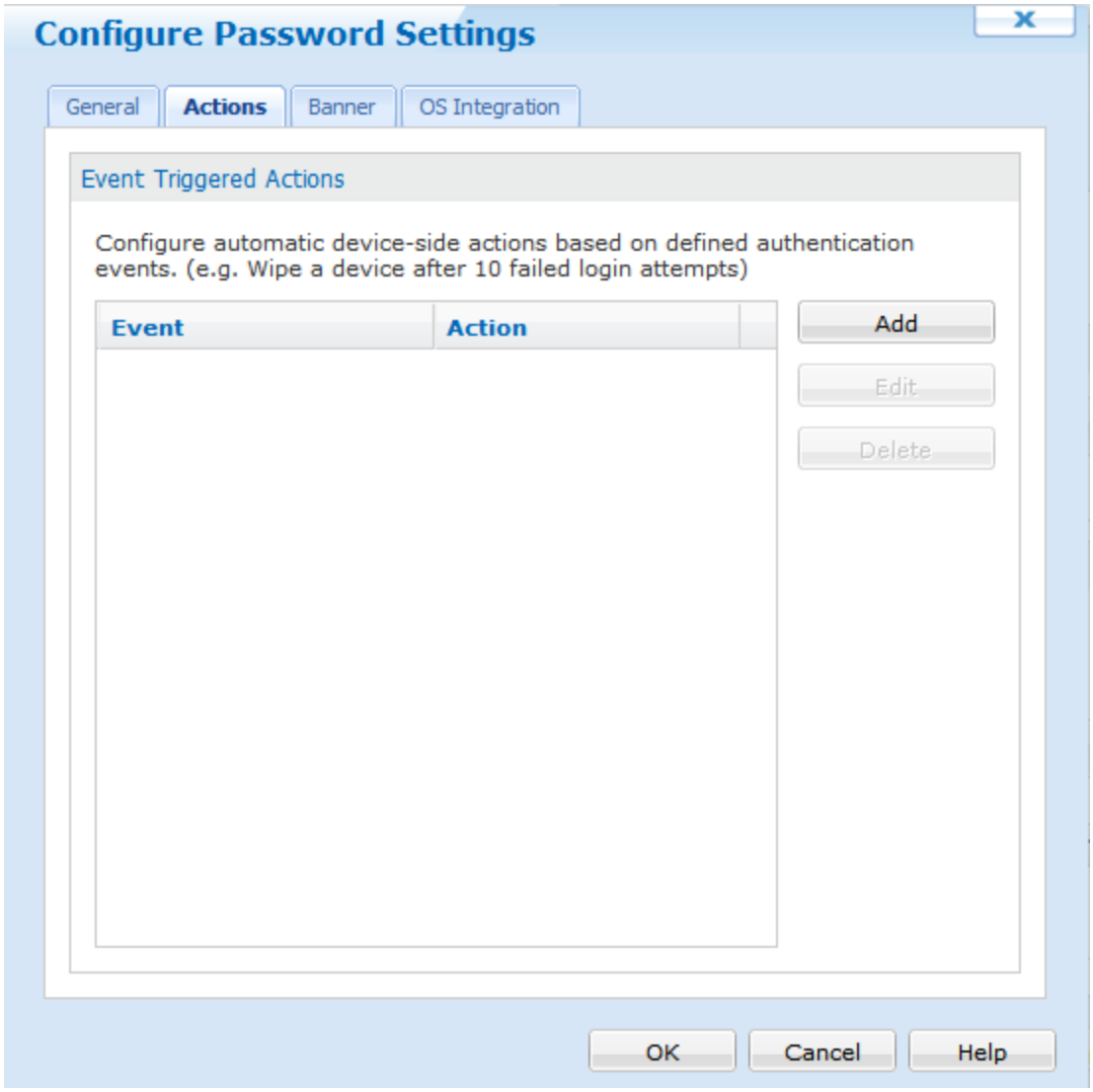
Configure Active Directory Settings dialog box

Field Name	Description
Restrict users to this domain	Select this option to force the user to be authenticated against a particular domain controller. When the domain is known ahead of time this option is recommended as it requires the device user to enter less information.
Specify UPN domain	Select this option to specify the domain portion of the UPN (User Principal Name) that should be used to identify users in the Active Directory system. This name typically takes the form of `domain.corp.mycompany.com` or simply `@mycompany.com`.
Specify Domain Controller	This is where you can specify a domain controller to use when your Deployment Server resides in a DMZ (Demilitarized Zone). This is also useful if you have more than one Domain Controller and want to specify a single one.
Warn Users when their	Advises the user that his or her password is about to expire, and requests that he or she changes it

Field Name	Description
password will expire	
Force Users to change their password	Forces the users to change their password before it expires in the Active Directory. This option is especially helpful in case your Deployment Server is located within a DMZ since in that configuration, the Deployment Server is unable to facilitate the password change if the password has already expired.
Allow only a single device user	This option will lock the device to the first user that successfully logs on to the device. Another user will be unable to login and use the device. This option must be selected if you are using Microsoft Exchange ActiveSync, since a Windows Mobile device is only capable of synchronizing with the account of a single user. If you wish to reset which device user is bound to a given device: While the device is online, right-click on it in the device tree, and click **Configure Devices**, then click **Security**, click **Authentication Policy** and click **Configure** to get to the dialog box displayed above. Then, click the **Reset User Binding** button. **NOTE:** When you click the **Reset User Binding** button it will reset the binding instantly, so there is no need to click the **OK** button.
Allow all domain users to log on to the device	Allows for all domain users to log on to the device and use the device This option is suitable only for environments where devices are shared amongst a group of people, and there are no personal settings stored on the device.
Allow users to create a simple authentication password	This option will allow the user to create a simplified password and use this password when trying to log on to the device instead of using their Active Directory password. This option is handy when the Active Directory password for the user is very complex and it is too tedious to enter on the device. Although called "simple," you may force the user to use a password of a given complexity by clicking on the **Policies** button.

User Authentication Events and Actions

You can specify actions for user authentication events. For example, you may wish to wipe all the data on the device if there are 10 consecutive failed log-in attempts. To create, edit, or remove an action, click the **Advanced** tab of the **Configure Password Settings** dialog box. This will bring up the following screen:



Password Settings (Advanced)

Password Settings (Advanced)

Password Settings (Advanced)

To add an action, click the **Add** button. MobiControl will prompt you for the event that will trigger the new action. This event can be either a successful login or a certain number of failed attempts. After you have made your selection, click **OK** to bring up the **Action Configuration** dialog box. Please see the "Configuring Event Scripts" topic on page 251 for further details. To edit an existing action, select the action from the list and click **Edit.** This will bring up a small menu that lets you choose whether to edit the event that triggers the action or the action itself. To delete an action, select it from the list and click **Delete.**

Custom Banner

You have the option of replacing the default banners that appear on your device with custom images (The default dimension is **214x36 Pixels** and the image file must be of .BMP format). Next to the **Login Screen** drop-down menu, click on the **Import** button to browse to the desired .BMP file that you'd like to replace the default banner with. For the **Device Lock Screen** drop-down menu you can do the same. Simply click on the **Import** button to browse to your .BMP file and -once selected- it will be available as an option in the drop-down menu for the **Device Lock Screen** feature.

Operating System Integration

The **Display notification screen when device is locked(Pocket PC only)** check box option configures the device to present clear indication of the device's locked status to users.

Windows Mobile Authentication Plug-in

When the **Integrate with Windows Mobile device authentication subsystem** option is selected, the MobiControl agent is registered with the operating system authentication subsystem, and replaces the standard password prompt with its custom password prompt. This provides maximum security for the device because the password prompt engages immediately on device startup, ensuring the device cannot be accessed without the user first providing the user or administrator password. With this option, the password prompt is automatically re-engaged when the operating system dictates the idle timeout has expired.

This option is only applicable when both an administrator and a user password have been configured and the device is running the Windows Mobile 5 or later operating system. For devices running other operating systems, the password prompt is handled at the application layer and is not driven directly by the operating system. In some cases you may wish to disable this option to avoid the authentication plug-in from conflicting with other third-party security solutions that may be running on the mobile device.

Windows Mobile Certificates

With MobiControl's certificate policy, we are able to install certificates on devices on behalf of authenticated users or devices.

To get here, right click a device/device group, and select Device Configuration. Once the Device Configuration window appears, click **Certificates**.

Here, we are able to upload certificates, or generate new ones based on Templates.

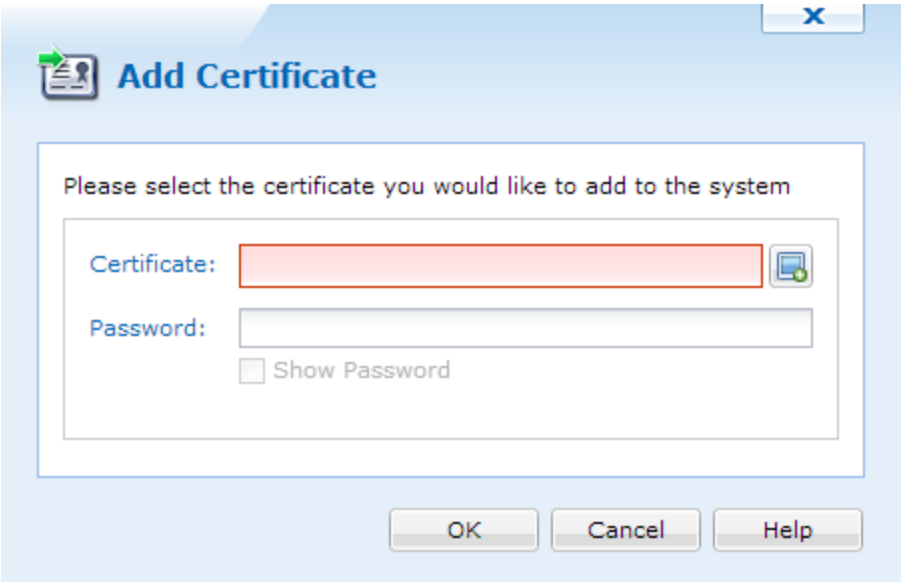
NOTE:

To set up certificate templates, Certificate Authorities must be set up. Please see the Certificate Authorities page for more information.

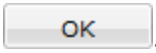
Certificates

Device Configuration - Certificates

When the Certificates window is open, we can upload new certificates by clicking New.



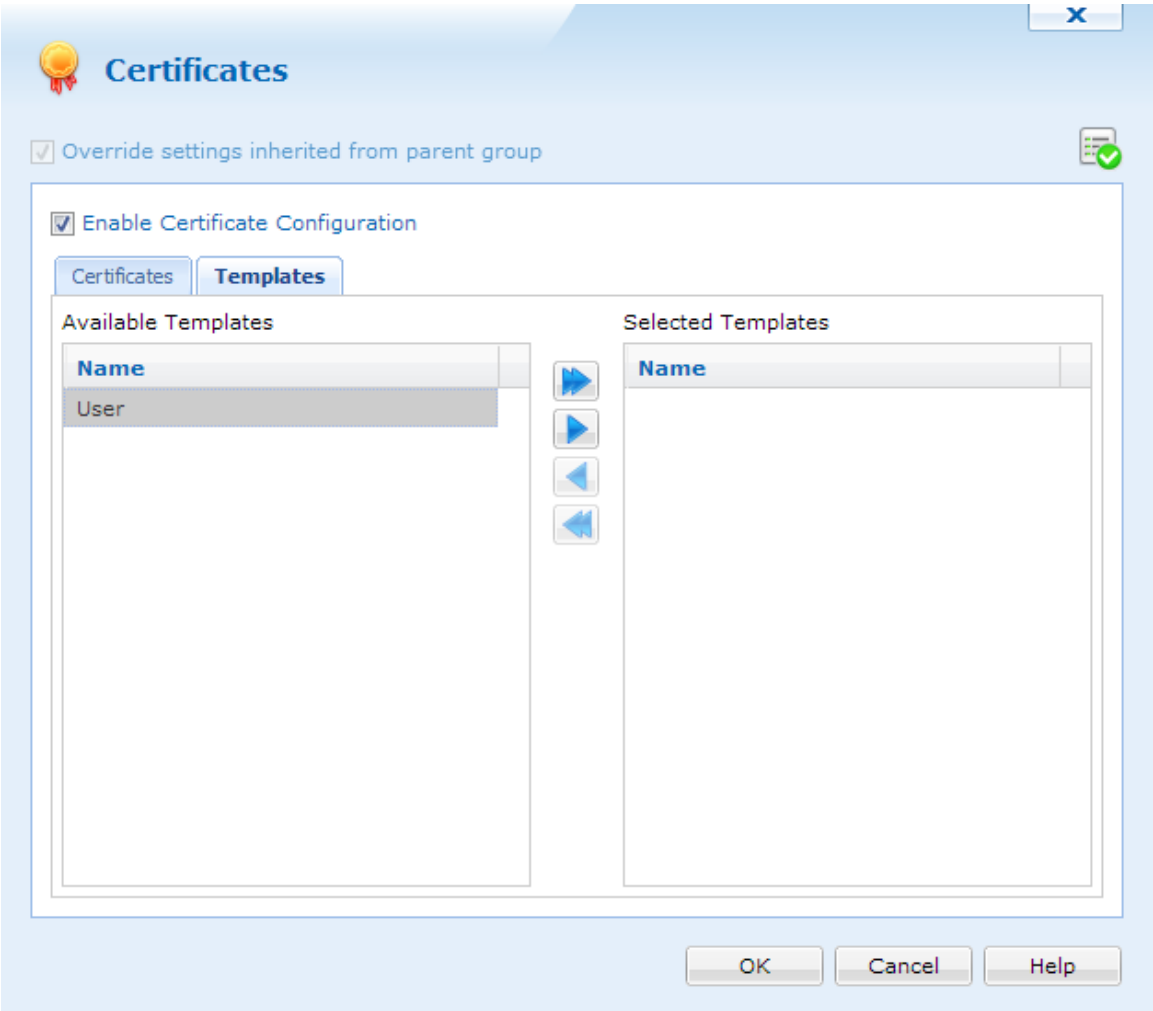
Adding new certificates

Click  to select a certificate. When uploaded, type the password associated with it, and click  .

When the certificate is added, we can select it and click any of the right arrows to move it to the *Select Certificates* panel. This will now install the certificate on the device or device group it is configured for.

Templates

Templates allows MobiControl to request a certificate on behalf of a user or device, and install it. This allows for dynamic certificates.



Selecting Certificate Templates

Certificate Templates are based off the templates configured in Certificate Authorities. Please see the Certificate Authorities page for more information about certificate templates.

When templates are configured, we can select one or many, and move it to the **Selected Template**s panel.

After all certificates have been selected, clicking OK, will close the window and apply the settings.

Windows Mobile Connection Security

To ensure the integrity of the corporate firewall and to provide an additional layer of security for data flowing between the mobile device and the MobiControl Manager(s) and Deployment Server(s) over public networks, SSL Communication Mode is available to provide encrypted communication. When SSL is not enabled MobiControl encrypts all communications using proprietary algorithms. SSL provides the additional benefit of standards-based authentication and encryption security.

To enable SSL communication for a device or group of devices, select **Connection Security Policy** from the MobiControl Security Center. Please see the "Windows Mobile Device Configuration" topic on page 632.)

This dialog box allows you to enable SSL communication for specific devices. For example, one group of devices which are in your warehouse do not need to use SSL, whereas you do want another group of devices that are in the field and communicating over public networks to use SSL.

Configure SSL device settings dialog box

For assistance with Override Settings Click Here.

The dialog box above allows you to specify the means by which you wish to have the MobiControl system deliver the Device Agent's certificate and private key to the device.

NOTE:

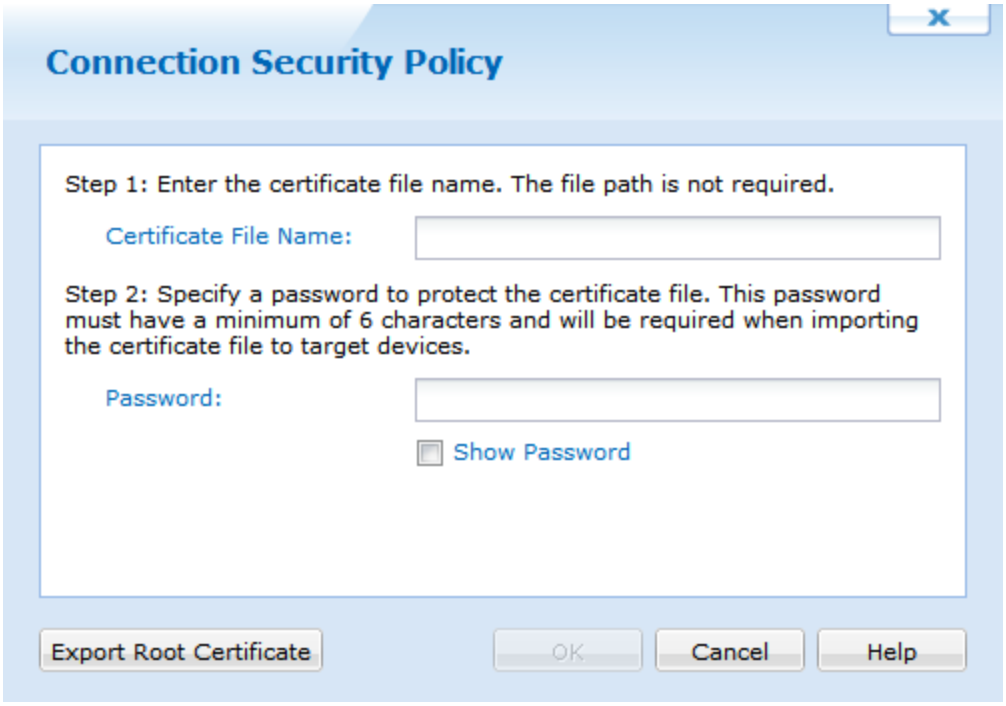
When SSL is enabled, MobiControl acts as its own certificate authority. It generates certificates for the MobiControl entities (Manager, Deployment Server, and Device Agents).

The table below summarizes the three available options for delivering and installing the device's MobiControl certificate:

Option	Description
Automatic delivery and silent installation of certificates	When this option is selected the Deployment Server will automatically deliver the certificate and private key for the device when the device connects. No user interaction is required.
Automatic delivery and prompt for password before installation on device	This option provides additional assurance that only authorized devices receive an SSL certificate and private key. When this option is selected, the Deployment Server will prompt the device user to enter the password specified in this dialog box before it delivers the certificate and private key. The device will be able to connect and stay online even if a password is not entered, however in this state the device will not receive any packages, or execute file synchronization. The administrative user can remote control the device to assist the device user with entering the password to retrieve the device certificate. The user will be given several chances to enter the correct password. If the user enters an incorrect password five times, and the **Keep Device Connected** check box is not selected, the device will be disconnected and disabled. To re-enable the device right-click on it in the device tree and select **Enable.** If the **Keep Device Connected** check box is selected, the device will remain online, and as described above, will not be eligible for package delivery or file synchronization but can be remote controlled.
Manual Installation (No automatic delivery or installation)	When this option is selected certificates and private keys will not be automatically delivered to the devices. The certificate and private key must be exported (`*.pfx` file), and delivered to the device by some means. This could be via email, file transfer, etc. **NOTE:** Importing certificates is only supported on Windows Mobile 5 devices and Windows desktop clients (Windows 2000/XP).

In all the cases above, the Device Agent stores the certificate and private key into the Windows operating system's personal certificate store. The MobiControl Root CA certificate, on the other hand, is stored in the operating system's trusted root certificate store.

Manual Installation



Export Device Certificate dialog box

When this option is selected, the certificate and private key must be exported (`*.pfx` file), and delivered to the device via email, file transfer, storage card, etc.

Once the `*.pfx` file has been delivered to the target device, the user must use the MobiControl applet running on the device to import it. For further information, refer to the SSL Cert tab in the mobile device configuration applet on importing the certificate. (Please see the "Mobile Device Configuration Applet" topic on page 397.

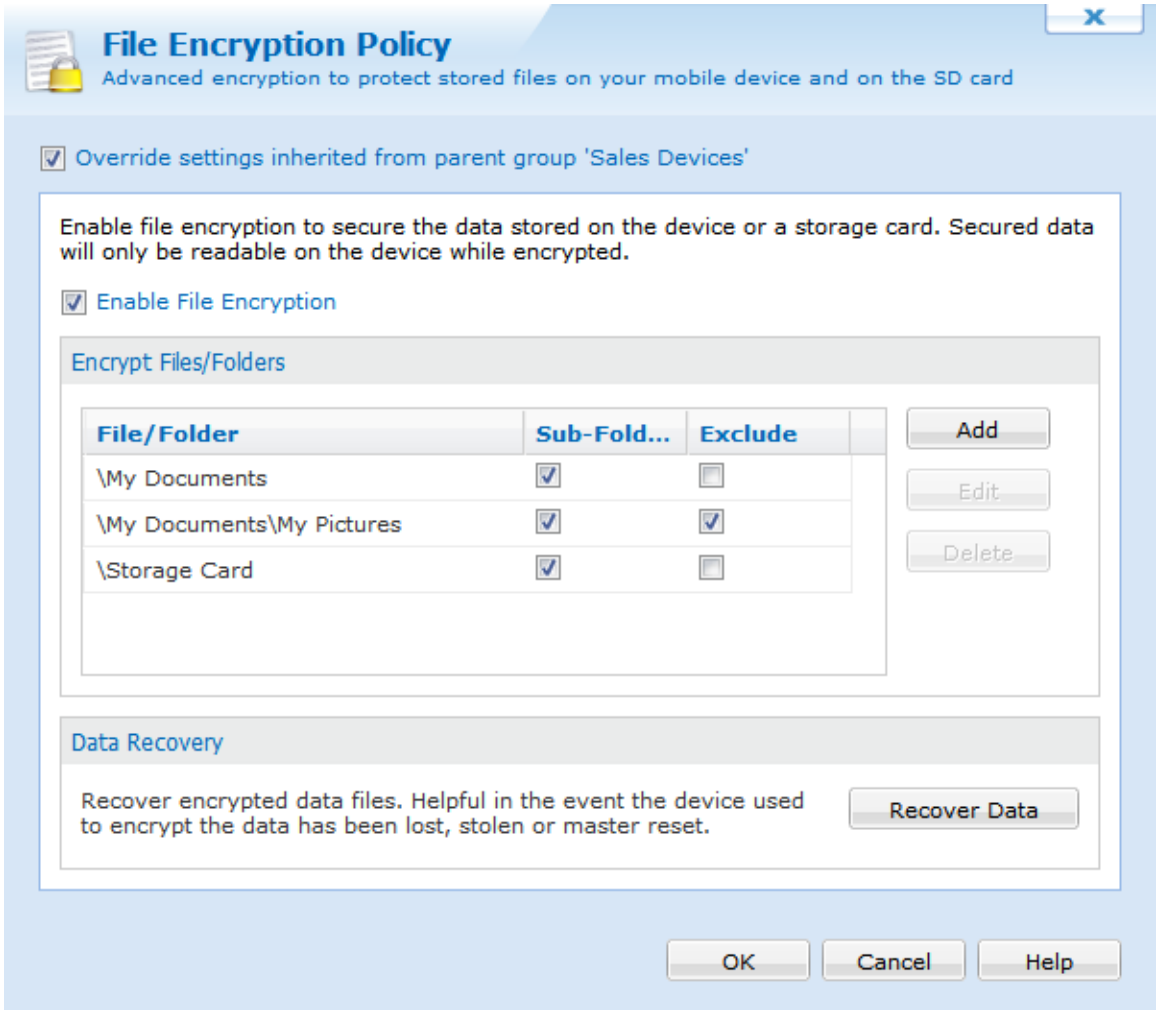
Windows Mobile File Encryption

Due to the portable nature of data stored on mobile devices, there always exists the possibility of this data being found by someone other than the intended user. For instance, if a device is lost or stolen, sensitive business information (contacts, emails, spreadsheets, documents or other confidential data) may be found. Data can be easily retrieved from the device using a variety of file transfer methods (i.e. USB cradle, Bluetooth or Wi-Fi file transfer, or infrared beam).

MobiControl helps secure data stored on the mobile device and SD memory cards or storage media to help businesses achieve compliance with strict data storage and processing regulations. The file encryption feature allows encrypting data stored on a device or memory card so that it can not be accessed by an unauthorized person. This protects sensitive data if an attempt is made to extract it from the mobile device and access it on another mobile device, computer or data reader by an unauthorized person.

IMPORTANT:

Due to some limitations of Windows CE6, the File Encryption policy cannot encrypt the files on CE6 devices.



File Encryption Policy dialog box

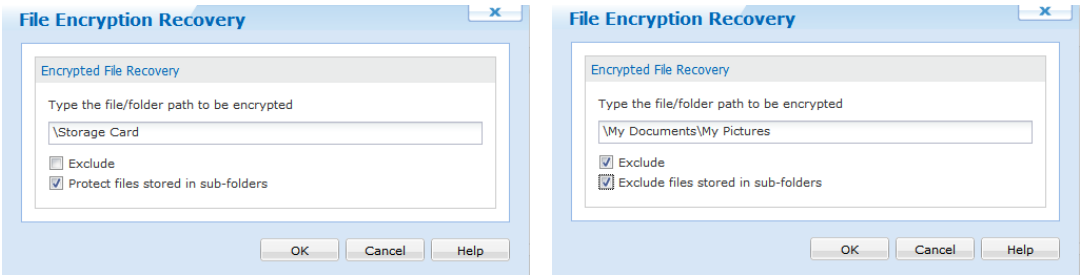
For assistance with Override Settings Click Here.

MobiControl's policy-based file encryption uses FIPS 140-2 validated AES-256 encryption algorithms to secure mobile data. On-the-fly file encryption is implemented easily and transparently without affecting the end users experience and allows data to be encrypted and decrypted in memory when needed by mobile applications on the device. MobiControl provides granular control allowing encryption of specified files and folders, including the ability to select an entire volume such as a storage card.

To enable file encryption for a device or group of devices, select **File Encryption Policy** from the MobiControl Security Center. User authentication must be enabled prior to enabling file encryption. (Please see the "Windows Mobile Device Configuration" topic on page 632 and "Windows Mobile Authentication" topic on page 634 for more information.)

Use the **Add** and **Edit** buttons to bring up the **Add File/Folder** dialog box to create a new entry or modify an existing entry. Individual files or entire folders can be encrypted. If a folder is selected and the option to **Protect files stored in sub-folders** is enabled, all sub-folders within it will also be encrypted. The

Exclude selected file/folder option makes it possible to exclude a file or folder from encryption. For instance, this option can be used to exclude a folder from encryption if its parent folder is encrypted, and the option to protect files stored in the parent folder's sub-folders is enabled. When the **Exclude selected file/folder** option is selected, the option below it changes to **Exclude files stored in sub-folders.** When this second option is selected, sub-folders of the selected folder will also be excluded from encryption.



Add File/Folder dialog box for encrypting a folder (left) and excluding a folder from encryption

TIP:

MobiControl supports the use of wildcards when entering folder/file names. The asterisk ("*") substitutes for any zero or more characters, and the question mark ("?") substitutes for any one character. For example, entering "*.doc" with Protect files stored in sub-folders enabled will encrypt any document with the .doc extension on the device.

Automatic Key Archiving for Recovery of Encrypted Data

During the encryption process, the encryption key is stored on the mobile device so that any encrypted data on the mobile device or the storage / SD memory card can be accessed on the mobile device by an authenticated user. It may become necessary in certain situations to decrypt that data for use on another device (i.e. a hardware failure on the mobile device requiring the data on the storage card to be recovered on another device). If the encryption key is saved on the mobile device only and the device is stolen or damaged, the data on the accompanying storage cards would be rendered unusable as well.

File Encryption Recovery dialog box

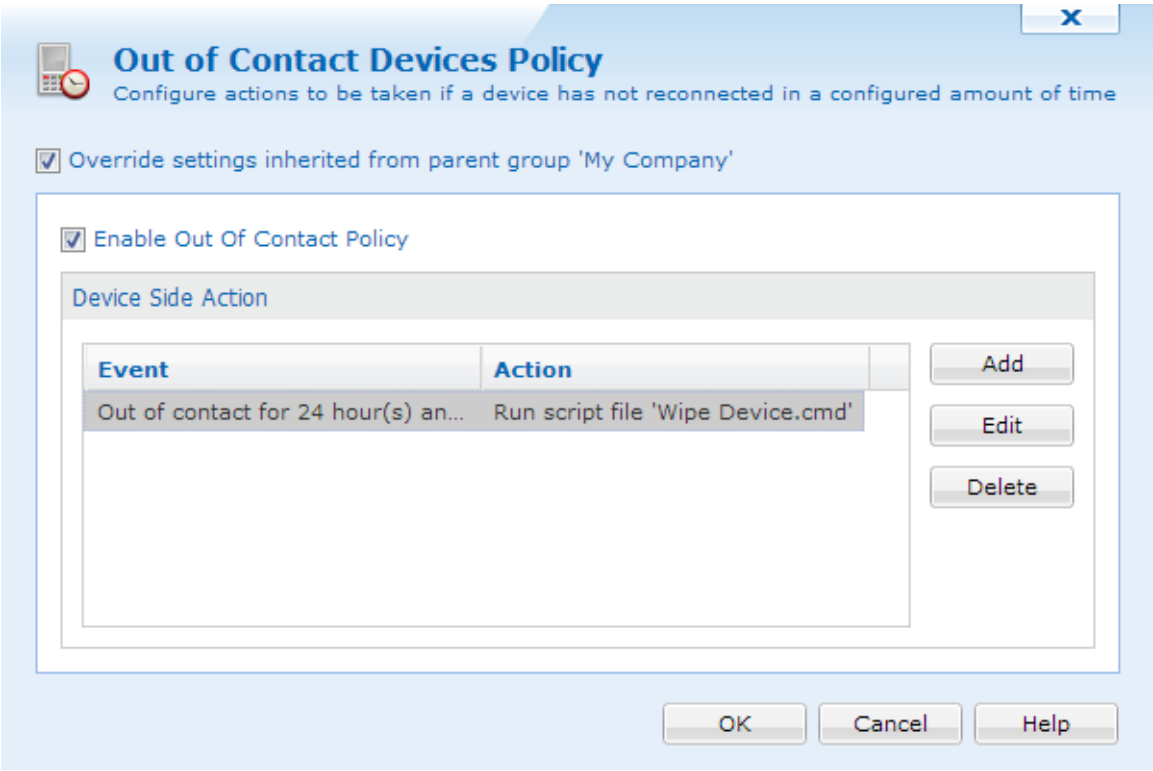
MobiControl automatically, and transparently to the end user, archives a backup copy of the encryption key in the MobiControl database to allow the recovery of encrypted data in exceptional scenarios. This archiving of the encryption key takes place at the same time as it is generated to allow easy recovery of encrypted data, to deal with extraordinary situations and device failures.

Files can be decrypted using the MobiControl Manager. Click on the **Recover Data** button in the **File Encryption Policy** dialog box to recover encrypted files. The **File Encryption Recovery** dialog box allows you to specify the encrypted file (on a storage card or any other medium) and decrypt the file, recovering it to the destination file specified as the output file.

Windows Mobile Out-of-Contact Devices

The out-of-contact devices policy dialog box allows you to manage security on "out-of-contact" devices which are not able to connect to the MobiControl Deployment Server. This feature can be used to define security actions that can be triggered if a device has not contacted the MobiControl server for a specified time interval, or has been lost or stolen and appears as offline in the device tree.

To enable the out-of-contact devices policy for a device or group of devices, select **Out of Contact Devices Policy** from the MobiControl Security Center. (Please see the "Windows Mobile Device Configuration" topic on page 632.)



Out of Contact Device Security Policy dialog box

EXAMPLE:

If a device does not contact the server for two days, you can configure it to be wiped to avoid losing any sensitive data on the device. Other actions and standard script commands can also be executed.

For assistance with Override Settings Click Here.

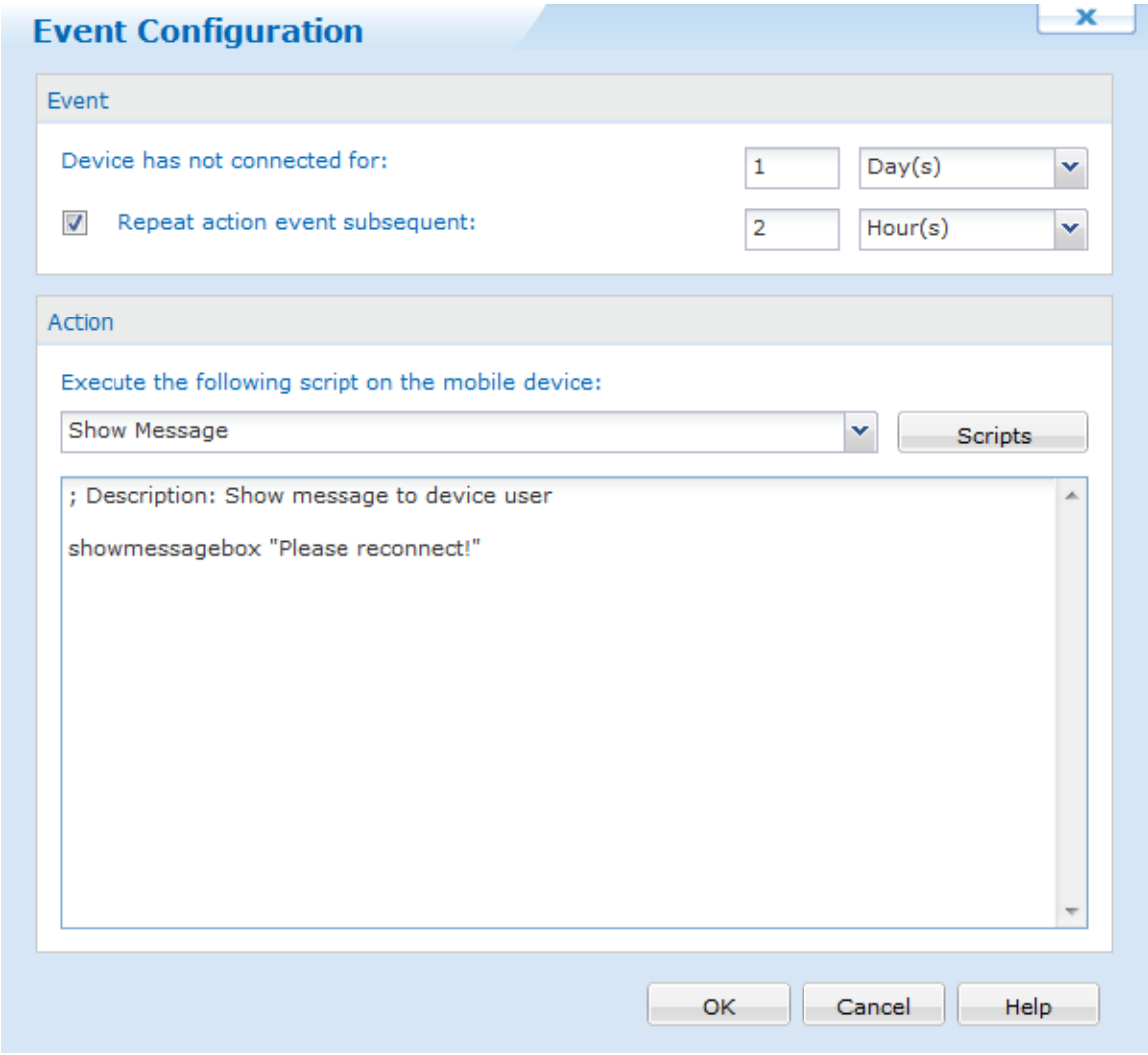
To add an event for which security actions can be specified, click the **Add** button. Click on the **Edit** button to modify an existing event or an action. Click on **Delete** to remove an event and its corresponding action from the list.

Action	Description
Add	To add an event for which security actions can be specified.
Edit	To modify an existing event or an action. Clicking this button presents the option to edit an action or the corresponding action.
Delete	To remove an event and its corresponding action from the list.

Add Event

To add an event, click the **Add** button to bring up the **Out of Contact Event Configuration** dialog box. Specify the time interval after which an action (or a script) should be triggered if the mobile device has not connected to the MobiControl Deployment Server (which is indicated by the device appearing as online in the device tree).

After you have specified the time interval, select a script to execute, or click **Scripts** to bring up the **Manage Scripts** dialog box. Please see the Script Manager page for further details.



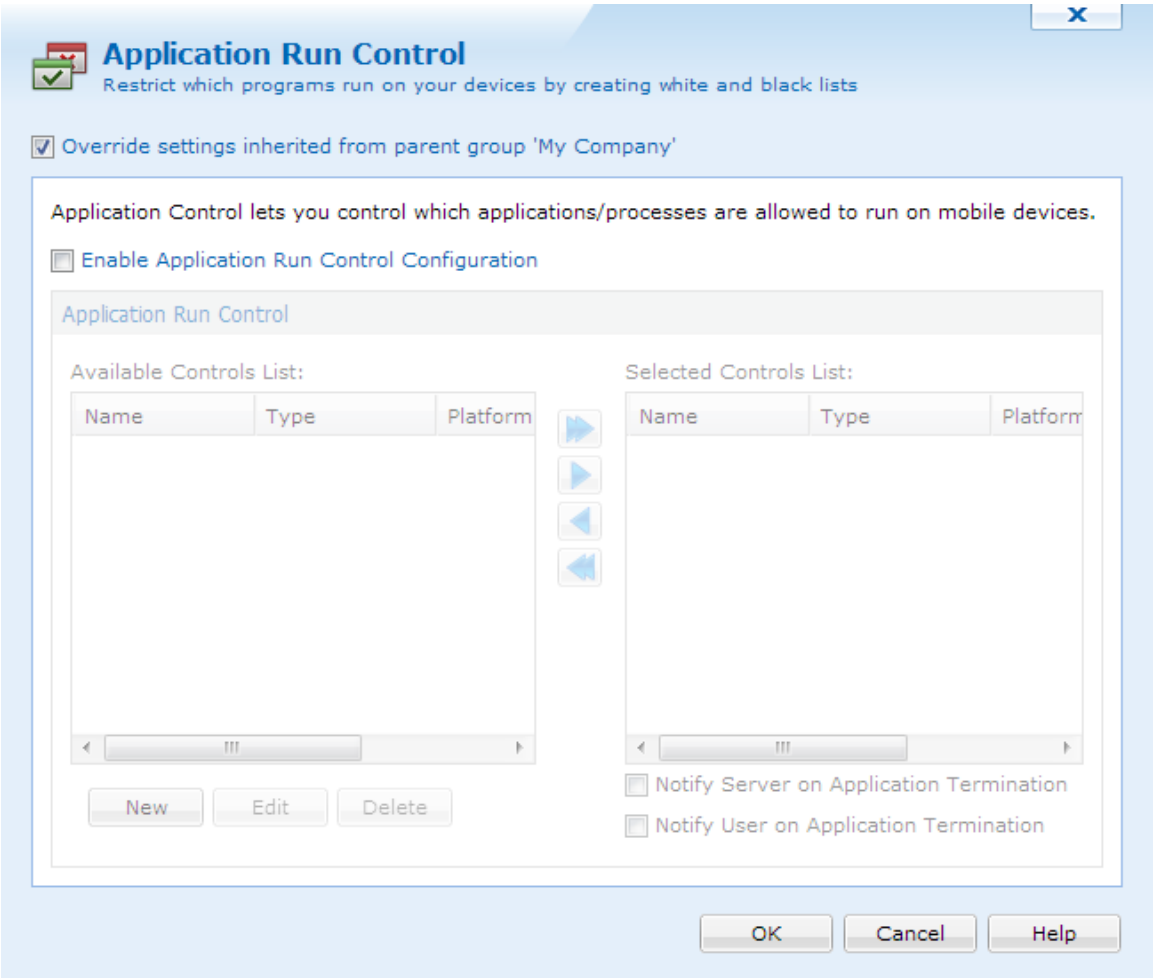
Out of Contact Event Configuration dialog box

Windows Mobile Application Run Control

The easy availability of applications—games, consumer-oriented utilities and third party tools—for mobile devices results in end users installing and running unauthorized personal programs and recreational software on devices meant for business use. In addition to contributing to memory and battery life overhead, this situation also contributes to productivity losses. The installation of unauthorized and unapproved non-business applications contributes to a significantly higher volume of support calls, increasing the IT help desk's support burden. Most critically, it is imperative for security-conscious users to control and restrict the unauthorized installation of personal applications to ensure compliance with strict mobile data protection requirements.

MobiControl's application run control features reduce the risk of leakage of sensitive data and complement the existing network security model by preventing the introduction of malware and viruses into the network through the mobile devices. Additionally, it also allows memory management on the mobile devices to free up resources taken up by unnecessary processes, and allowing for better device performance. MobiControl integrates tightly with the operating system to prevent restricted

applications from running entirely on the mobile device, making it much more efficient than competing white list and black list solutions which use CPU and battery-consuming processes to monitor for and destroy restricted applications.



Application Run Control dialog box

For assistance with Override Settings Click Here.

Application Run Control Modes

MobiControl provides two modes of operation for Application Run Control with two control list types:

1. The **black list**, or list of restricted applications, allows IT administrators to ensure that an application will not be allowed to execute on the device. The MobiControl Device Agent prevents any black-listed processes from executing on the device.
2. The **white list**, or list of approved/allowed applications, limits what programs can be executed on the devices. Only the applications and processes included in the white list are allowed to execute on the device. This provides an added layer of security for organizations concerned about unknown processes and applications that may be introduced to the device—maybe without the end user being aware of it, as is frequently the case with viruses, spy ware and other malicious applications.

> **NOTE:**
>
> If an application is being run from the lockdown, and it is blacklisted on the device, the application will still run as the lockdown takes precedence over the blacklist.

> **IMPORTANT:**
>
> If the white list is not set up correctly, you may end up blocking a potential system critical applications and cause the device to crash.

To enable application run control for a device or group of devices, select **Application Run Control Policy** from the MobiControl Security Center. (Please see the "Windows Mobile Device Configuration" topic on page 632.)

Control List Creation Methods

> **IMPORTANT:**
>
> Whether you are creating a white list or a black list, the use of learning mode is strongly encouraged.

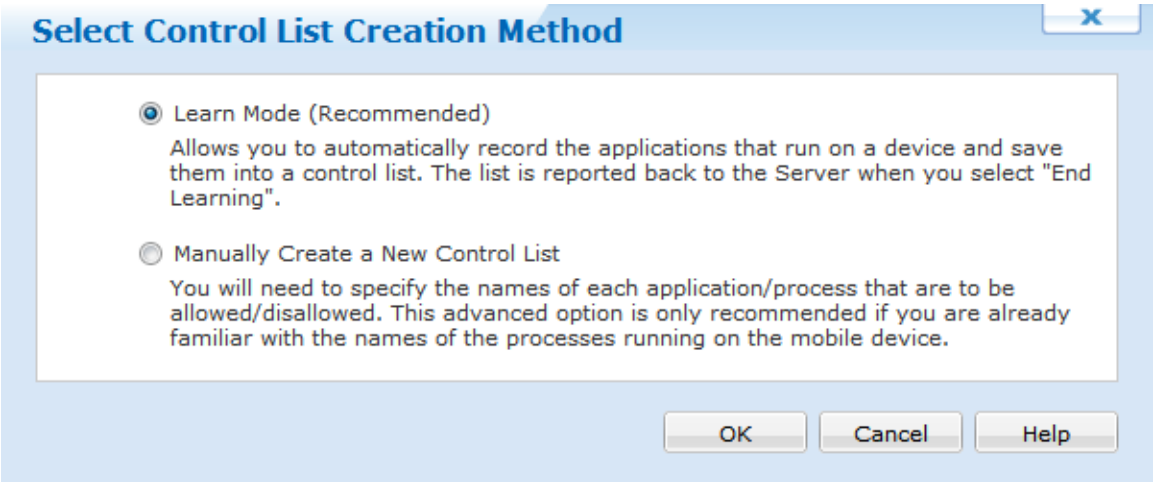
Configuration of application run control begins with the creation of an application control list. An application control list is simply a listing of the names of the executables files that correlate to the application you may wish to allow or disallow on the mobile device. For example, `pword.exe` corresponds to Microsoft Word for Windows Mobile, and `tmail.exe` corresponds to Microsoft messaging client for Windows Mobile. The categorization of the application control list, either as a white list or a black list, determines whether the specified programs will be allowed or disallowed.

Application control lists may be specified manually or they can be auto-generated using learning mode.

Learning Mode

Learning mode can only be enabled or disabled on a device that is **online**. If you right-click on a device group or an offline device, you will receive an error message if you try to enable learning mode.

Learning mode allows you to quickly and easily capture the names of all the executable processes that might be relevant to the everyday use of the device by the end user. Once generated, you may edit the list that was created. One device can be used to capture the applications that are commonly used. A control list can then be applied to a larger set of devices, for instance by applying the control list at a group level.

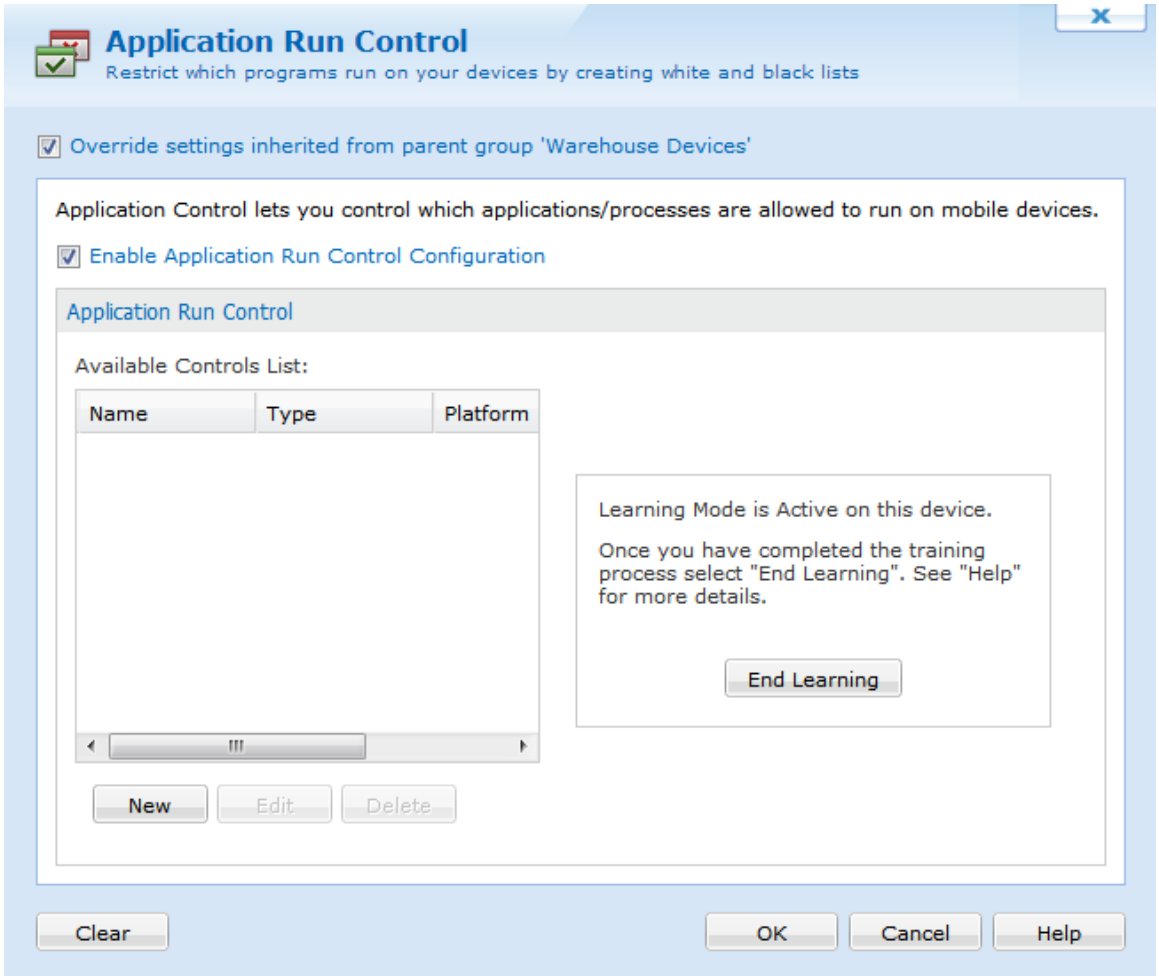


Select Control List Creation Method dialog box

Enable learning mode by selecting the **New** button in the **Application Run Control** dialog box, and then choosing **Learning Mode** in the **Select List Creation Method** dialog box.

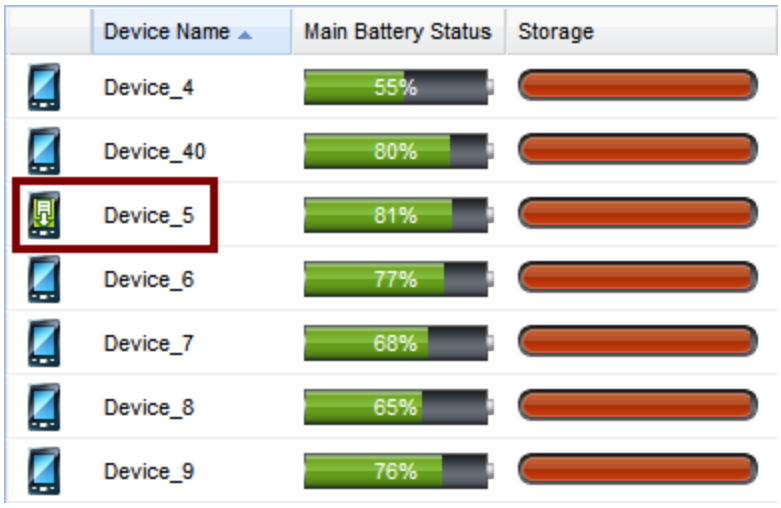
Once you have enabled learning mode, begin using the device. If you wish to develop a white list, run all the applications that the typical end user will need (i.e. Microsoft Messaging, Microsoft Word, Calendar, Contacts). Go through normal, everyday situations like making and receiving a phone call, soft-resetting the device, etc. Use the device with learning mode enabled for as long as it takes you to ensure that all the applications that your user will need to execute have been launched at some point. (You can run it for an hour, a day, a week,…)

Once you are satisfied that you have fully trained the device's application run control, click the **End Learning** button.

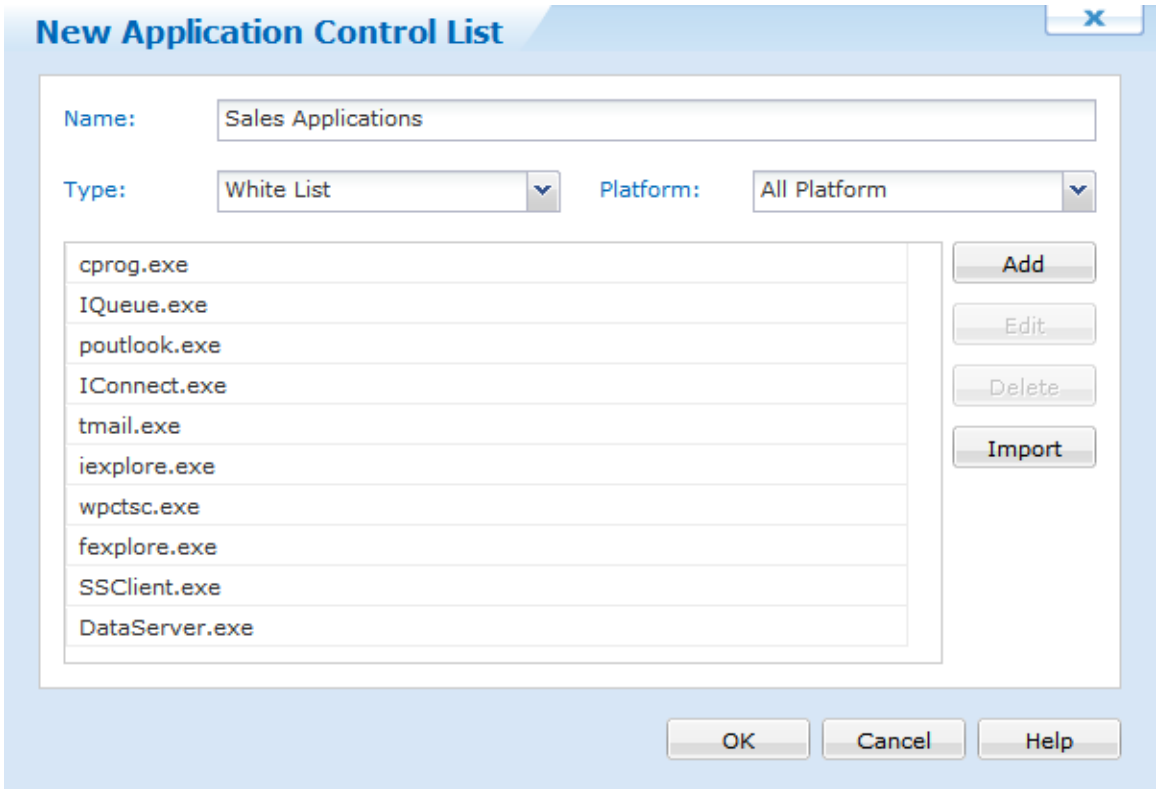


Application Run Control Learning Mode dialog box

While the device is in learning mode, a red **L** icon will appear on the device until learning mode has ended.



The list of "learned" applications will be presented to in a dialog box that allows you to edit the list. For example, you may wish to delete an application that was mistakenly executed during the learning. Before saving the control list, you must name it.

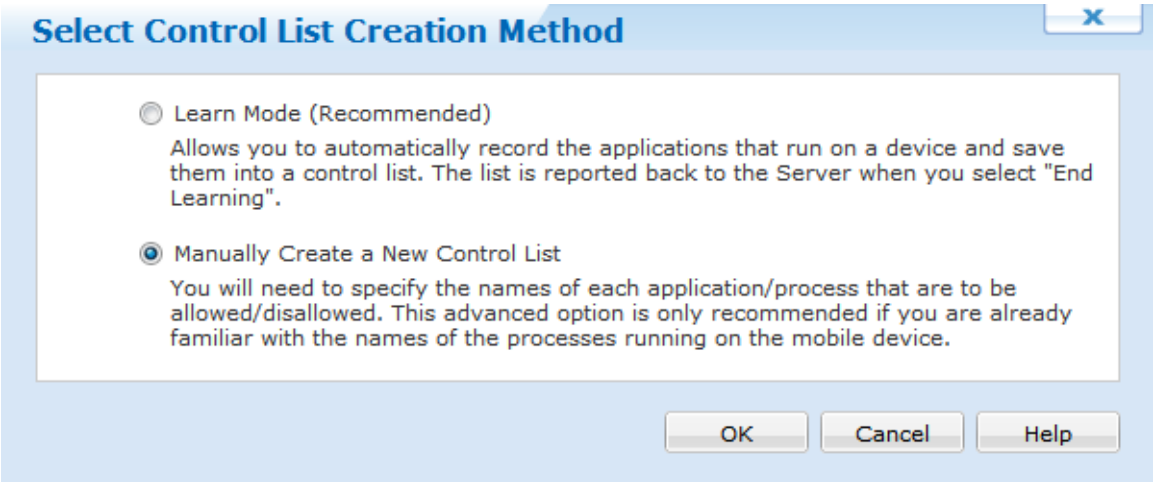


Application Run Control Learning Mode list

Now the application run control list has been created, you may assign it to various devices and groups.

If you wish to develop a black list using the Learning Mode, run all the applications that you do not want your user to be able to access (i.e. Solitaire, Bubble Breaker, Internet Explorer, etc.) Once you are satisfied that you have executed all the applications that are to be banned, click **End Learning.** Since learning mode lists all the processes that were found to be running, it is important that you go through and remove from the blacklist those application that are not to be disallowed.

Manual Mode

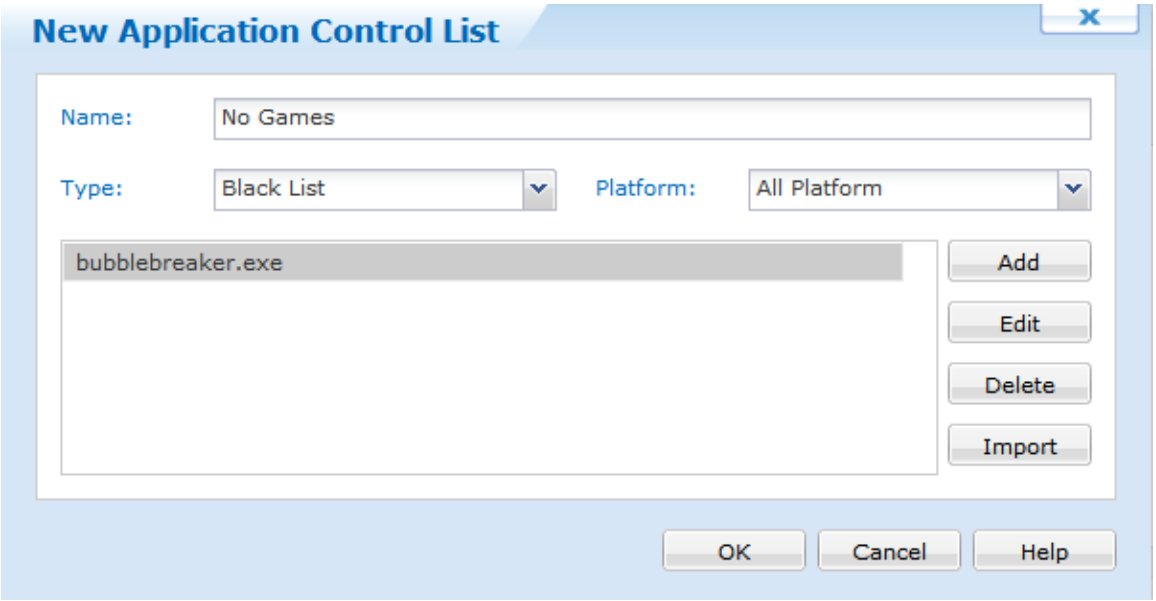


Select Control List Creation Method dialog box

Manual list creation is provided for the expert device administrator who already knows exactly which executables are to be put on the white list or black list. This advanced feature is only recommended if you have already used learning mode and are aware of the names of the executables that need to be allowed for correct device operation, and those that you wish to restrict.

You can manually create a new application control list by clicking the **New** button in the **Application Run Control** dialog box, and then choosing the **Manually Create a New Control List** option in the **Select Control List Creation Method** dialog box. The **New Application Control List** dialog pops up, allowing you to specify the application that you want to add to the list, and the platform for which this entry would be valid. This allows you to restrict applications on a device running a specific operating system (e.g. Windows Mobile 5), if you have a mix of devices with different operating systems in the same group.

Once created, the list may be applied to one or more devices or groups.



Creating a black list in manual mode

IMPORTANT:

Application run control can adversely impact the operation of the mobile device if configured incorrectly. After you have developed a control list, apply it to one or two select devices for extended field testing before expanding it to the general deployment. As a general rule, if you don't know what the executable does (e.g. `somestrangename.exe`), allow it to run instead of blocking it as it might be critical for the device's proper operation.

Modifying or Deleting a Control List

An application control list can be edited whether it is currently in use or not, but its type (white list or black list) cannot be changed once created.

An application control list can only be deleted if it is currently not selected for any devices or device groups. A control list that is listed in the **Selected** field is considered in-use, even if the application run control is disabled for the given group or device.

NOTE:

If you edit an application control list that is shared among device groups that are not subgroups of the group you are configuring, the changes will not be propagated to the other devices. The modified control list will only affect devices belonging to the group being configured or its subgroups.

Application Run Control Event Notification

Every time MobiControl's application run control feature blocks or terminates an application that is not allowed to run by the security policy in effect, it can notify the server or the user if the appropriate options are selected.

The following two options are available:

- The **Notify Server on Application Termination** option will generate a log event on the server and display it in the Event Logs for that particular device when an attempt is made to run a blocked operation. Device logs can be viewed in the MobiControl Manager by highlighting the device or the group of devices and enabling the **Logs** tab. This allows the administrators using MobiControl Manager to track any attempts by the end users to run or install unauthorized applications and ensures a higher level of monitoring.
- The **Notify User on Application Termination** option causes a message box to be displayed on the user's device when an application is blocked.

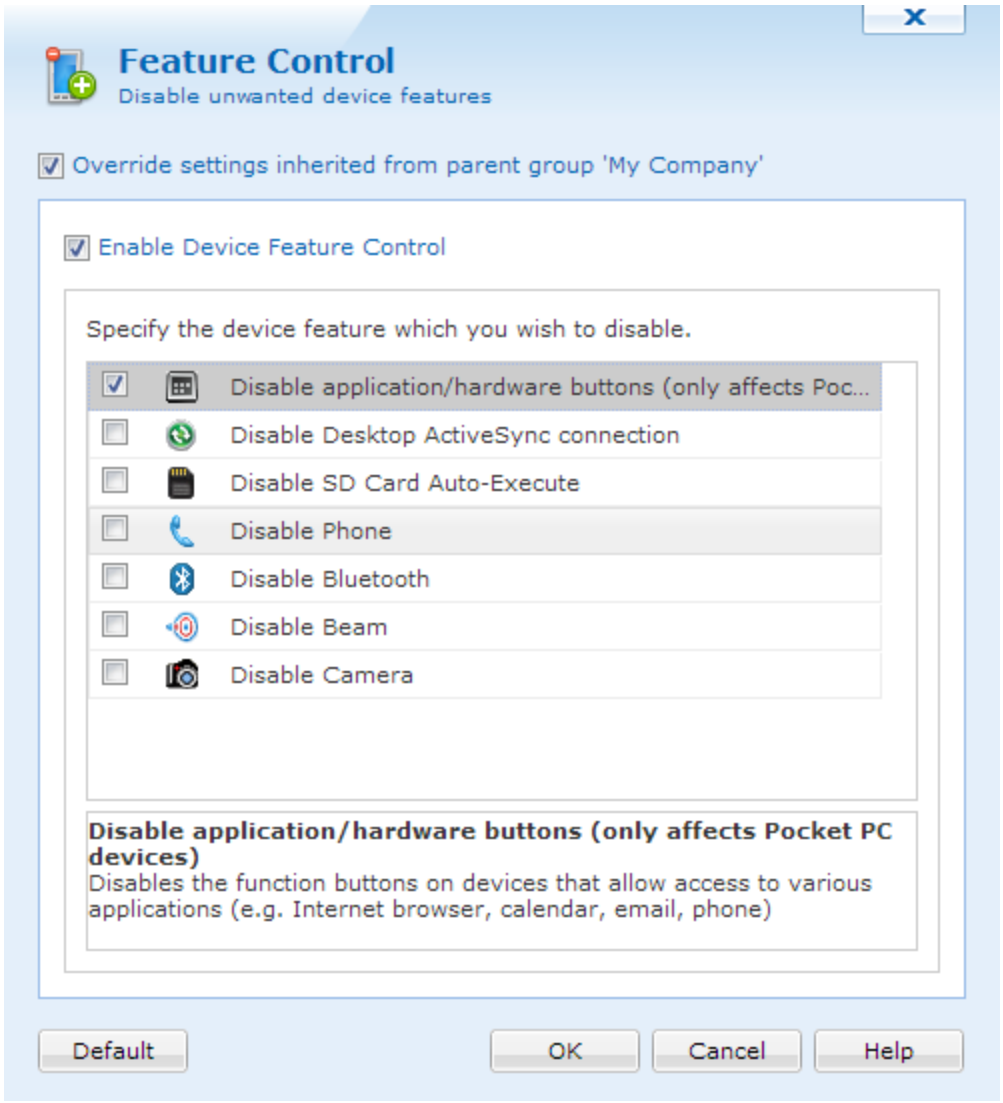
NOTES:

- When logged in as Admin on the mobile device, application control enforcement is suspended.
- Certain processes and applications are critical and necessary for stable device operation and normal execution of the MobiControlDevice Agent. These processes are automatically protected through a built-in "permanent white list" and cannot be put on a black list. Applications that are included in a lockdown program menu are automatically on a white list, and cannot be put on a black list.

Windows Mobile Device Feature Control

For security-conscious organizations and environments where privacy and information security concerns require controlling the unauthorized transfer of mobile data out of the mobile devices, MobiControl provides various on-device feature controls including the capability to block various device communications, similar to firewall functionality. MobiControl's device features control policy allows IT administrators to selectively disable device features. Applying the policy at the individual or group level allows custom profiles for different users and locations in an organization. The ability to disable or enable Bluetooth and infrared ports allows controlling whether end users can beam business cards, applications or documents to one another.

To enable device feature control for a device or group of devices, select **Device Feature Control Policy** from the MobiControl Security Center. (Please see the "Windows Mobile Device Configuration" topic on page 632.)



Device Feature Control Policy dialog box

For assistance with Override Settings Click Here.

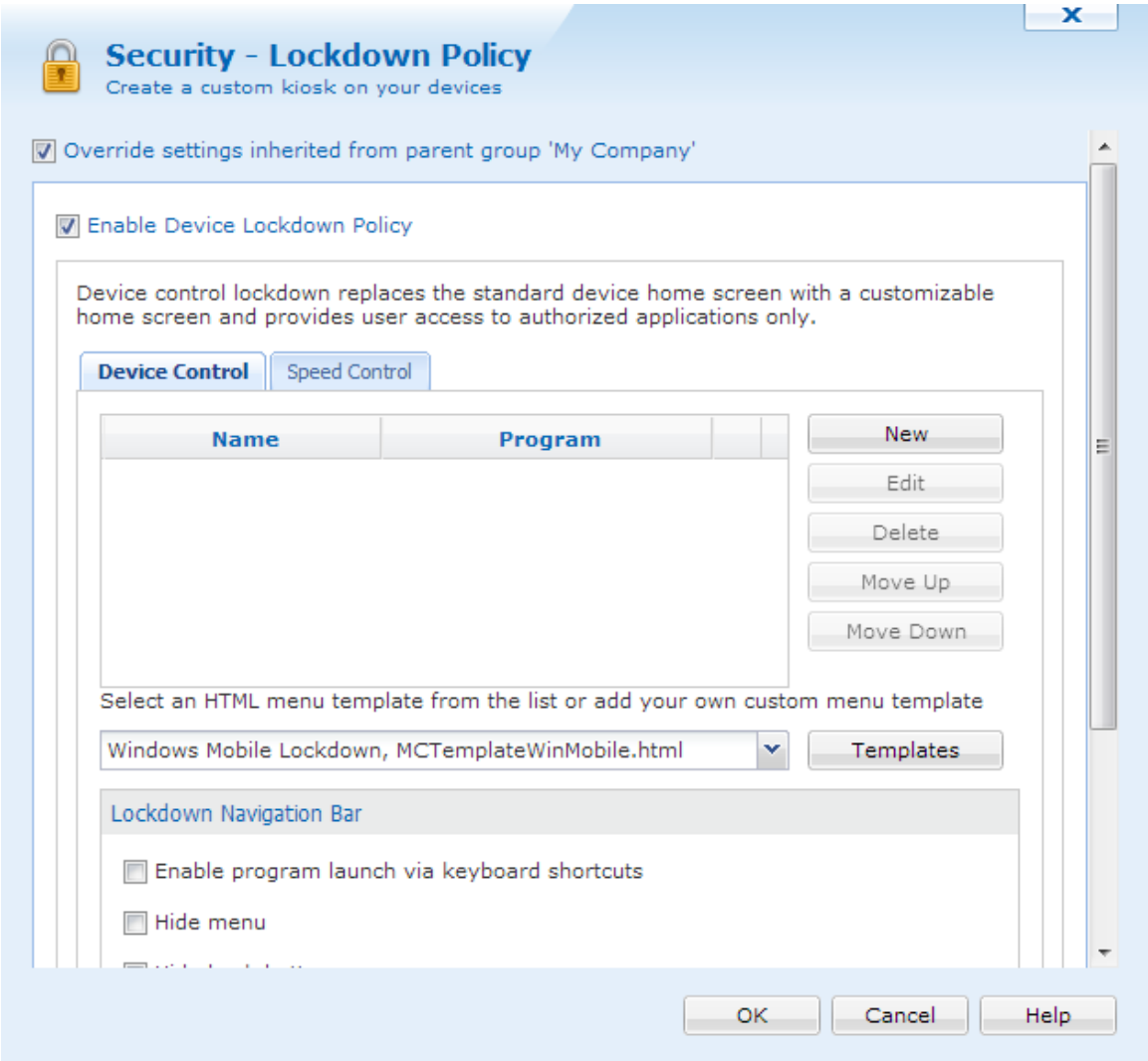
The following features can be enabled or disabled using the device feature control policy:

Field Name	Description
Disable application/hardware buttons	Disables the function buttons on PDAs that allow access to various applications on the device (i.e. Internet browser, calendar, email, phone) **NOTE:** This feature applies only to Pocket PC devices and results may vary depending on the device's manufacturer and model.
Disable Desktop ActiveSync connection	Disables the ActiveSync connection on the device so that data cannot be transferred from the device to a computer using the ActiveSync or WMDC (Windows Mobile Device Center) connection
Disable SD Card Auto-Execute	Prevents programs and applications from automatically executing from an SD or flash memory card when it is inserted in the device This feature can be used to prevent installation of unauthorized applications on the device.
Disable Phone	Restricts unauthorized voice calls and phone usage on PDAs and Mobile Devices with phone capability
Disable Bluetooth	Disables the Bluetooth wireless connection on the device preventing data transfer to and from the device **NOTE:** In certain environments, the Bluetooth radio may need to be disabled due to regulatory requirements.
Disable Beam	Disables the infra-red port on the device preventing beaming of important business data and information from the mobile device to other devices
Disable Camera	If the PDA is equipped with a camera function, this feature can be disabled to prevent unauthorized or unnecessary usage of the camera.

Windows Mobile Device Lockdown

Device lockdown replaces the standard device home screen and Windows **Start** button with a customizable home screen. Users have access only to authorized applications and websites, and are prevented from accessing all other applications and device controls. With the lockdown policy we are also able to change the home screen based on their current speed. This is called the Speed Lockdown.

Please see the "Windows Mobile Device Speed Lockdown" topic on page 676 for more information about the Speed lockdown.



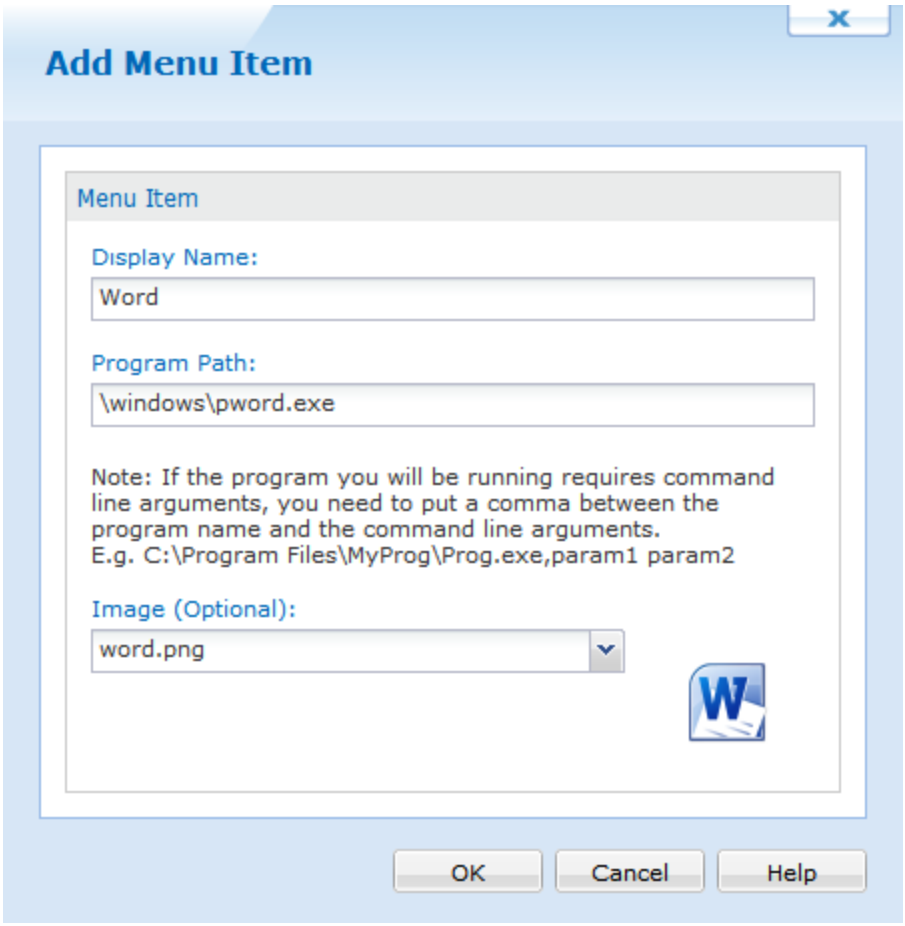
Lockdown Policy dialog box

By locking down devices, organizations can minimize the risk of unauthorized persons accessing information on their mobile devices. Administrators can control exactly which programs users are allowed to run, and which websites they are allowed to visit. This decreases the amount of down-time caused by users changing settings that may adversely affect the operation of the device or application software, and also decreases support costs. MobiControl allows running the mobile devices in a kiosk mode with a read-only access to provide critical information to the end users, without giving them access to change the settings.

The lockdown menu can only be dismissed by an administrator. Specification of a user password is optional. If not configured the device user can access the lockdown menu directly after turning on the device. If a user password is defined, then the password must be entered in order to access the lockdown menu.

To configure lockdown settings for a device or group of devices, select the target device or group in the device tree view in the main console window and select **Security** from the **Configure Device(s)** submenu.

Field Name	Description
Enable lockdown menu	Use this checkbox to enable or disable the device lockdown menu.
Device Program Menu	The device program menu is a list of programs and websites to which the user has access. There are pre-configured HTML menu templates that can be edited or applied to the menu, and an option to enable or disable the launching of a menu item with keyboard shortcuts. Please see the Device Program Menu section below for details.
HTML menu template	Select a menu template from the drop-down list. Please see the Templates section below or the "Customizing Lockdown Program Menu Templates" topic on page 678 for more information.
Enable program launch via keyboard shortcuts	Keyboard shortcuts such as numeric keys can be used to launch lockdown menu items. See the Shortcuts section below.
Device Navigation Bar	The device navigation bar, commonly referred to as the task bar, contains the **Start** button and small icons for quick access to device status and settings such as the time, date, wireless status, or volume control. By default, when lockdown is enabled, the standard operating system navigation bar is replaced with a customizable navigation bar. **NOTE:** This applies to only Pocket PC and CE devices; it does not apply to Smartphone devices. Select the **Configure** button to specify which icons in the custom navigation bar are to be made available to the device user. Please see the Navigation Bar Configuration section below for details.



Add New Menu Item dialog box

TIP:

- To provide the device users with access to specific websites and prevent access to other websites, provide the URL in the **Program Path** of the **Add New Menu Item** line.
- If you link to a search engine the end user will gain full access to the Internet.

Device Program Menu

Use the **New** button to add menu items. Each entry consists of a user-friendly name and a complete file path to the executable, `.lnk` shortcut file, `.cmd` script file, or website address (URL). To adjust the position of the menu items, use the **Move Up** and **Move Down** buttons.

Field Name	Description
Display Name	This is the displayed name of the menu item which will appear on the device.
Program Path	This is the path for the web address, or executable file on the device. You can either type in the path or you can browse the file using the browse button ⋯. You can only browse the files if the device is connected to the desktop via ActiveSync. For instance, the program path for Pocket Word is

NOTES:

- For command line parameters, a comma must be used to separate the program path from the parameter. For example, write `\windows\poutlook.exe,contacts` without spaces

Field Name	Description
	`\windows\pword.exe`. The path will not be displayed on the Menu page.
Image (optional)	This is the name of the image file that you want to display in the lockdown menu with this menu entry. By selecting the image in this dialog box, it will be automatically delivered to the device along with the lockdown configuration. Select an image from the drop-down list, or click the browse button to select an image from your desktop computer. In order to display this image in the lockdown menu, it is necessary for the HTML template to have a special `<MCDispImgN>` tag. Please see the "Customizing Lockdown Program Menu Templates" topic on page 678 for instructions on how to make this image appear in the Lockdown menu. **NOTE:** If you wish to replace an image that had been previously imported, upload the new graphic file, maintaining the same file name as the old one. You will be asked to confirm the overwrite of the old file. Click **Yes,** and the new image will be in effect.
Launch automatically on startup	When this option is checked, the selected program will be automatically executed on startup (i.e. after a soft reset, or restart of the lockdown process).

TIP:

On devices that feature a numeric keypad, an alternative to tapping the screen to launch the menu entries is entering the number that corresponds to the menu item. For example, press 2 to launch the second menu item.

Templates

The lockdown program menu is displayed as an HTML web page to the user. The Template drop-down box allows you to select an HTML template from a list of built in templates and your own customized templates.

You can easily create a customized lockdown template by copying an existing template and directly modifying HTML code in the built-in Lockdown Menu Template Editor available in MobiControl. (Please see the "Customizing Lockdown Program Menu Templates" topic on page 678.) You can also use your favorite HTML editor. When editing the HTML file, be sure to preserve the special MobiControl Menu tags. These special tags are automatically replaced with the appropriate Program Menu entries by MobiControl.

Once you have selected the desired template and clicked the **OK** button, MobiControl will merge the menu items that you have configured with the selected template and generate a custom HTML menu page.

Device lockdown page

Keyboard Shortcuts

If the checkbox next to **Enable program launch via keyboard shortcuts** is selected, program menu items may launch in a few additional ways: pressing a numeric key on the device or using a scanner will launch the program menu item corresponding to the value of the numeric key or barcode. To prevent this, clear the checkbox next to **Enable program launch via keyboard shortcuts**.

Navigating Device Lockdown

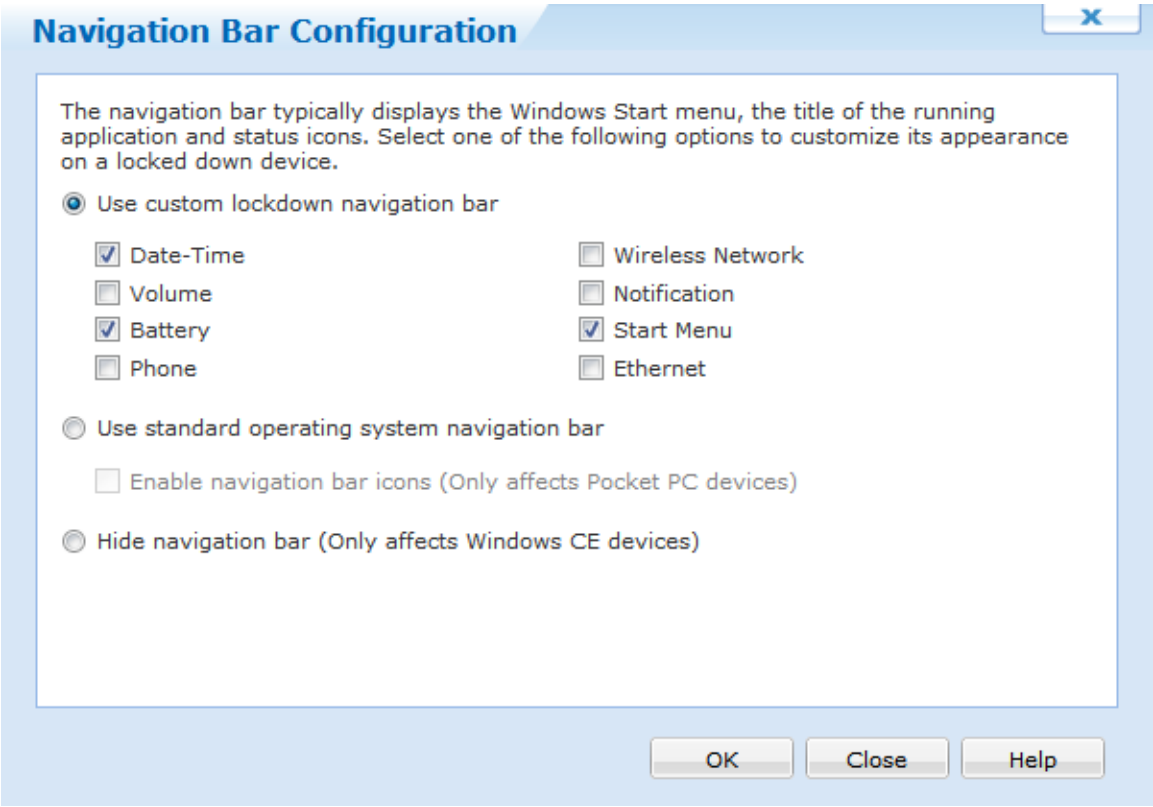
Back Button:
While you are navigating a web page within the lockdown, the back button will allow you to return to the previous page.

Right Click Option:
Click and hold on the device screen to bring up the "Right Click" menu. This allows you to copy and paste contents from within the lockdown.

NOTE:

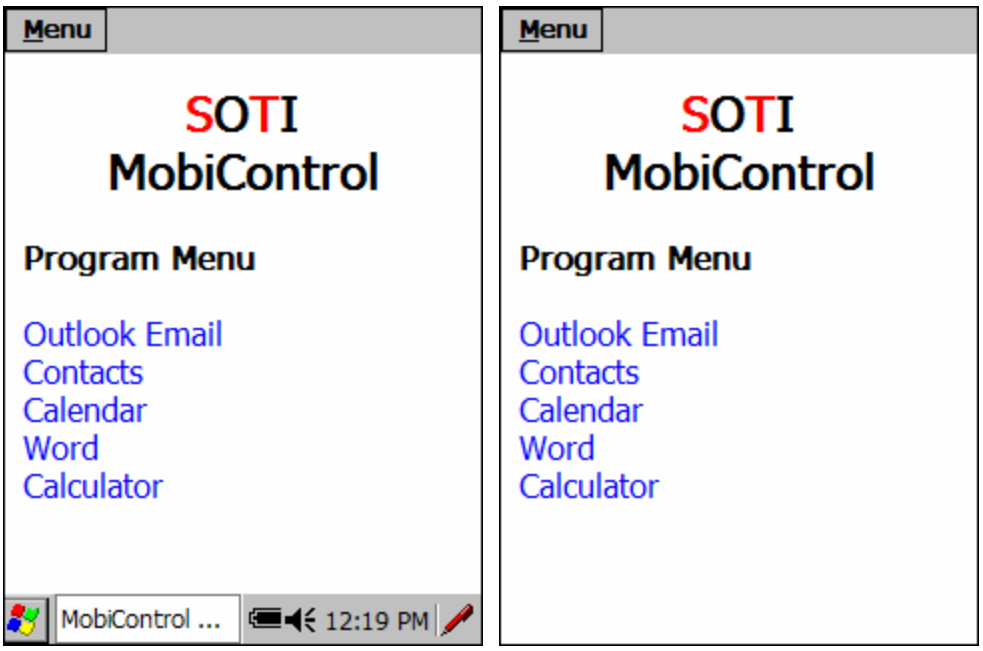
This feature is only supported on Windows Mobile 5.0 or later devices.

Navigation Bar Configuration



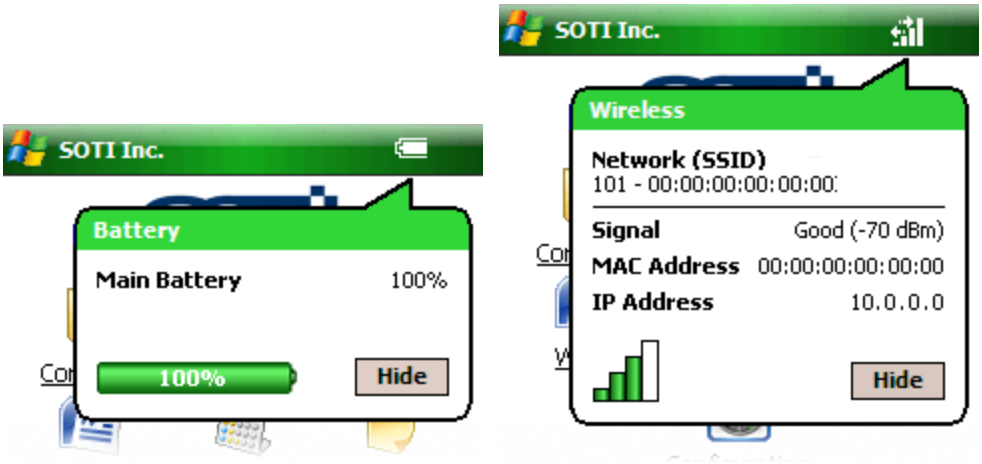
Navigation Bar Configuration dialog box

Field Name	Description
Use custom lockdown navigator	This option will only allow the selected icons to show up in a custom navigation bar. The user will have the ability to click on the icons and have view-only access. The user will not be allowed to make any configuration changes using the icons on the navigation bar. Please see the descriptions of the six options following this table.  *Enabled custom lockdown navigation bar displaying all the available icons* **NOTE:** The icons of the lockdown custom navigation bar are non-responsive on Windows CE 6.0 devices due to a current limitation. This will be addressed in a later version.
Use standard operating	This option will display the standard operating system's navigation bar. This option is recommended if there are specific  *Enabled Windows navigation bar*

Field Name	Description
system navigation bar	icons that appear in the standard navigation bar that are not available in the custom navigation bar. In order to prevent the user from accessing Programs listed in the Start menu and links to Settings from popup balloons accessed through the navigation bar icons, the navigation bar is disabled by default. For only Pocket PC devices, it is possible to enable the navigation bar icons. This option will allow the user unrestricted access to the Windows navigation bar.
Hide navigation bar	For only Windows CE.NET devices, this option will hide the navigation bar completely.  *Disabled and enabled "Hide navigation bar"*

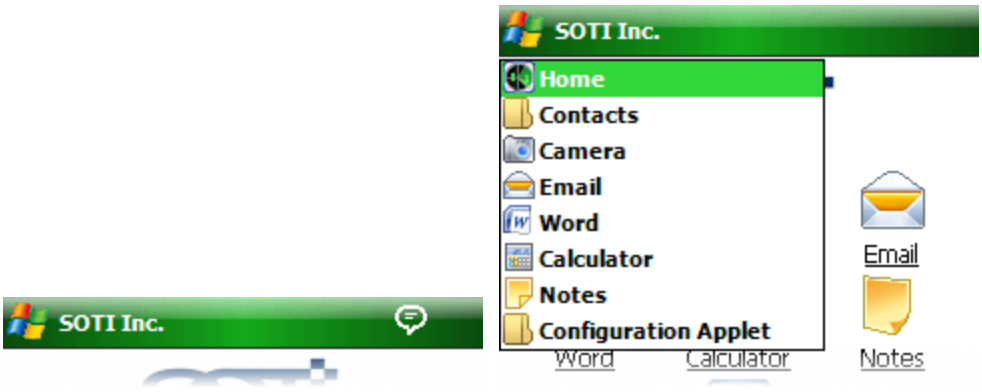
Enabled custom lockdown navigation bars with date-time and volume

- The **Date-Time** option will display the time on the custom lockdown navigation bar. When the time is selected, a window will display the date, time and user's appointments.
- The **Volume** option will cause the volume icon to be displayed on the custom lockdown navigation bar. When the volume icon is selected, the volume window will open and the user will be able to adjust the mobile device's sound and volume, change it to vibrate or turn off the sound completely.



Enabled custom lockdown navigation bars with battery and wireless network

- The **Battery** option will cause the battery icon to be displayed on the custom lockdown navigation bar. When the battery icon is selected, a window will display the percentage of the battery charge.
- The **Wireless Network** option will cause the wireless bar icon to be displayed on the custom lockdown navigation bar. When the wireless bar icon is selected, a window will display the mobile device's wireless settings such as the signal strength, MAC address and IP address.

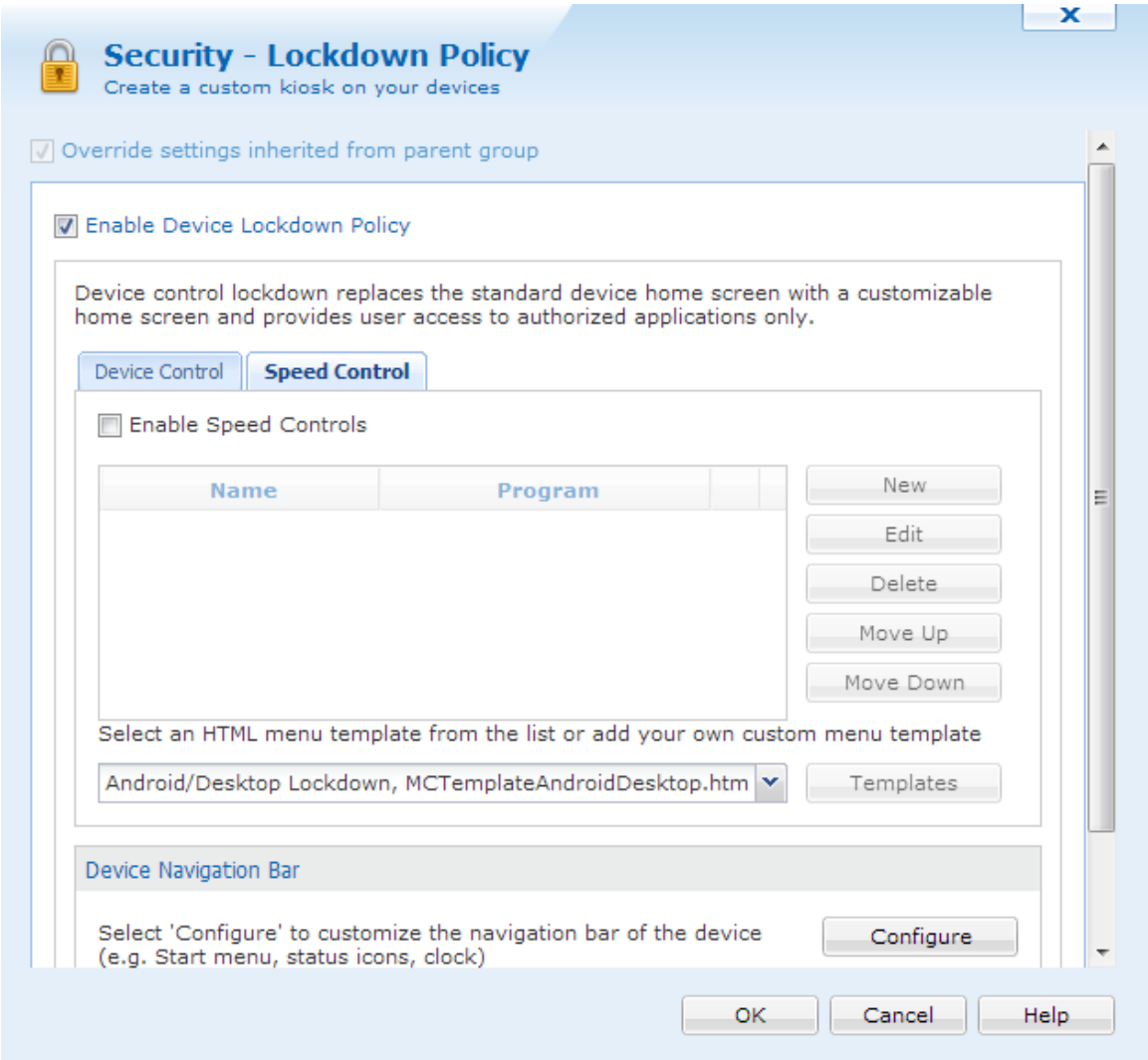


Enabled custom lockdown navigation bar notification and Start menu

- The **Notification** option will cause the Notification icon to appear in the custom lockdown navigation bar when there is an unacknowledged notification on the device. When the notification icon is selected, a pop-up menu will display, from which the user can select the notification to be displayed. This option also controls the display of the Notification menu entry in the Lockdown window.
- The **Start Menu** option allows the custom navigation bar to replace the standard Start menu with a listing of the programs specified in the Program Menu. This allows the Start menu to be used as an "application switcher" to move quickly from one application to another.

Windows Mobile Speed Lockdown

Device lockdown replaces the standard device home screen and Windows **Start** button with a customizable home screen. Users have access only to authorized applications and websites, and are prevented from accessing all other applications and device controls while on the road. This promotes greater safety by disabling distracting features on a mobile device while workers are on the road.

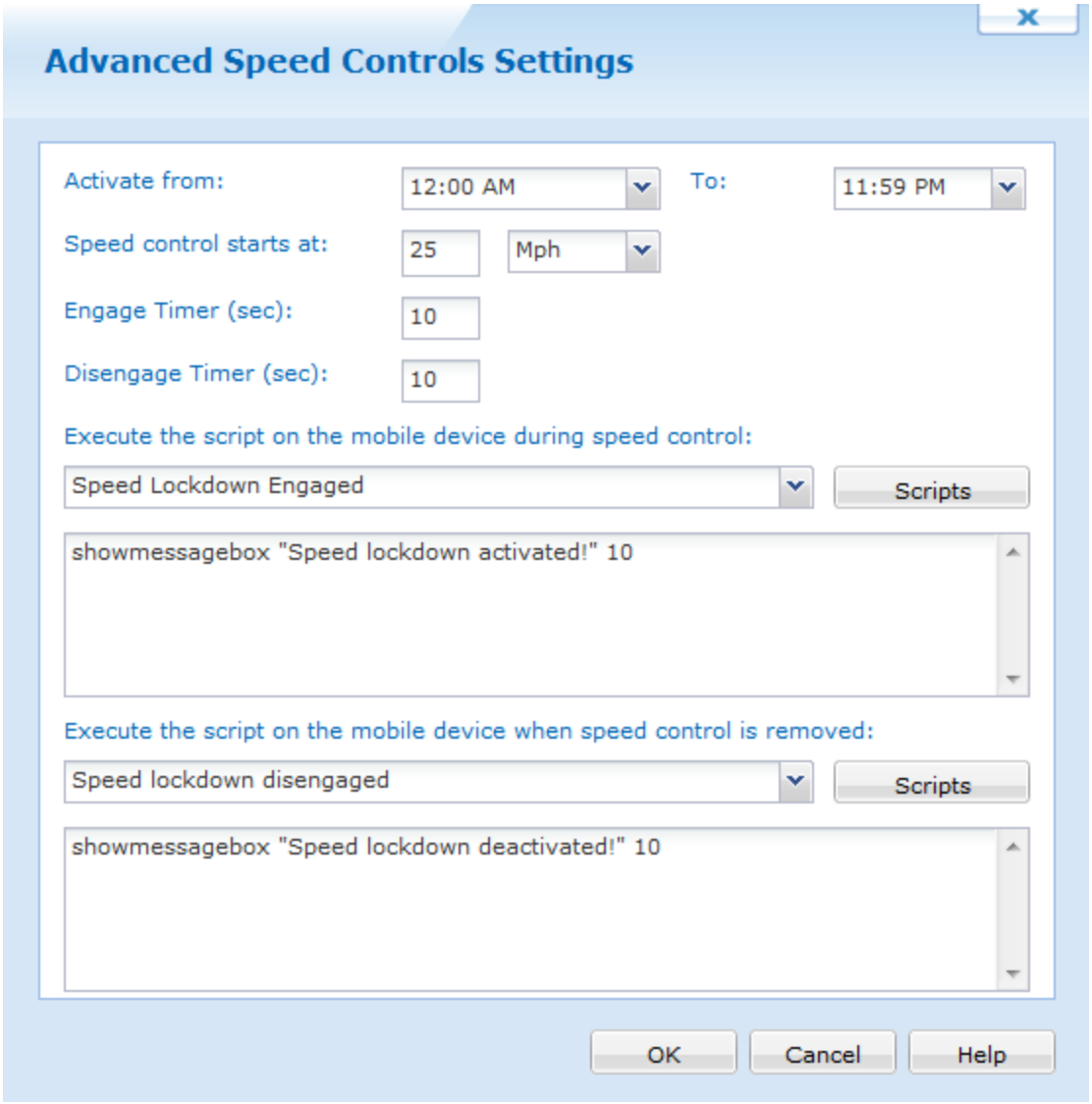


Lockdown Policy dialog box

For information on how to set up menu items and configuring lockdown templates, please click here.

Speed Lockdown triggers when the device is going a certain speed, as set in the Advanced settings. The speed of the device is determined by utilizing the device's GPS unit. Using the device's GPS unit, MobiControl periodically checks the location of the device along with the time. It will then check again and determine the distance between the two points and calculate the device's speed.

Since there are times where there could be traffic, or stop lights, having the speed lockdown disengage and re-engage constantly will cause distraction to a driver. Because of this, the speed lockdown has engage and disengage functionalities. These and other settings can be configured by clicking Advanced.



Advanced Speed Control Settings

Below are brief descriptions of each feature in the Advanced Speed Control settings.

Field	Description
Activate From, to	Here we can set when the speed control should activate. We can set it for the whole day or even 15 minutes.
Speed Control starts at	This is where we decide what speed the device should be travelling before the engage timer starts counting. We can change the speed measurement to either Mph or Km/h.
Engage Timer	The amount of time the device should

Field	Description
	stay on or above the speed control before the lockdown activates.
Disengage Timer	The amount of time the device stays below the specified speed control before disengaging.
Execute script on the mobile device during speed control	When the speed control lockdown is activated, send this script to the device.
Execute script on the mobile when speed control is removed	When the speed control lockdown is deactivated, send this script to the device.

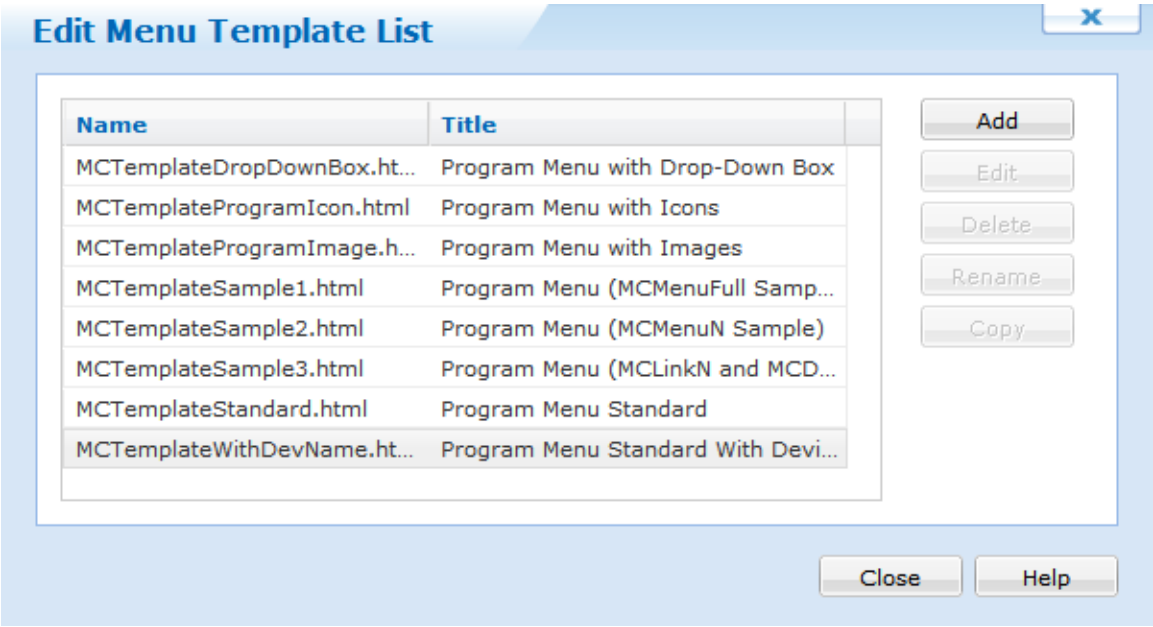
Using the above screen shot, the speed lockdown is activated the whole day, should engage when the device is travelling at 25 Mph or higher for at least 10 seconds. If it falls below the specified speed, wait 10 seconds before disengaging the speed control. When the speed control is activated, send a message box to the device, and when the speed control is removed, send another script.

Customizing Lockdown Menu Templates

MobiControl allows you to modify pre-configured HTML menu templates or to build your own HTML menu templates. A menu template is an HTML file with special menu tags that get replaced by MobiControl when it generates the menu. Essentially, the menu tags get replaced by the menu item links that you configure for your program menu. The table below describes the special menu tags that get replaced in the HTML file.

The easiest way to create a custom program menu template is to make a copy of one of the default templates, customize it, and then add it to the list of available templates:

1. Select **Edit** in the **Lockdown Configuration** dialog box.
2. Create a copy of one of the default templates listed in the **Templates** dialog box. (Copy and paste it into another folder, e.g. My Documents.)
3. Edit the copied file according to the guidelines below and name the file appropriately.
4. Add the new template by selecting the **Add** button in the **Templates** dialog box.



Edit Menu Template List dialog box

The following table describes menu tags:

Tag Name	Description
<MCMenuFull>	This tag gets replaced with the full menu list that the user has configured. The menu items are separated by carriage returns. **Sample Menu Entries:** Pocket Word (\windows\pword.exe); Pocket Excel (\windows\pxl.exe); My Website (mywebsite.com) **Template:** <html> <body> <MCMenuFull> </body> </html> **Resultant Menu:** <html> <body> Pocket Word Pocket Excel My Website </body> </html>

<table>
<tr><th>Tag Name</th><th>Description</th></tr>
<tr><td><MCMenuN>
where "N" is the menu item number</td><td>This tag allows you to place each complete menu item where you want it in the HTML.

Sample Menu Entries

Pocket Word (\windows\ pword.exe)
Pocket Excel (\windows\ pxl.exe)
My Website (mywebsite.com)

Template

<html>
<body>
1. <MCMenu0>

2. <MCMenu1>

3. <MCMenu2>

</body>
</html>

Resultant Menu

<html>
<body>
1. Pocket Word

2. Pocket Excel

3. My Website

</body>
</html></td></tr>
<tr><td><MCLinkN> and <MCDispN>
where "N" is the menu item number</td><td>These tags let you further separate the menu item to be inserted into the "link" and the "display" text and control where in the HTML template they will be inserted.

Sample Menu Entries

Pocket Word (\windows\ pword.exe)
Pocket Excel (\windows\ pxl.exe)
My Website (mywebsite.com)

Template

<html>
<body>
1. <a href="<MCLink0>">

<MCDisp0>

2. <a href="<MCLink1>">

<MCDisp1>

3. <a href="<MCLink2>">

<MCDisp2>

</body>
</html>

Resultant Menu

<html>
<body>
1. Pocket Word

2.
Pocket Excel

3.
My Website

</body>
</html></td></tr>
</table>

Tag Name	Description
<MCExeIconN> where "N" is the menu item number	This tag lets you display the built-in icon for an application executable that is in the program menu. Sample Menu Entries: Pocket Word (\windows\pword.exe); Pocket Excel (\windows\pxl.exe); Calculator (\windows\calc.exe) Template: `<html> <body> 1. <a href=" <MCLink0>"> <img src=" <MCExeIcon0>"> </a>   2. <a href=" <MCLink1>"> <img src=" <MCExeIcon1>"> </a>   3. <a href=" <MCLink2>"> <img src=" <MCExeIcon2>"> </a>   </body> </html>` Resultant Menu: `<html> <body> 1. <img src= " %ExeIcon_ 1%%MCSTABLESTOREDIR%\ Lockdownimage\ MCLD_pword.bmp"> 2. <img src= " %ExeIcon_ 2%%MCSTABLESTOREDIR%\ Lockdownimage\ MCLD_excel.bmp"> 3. <img src= " %ExeIcon_ 3%%MCSTABLESTOREDIR%\ Lockdownimage\ MCLD_calc.bmp"> </body> </html>`

<table>
<tr><th>Tag Name</th><th>Description</th></tr>
<tr><td><MCDispImgN>
where "N" is the menu item number</td><td>This tag lets you associate a picture with an entry in the lockdown screen.
<table>
<tr><th>Sample Menu Entries</th><th>Template</th><th>Resultant Menu</th></tr>
<tr><td>Terminal Emulator (\Appl\Term\Term.exe)
Credit Card Sales (\Appl\CCard\CCSales.exe)
My Website (mywebsite.com)</td><td><html>
<body>
1. <a href= "<MCLink0>"> <img src =" <MCDispImg 0>">

2. <a href= "<MCLink1>"> <img src= " <MCDispImg 1>">

3. <a href= "<MCLink2>"> <img src= " <MCDispImg 2>">

</body>
</html></td><td><html>
<body>
1. <img src = "%MCSTABLESTOREDIR%\ Lockdownimage\ Term.png">

2. <img src= "%MCSTABLESTOREDIR%\ Lockdownimage\ CreditCardSales.jpg">

3. <img src= "%MCSTABLESTOREDIR%\ Lockdownimage\ MyWebsite.jpg">

</body>
</html></td></tr>
</table></td></tr>
</table>

Including Pictures in Menu Templates

You can insert images into your template by simply using the Insert Image feature in the built-in HTML Template Editor. MobiControl will deliver the image to the device. Alternatively, if you do not want to use MobiControl to deliver the image, you can simply specify in the HTML template the full path to the graphic for where it will be found on the mobile device (e.g. `<img src="file://\IPSM\images\CompanyLogo.jpg">`).

Using MobiControl Script Variables

If you generate your own custom menu template, you can use MobiControl script variables in your menu template. Using script variables allows you to display device or system information in the lockdown menu. Please see the "Script Variables" topic on page 424 for a full list of the various script variables that are available.

NOTES:

- MobiControl script variables are case-sensitive.
- When you use a script variable, you must enclose the variable name between "%" characters, in the same way that you would use them in an actual script.

EXAMPLE:

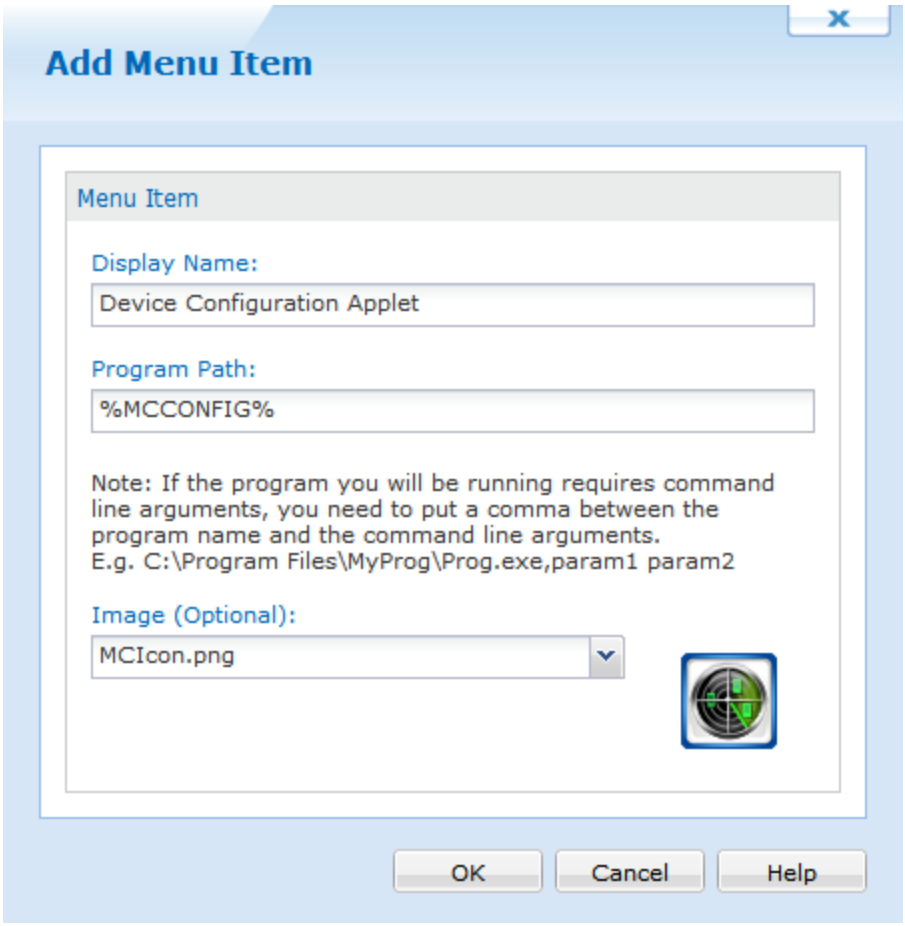
If an HTML template were to contain the line shown below, then when the lockdown menu is displayed on the device, the variable (including the leading and trailing "%" characters) would be replaced by the name of the device.

```
Device Name: %MCDEVICENAME%
```

Linking to the MobiControl Device Configuration Applet

The MobiControl device applet that is normally accessed by tapping on the MobiControl icon on the Today screen or system tray of the device contains a bounty of useful status information. This information can be very useful when trying to troubleshoot a problem in the field, for example resolving connectivity issues between the device and the MobiControl Deployment Server.

To create a link to the applet from the lockdown program menu add a program entry to the following path: `%MCCONFIG%`



Program menu entry for MobiControl Configuration Applet

IMPORTANT:

For WM devices, since you can't specify an exact page you can simply embed the following macro into the template: %MCCONFIG%
If %MCCONFIG% was specified in a earlier version of MobiControl with specific Tab controls to display, this option is no longer valid, but will still open the Configuration Applet.

NOTE:

When the MobiControl Device Configuration Applet link is applied in the lockdown menu, the end user has limited functionality of the settings. This is to prevent unauthorized modifications. The only functions that the user can access are the manual **Connect/Disconnect** button and **Log to File** check box in the **General** Tab, and the **Add** and **Test** buttons in the **Servers** tab. When the lockdown is accessed in Admin mode, the administrator has full control of the MobiControl Device Configuration Applet settings.

Embedding custom data variables

To insert custom data to your lockdown, click on **Edit** and **Insert Custom Data** button or click on the **Insert Custom Data** button on the toolbar. A new dialog window will open which will give you the option to select which custom data profile that has been previously created which you wish to include in your lockdown. As an alternative to pre-defined custom data you can explicitly include the Custom Data URL (REG://...) in the template.

If you wish to have a custom refresh mechanism within your lockdown use the following variable which refreshes the data on your lockdown screen: <a href="mc://home">Refresh<a>

EXAMPLE:

If an HTML template were to contain the line shown below, then the variable (including the leading and trailing "%" characters) would be replaced by the value.

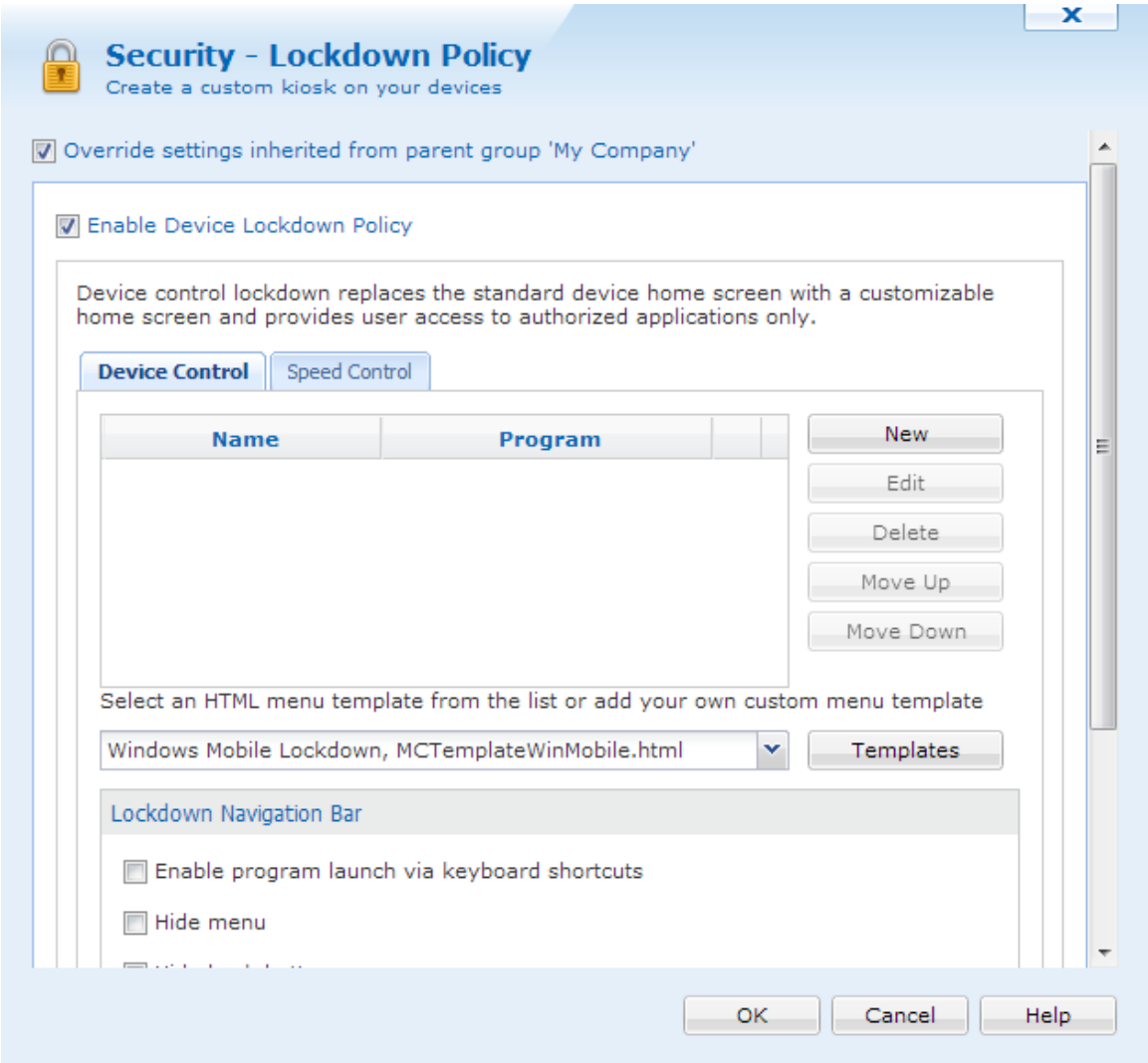
MobiControl Agent: %REG://HKEY_Local_
Machine\Software\APPS\SOTI\MobiControl\DeviceAgent?VN=Connection%
<a href="mc://home">Refresh<a>

Lockdown Menu Template Editor

In MobiControl, you can generate your own custom menu template. To edit the custom template, you can use your favorite HTML editor, or use the built-in editor available in MobiControl. When editing the HTML file be sure to preserve the special MobiControl Menu tags. These special tags are automatically replaced with the appropriate Program Menu entries by MobiControl.

Lockdown Menu

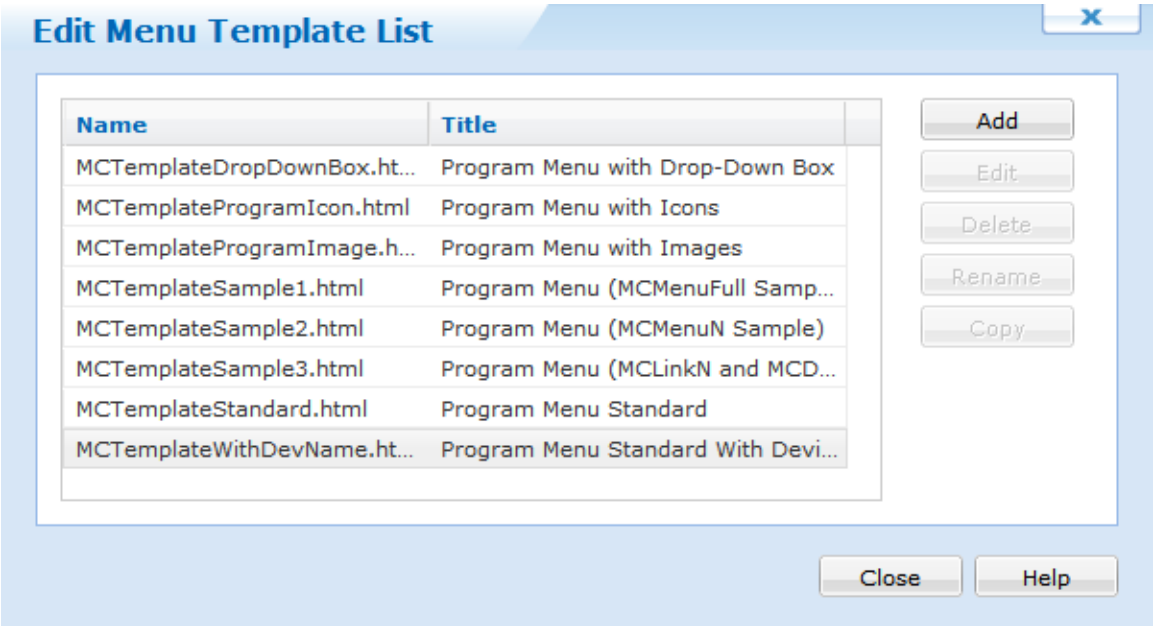
In the lockdown menu, you can select a template available in MobiControl. If you wish to use your own, click the **Templates** button and you will reach the **Template Menu List.**



Lockdown menu main screen

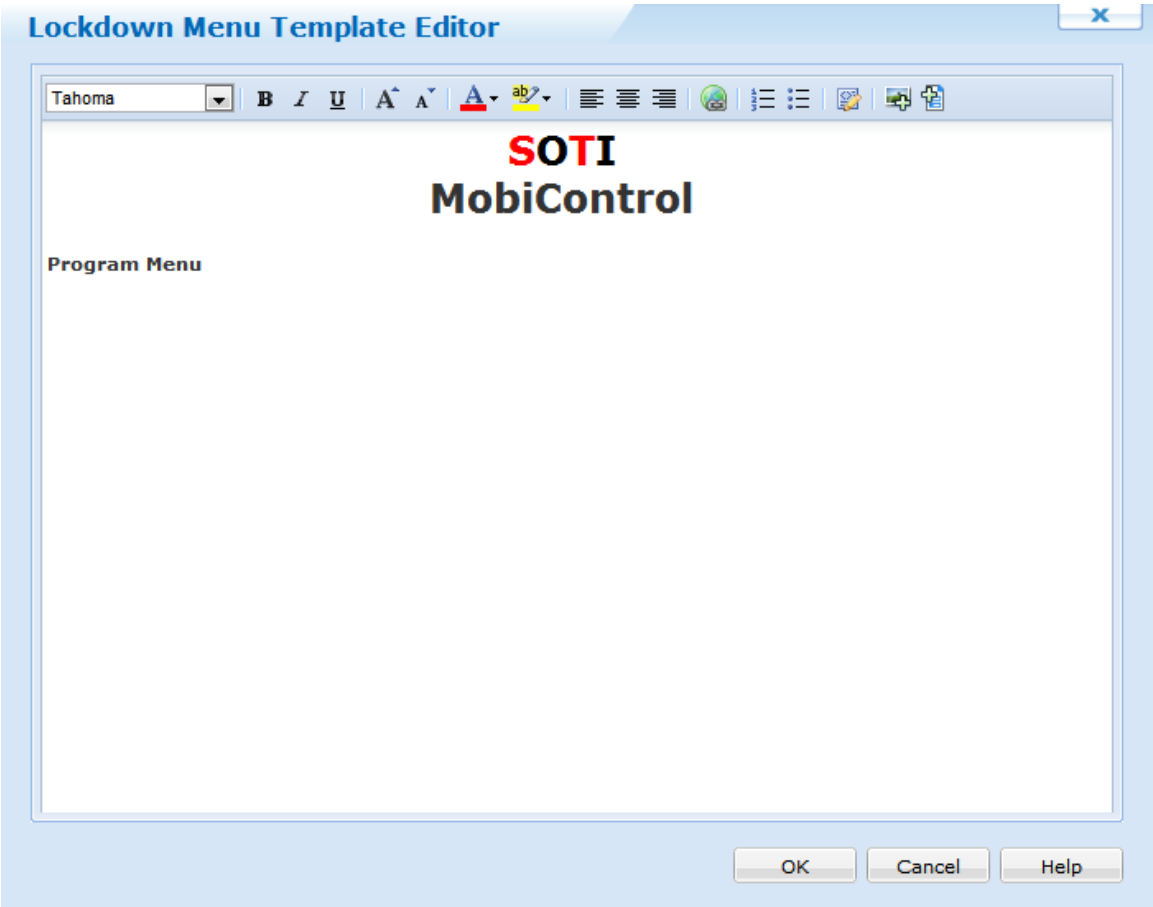
Edit Menu Template List

In the **Edit Template Menu List** dialog box, click **Add** and navigate to the location of your customized lockdown page and select it. You will see the customized menu template in this list now. You can chose to edit this template further by clicking on **Edit** and launching the lockdown menu template editor, or click on **Close** and then select the template from the **Lockdown Menu**.



Edit Menu Template List dialog box

You can edit the lockdown menu templates using the built-in HTML editor. In this editor, all the tags specific to MobiControl's lockdown templates are automatically colored green to highlight the special syntax. After saving a modified template, be sure to select the template file in the combo selection box on the main **Lockdown Configuration** page.



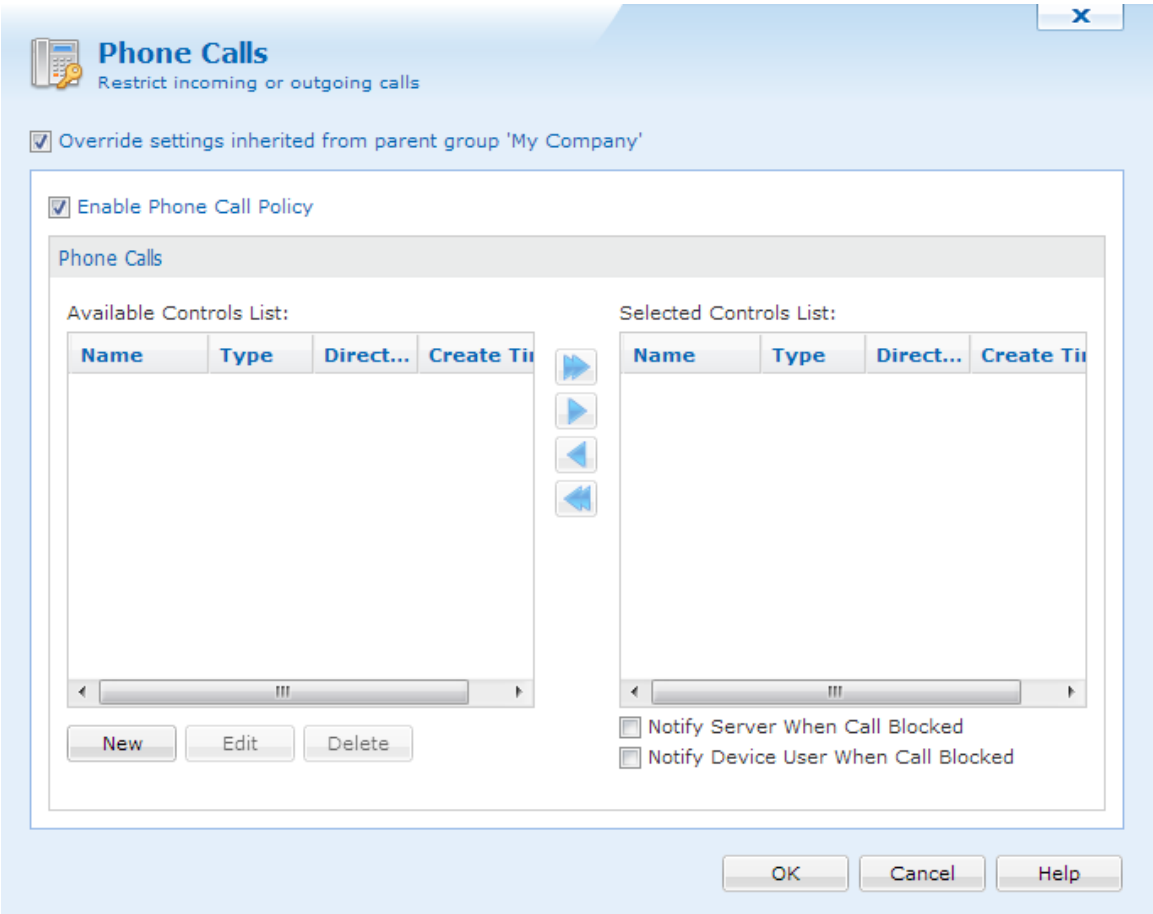
Lockdown menu HTML editor

TIP:

You can easily include a graphic in your HTML template by selecting the **Insert Image** menu option in the HTML Editor.

Windows Mobile Phone Call Policy

MobiControl provides various on-device feature controls including the capability to block various device communications, including what numbers a device is able to call or receive calls from.



Phone Call Policy dialog box

For assistance with Override Settings Click Here.

Phone Call Policy Control Lists

MobiControl allows you to specify the numbers to which users may place calls to and receive calls from:

1. The **Available Control Lists** displays all control lists that have been defined, but currently are not in use. IT administrators are able to create several different phone call policies without having them be activated on the devices.
2. The **Selected Control Lists** displays all currently activated control lists. Only the control lists included in the selected control lists are allowed to execute on the device. This provides an added layer of security for organizations concerned about unknown phone calls that may be placed from or received by the device. This can potentially happen without the end user being aware of it, as is frequently the case with viruses, spyware and other malicious applications.

NOTE:

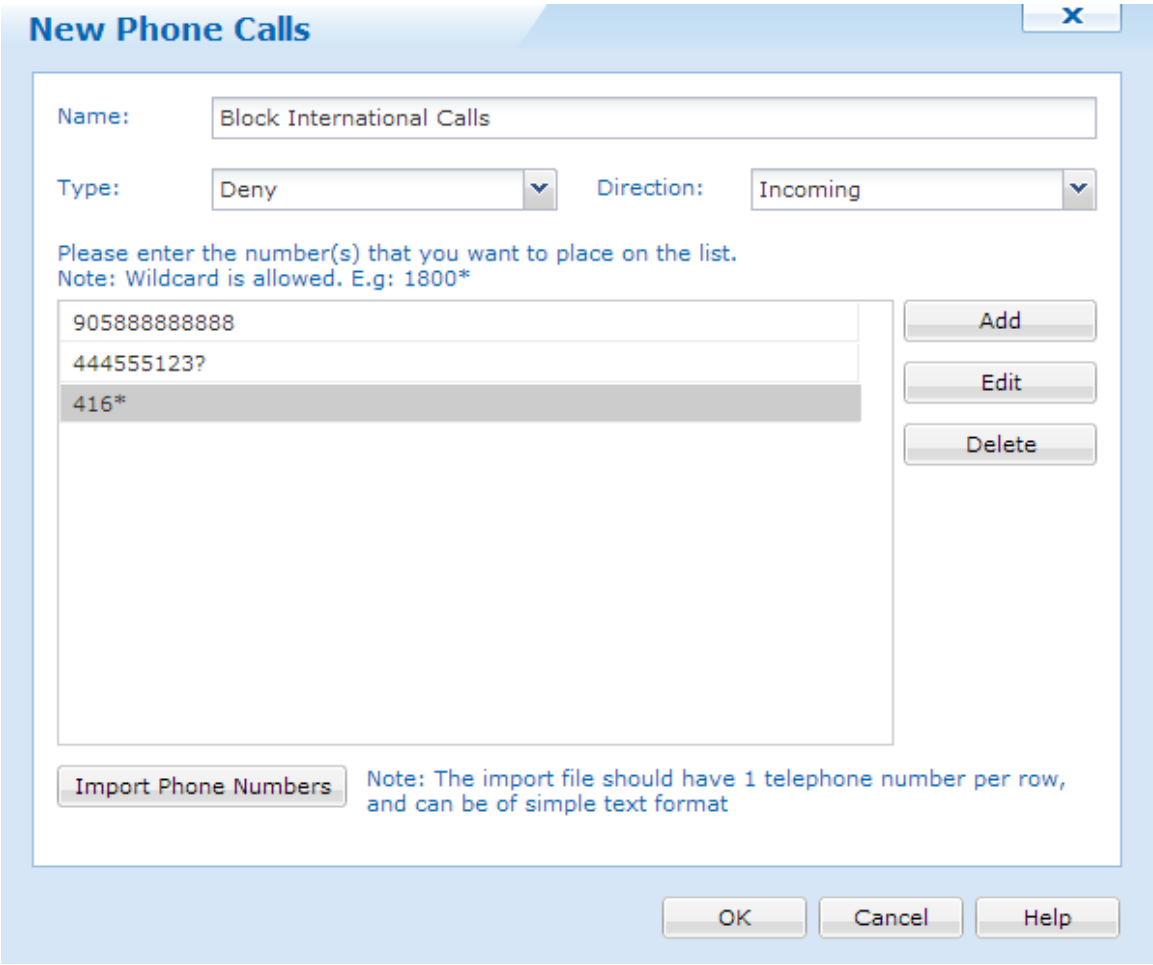
You can't have both deny and allow control lists activated at the same time. All control lists for a particular direction must be the same type.

IMPORTANT:

If the allowed list is not set up correctly, you may end up blocking or not allowing a potential system critical phone call.

3. When the **Notify Server on Call Blocked** check box is checked, the server's log file will output all calls that were blocked, along with the phone number that was trying to call in or out for the particular device.
4. When the **Notify User on Call Blocked** check box is checked, and the user receives an incoming call from a phone number that was blocked, a message box will be displayed

To enable phone call policy control for a device or group of devices, select **Phone Call Policy** from the MobiControl Device Configuration Center. (Please see the "Windows Mobile Device Configuration" topic on page 632.)



New Phone Call Policy entry dialog box

Field Name	Description
New	Clicking on this button allows you to create a new phone call policy with the dialog box as shown above. Assign a meaningful name to help distinguish between the various phone call policies you may setup.
Type	The available options allowed are either Allow or Deny. The type Allow indicates the phone calls that can either be placed from the phone or received by the phone or both based on Direction set for this policy. The type Deny indicates the phone calls that can not either be placed from the phone or received by the phone or both based on Direction set for this policy. If attempting to block restricted or unknown callers simply add **<unknown>** and/or **<restricted>** to the deny list.
Direction	The available options are Incoming, Outgoing, or Both. Incoming indicates that this policy is for calls received by the device. Outgoing indicates that this policy is for calls placed by the device. Both indicates that the policy is for both incoming and outgoing calls. For example, you may want to allow all communication to and from your device to your IT Support team and hence you would select both in this case with the appropriate phone numbers that can be dialled to work with your support team.

Once you have configured the Name, Type and Direction, click on Add in order to enter in the phone number(s) that the policy applies to and the dialog box is displayed above.

MobiControl will compare the number either received or placed with the list of numbers mentioned in the policy and compare the exact phone number displayed with the list of numbers you provide. If you have a series of numbers that you would like to enter in, there are a few options available, which can be used in combination with each other:

1. Leverage the wild card character, which is the asterisk, or '*'. The asterisk indicates any number of digits. For example, you may want to only allow calls coming from a particular area code. In this case, you can enter in '<area code>*' as the number.

   EXAMPLE:

   416* would match all calls that start with 416.

2. Leverage the single wild card character, which is the question mark, or '?'. The question mark indicates any single digit.

   EXAMPLE:

   You may want to allow communication to a list of phone numbers that only vary by a single digit. In this case, you can enter in as an example, 444-555-123?. This indicates the policy applies to the following list of numbers:
   444-555-1230
   444-555-1231
   444-555-1232
   444-555-1233
   444-555-1234
   444-555-1235
   444-555-1236
   444-555-1237
   444-555-1238
   444-555-1239
   Combinations of the two wild card characters can also be used if required. For example, 4??-555-12* would succeed if the phone number is 432-555-1234, but not if the phone number is 432-432-1234

When the Import Phone Numbers button is selected, a file explorer appears. From here you can select any text file that has **one number per line**.

EXAMPLE:

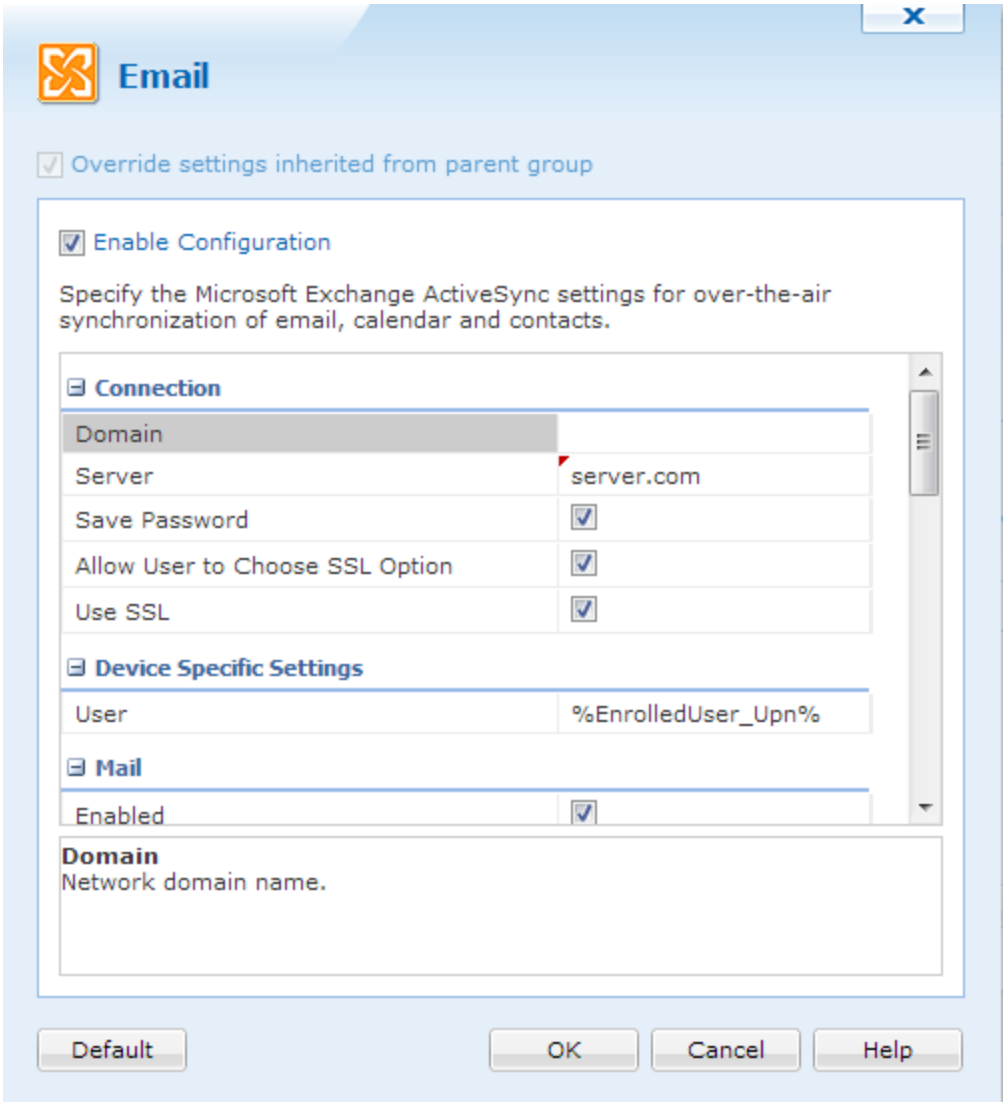
905-888-8888
519-222*
416*
Upon reading in the file, the individual numbers will be added to the list control, just as though they were individually typed in using the Add button.

IMPORTANT:

The file being imported must not contain more than 2000 lines.

Device Exchange ActiveSync

With MobiControl, you can configure Microsoft Exchange ActiveSync settings for your mobile device. To arrive at this configuration menu, select the device or the group, right-click, select **Configure Devices**, and click **Email**.



Connection Options

Field Name	Description
Domain	Enter the domain name of your organization.
Server	Enter the server address of your organization.
User Name Format	This specifies the way user names should be formatted to use on your system. The options include UPN, Domain/Username, Username or Prompt user.
Save Password	Check this box if you wish to have your password saved. If this box is unchecked, you will be asked to enter the password each time you perform synchronization. Also, this box must be checked for push email synchronization.
Allow User to use SSL Option	This option allows the end user to select whether or not SSL is used for communication with the Exchange server.
Use SSL	This option enables the SSL protection on the connection.

Device Specific Settings

Field Name	Description
User	Active Directory user name. Recommended to leave this blank. If the Active Directory authentication policy is enabled on the device, then this field will automatically be entered with the user's Active Directory user name. Please see the "Windows Mobile Authentication" topic on page 634 for more information.

Mail Options

Field Name	Description
Enabled	This option will enable email synchronization.
Sync the past	This option will synchronize all email entries for the past up to the specified number of days.
Limit e-mail size to	This option will control the maximum amount of data in the email message that can be used during email synchronization.
Include file attachment size smaller than (KB)	Any email with attachments smaller than the specified size, will be downloaded to the device upon synchronization.

Calendar Options

Field Name	Description
Enabled	This option will enable calendar synchronization.
Sync the past	This option will synchronize all calendar entries for the past up to the specified number of days.

Contacts Options

Field Name	Description
Enabled	This option will enable synchronization of contacts.

General Settings Options

Field Name	Description
Limit Calendar and Contact Notes to	This option will control the maximum amount of data that can be used during calendar notes and contacts notes synchronization.
Peak Start Time	This time specifies the beginning of the peak service for peak days.
Peak End Time	This time specifies the end of the peak service for peak days.
During Peak Times, Sync	This option specifies how frequently synchronization should occur during peak times.
During Off-Peak Times, sync	This option specifies how frequently synchronization should occur during off-peak times.
Sun / Mon / Tue / Wed / Thu / Fri / Sat	Select the days you want to include in your peak-time synchronization schedule
Sync when roaming	This option will allow automatic synchronization for the mobile device even when it is using a roaming data service.
Send outgoing items immediately	When sending items from the mobile device, you have a choice to send it immediately or after a delay. This option controls this setting to send items immediately or after a delay.
Delay sending messages (seconds)	This option specifies the time interval for the delay when sending an email from the mobile device

Tasks Options

Field Name	Description
Enabled	This option will enable synchronization of tasks.

NOTES:

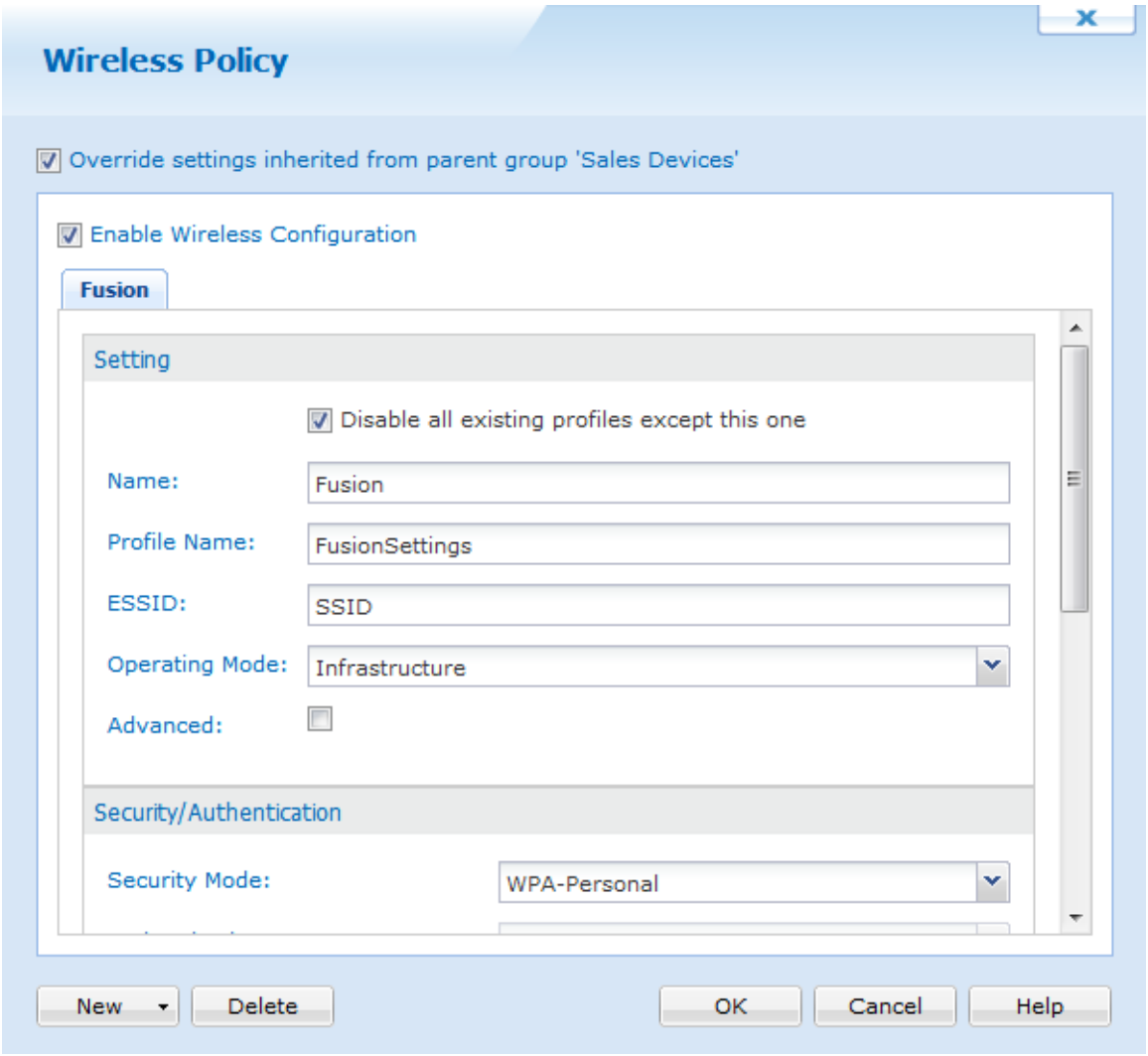
- It is recommended that you set up an authentication policy using Active Directory-based user authentication prior to using this feature. MobiControl will automatically set the user name when the Exchange settings are pushed down. You should leave the user name field below blank in this case, and MobiControl will automatically fill it in.
- If you need to deploy a certificate to the device (because the Root Certificate Authority certificate is not already in the devices certificate store), then you should do so using a package that includes a script to install it. Please see the "Script Command Set" topic on page 75.

Windows Mobile Wireless Policy

With MobiControl's Wireless policy, we are able to configure the WiFi connection on Windows Mobile devices.

This offers a way to safely and quickly configure the wireless connection on one device or hundreds.

To enable the Wireless Policy for a device or group of devices, select **Wireless Policy** from the MobiControl Security Center. (Please see the "Windows Mobile Device Configuration" topic on page 632.)



Device Feature Control Policy dialog box

MobiControl offers two ways to configure the Wireless on Windows Mobile devices. Fusion and ZeroConfig. Fusion is Motorola's wireless configuration utility while ZeroConfig uses Microsoft's configuration.

The default configuration setting for the Wireless Policy is for Fusion. Clicking New allows for new configurations to be made in either Fusion or ZeroConfig.

Fusion Settings

ZeroConfig Settings

If a policy is not needed anymore, select the policy and click Delete. After all configurations are done, click OK.

Advanced Settings for Windows Mobile / CE Devices

There are eight main aspects to device configuration. Each of these settings can be configured for a single device or applied at the device group level thereby configuring a set of devices. When the devices are moved from one device group to another in the device tree, the settings for the new device group are applied automatically to the devices. Please see the "Windows Mobile Device Relocation" topic on page 782 for more information on automatically re-configuring devices based on their location (using IP address or other custom criteria).

Custom Attributes

Custom Attributes allows us to create custom information that appears on the information panel on the right hand side of the web console. Please see the "Custom Attributes" topic on page 1343 for more information.

Custom Data

This option allows you to create your own monitoring fields to be shown in the Device Info window. This can be useful for monitoring various aspects of third-party applications. Please see the "Windows Mobile Custom Data" topic on page 700 for more information.

Connection Settings

This option allows you to configure connection settings for your mobile device(s), via. configure connection security by enabling or disabling SSL, select connection mode between persistent, scheduled and manual, change connection retry interval and set log file management, among other options. Please see the "Windows Mobile Connection Settings" topic on page 710 for more information.

Deployment Server Priority

This option allows you to specify the Deployment Server preferences for the devices. When a device is configured with more than one Deployment Server, it will try to connect to highest priority one first and if this server is not accessible, then it will try to connect to the next server available. Please see the "Windows Mobile Deployment Server Priority" topic on page 716.

Remote Control Settings

Select a device skin to display in the MobiControl Remote, and choose the connection profile to use when remote controlling the device. This allows for customized remote control settings, optimised for different types of connections, for instance, high-speed Wi-Fi or low-speed cellular connections). Please see the "Windows Mobile Remote Control Settings" topic on page 718.

Support Contacts Info

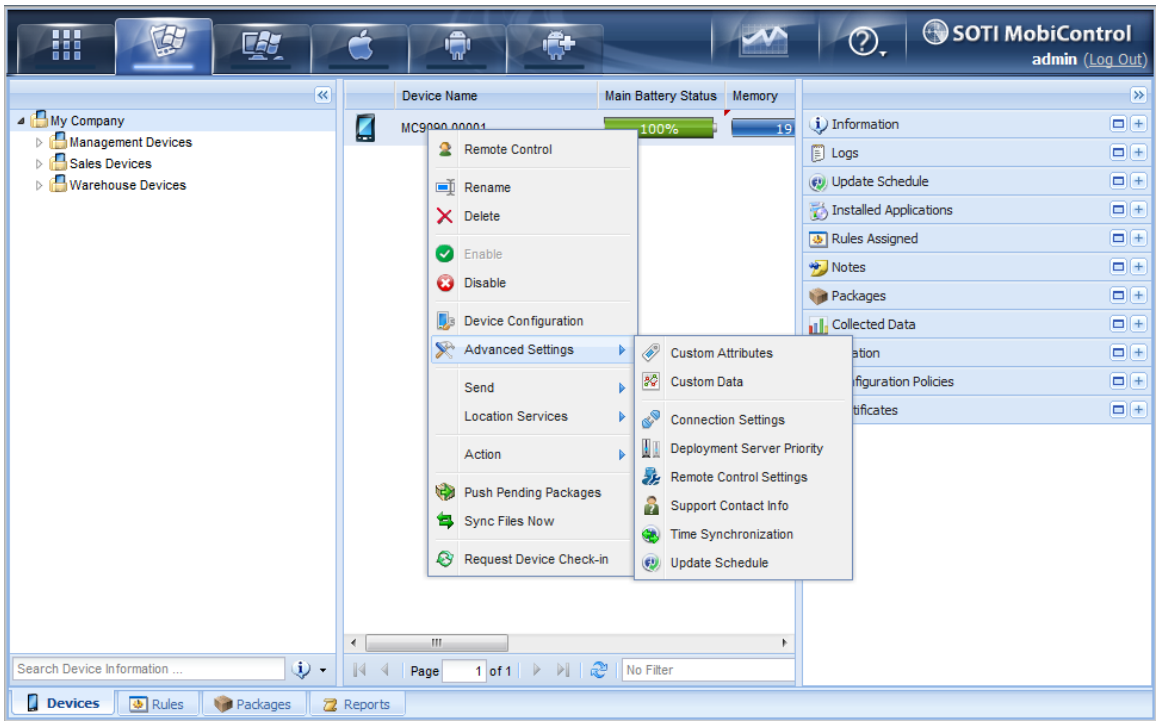
If users call support for their mobile device needs, configuring this option allows them to find the contact information reliably. Since this information is set centrally all information is updated once it's changed. Please see the "Windows Mobile Support Contacts Info" topic on page 719 for more information.

Device Time Synchronization

This option allows you to enable time synchronization for a mobile device, allowing the device to update its date and time settings by periodically synchronizing them with an SNTP/NTP time server or the MobiControl Deployment Server. Please see the "Windows Mobile Device Time Synchronization" topic on page 720.

Device Update Schedule

Adjust the interval at which the mobile devices contact the Deployment Server for new updates, configuration changes and packages. Please see the "Windows Mobile Device Update Schedule" topic on page 722.



Device Configuration Menu options

Custom Attributes

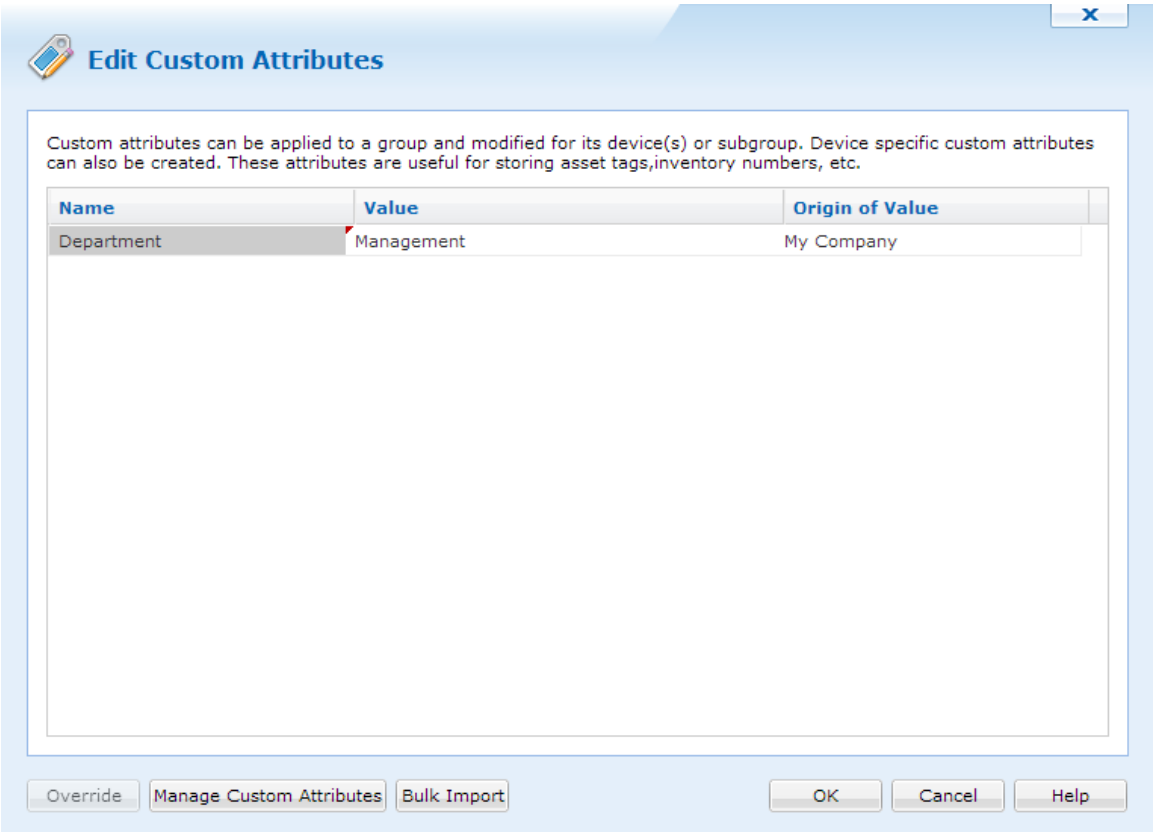
Custom Attributes allows us to create attributes to show in the information panel with our own data. This offers custom organization and labelling. For example, we can create a department attribute and put a different department for each device or device group.

Custom Attributes can also be propagated to devices so that they can be used in other applications and information.

NOTE:

Custom Attributes are available for all device types.

To set up Custom Attributes, right click a device or device group, go to Advance and click **Custom Attributes**.



Custom Attributes panel

The Custom Attributes panel has 3 columns: name, value and origin of value.

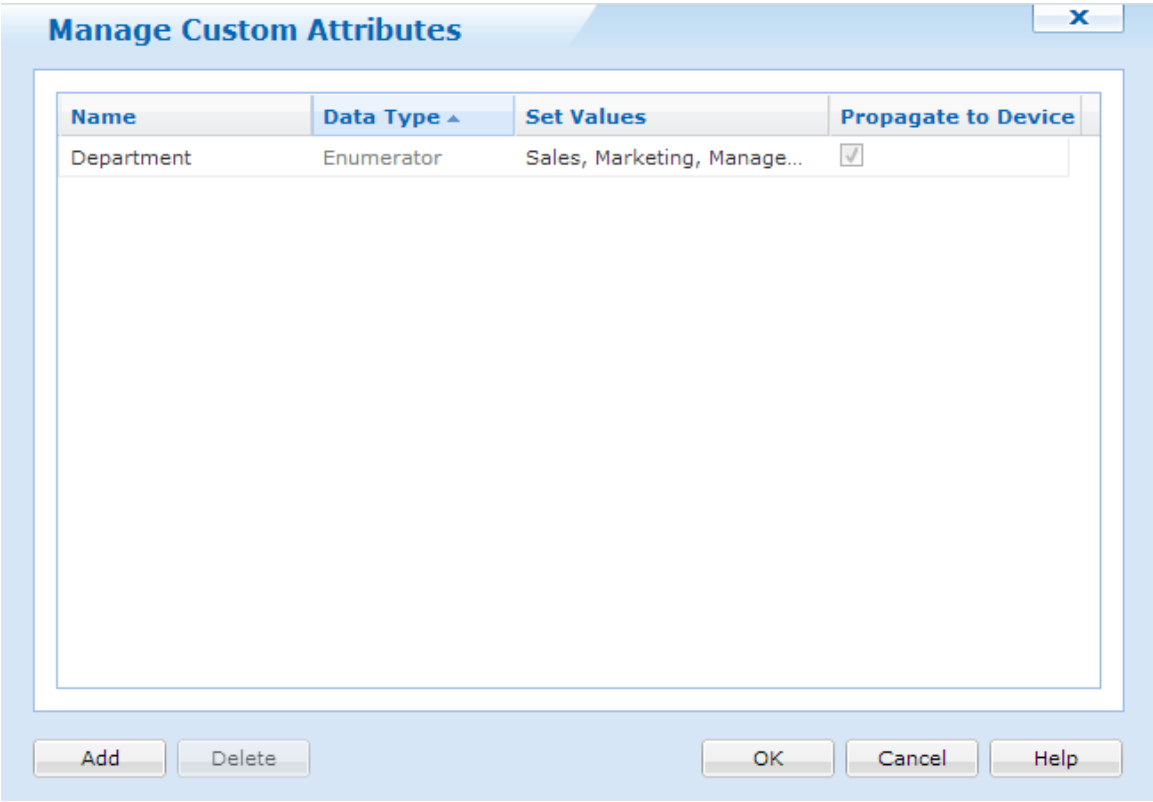
The name column shows the name of the Custom Attribute that will be shown in the info panel. Value contains the actual attribute for this field. Origin of value shows us where this field came from. For example, if Custom Attributes were set at the root level of the device tree, the origin of value will show the root level device group.

Clicking **Override** will change the origin of value to that where the device resides. This is useful if attributes change for each device. The Override button will change to **Remote Override** if we want to inherit the value from a parent group.

To create new attributes, click **Manage Custom Attributes**.

Manage Custom Attributes

When Manage Custom Attributes is clicked we a new dialog box appears. Here we will be able to create the Custom Attributes.



Manage Custom Attributes

Click  to add a new attribute.

When Add is clicked, a new row will appear. Clicking the field under name will allow us to name this attribute.

Data Types

There are 5 available data types to have for Custom Attributes:

- Text
- Numeric
- Date
- Boolean
- Enumerator

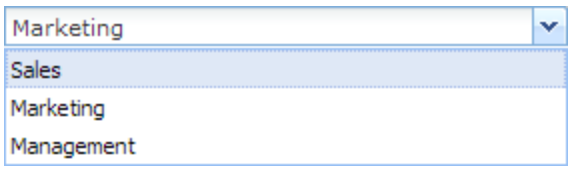
Text will allow us to create values with **letters and numbers**.

Numeric will allow us to create values with **only numbers**.

Date will allow us to set dates.

Boolean will create a checkbox for **yes or no / true or false**.

If we select enumerator, this allows us to create a drop down list when we set the attribute. To create the list, click the field in **Set Values** column. Here we can type the items we want in the drop down list. **Each value must be separated with a comma (,)**. For example, if we want to create a department attribute, we can have Sales, Marketing, Management. When we set this attribute, we will be presented with the drop down.



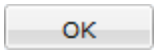
Enumerator Example

Propagate to Device

Checking this off will have MobiControl create the Custom Attributes in the pdb.ini file on the device. Applications can then read this file and pull the Custom Attribute value.

Bulk Import

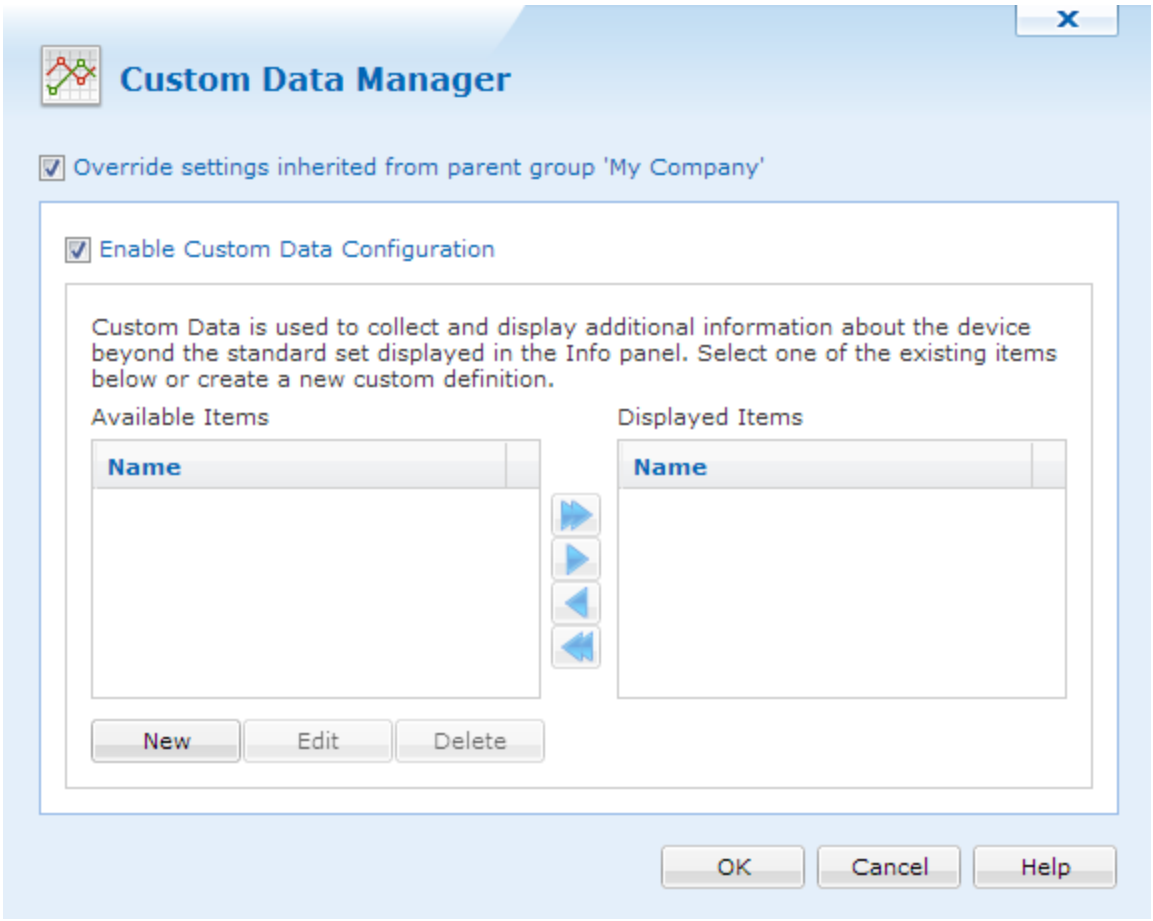
If there is a large amount of Custom Attributes to be inserted, we can do a bulk import so that everything is added at once.

Once everything is set, click 

to save and close the Custom Attributes.

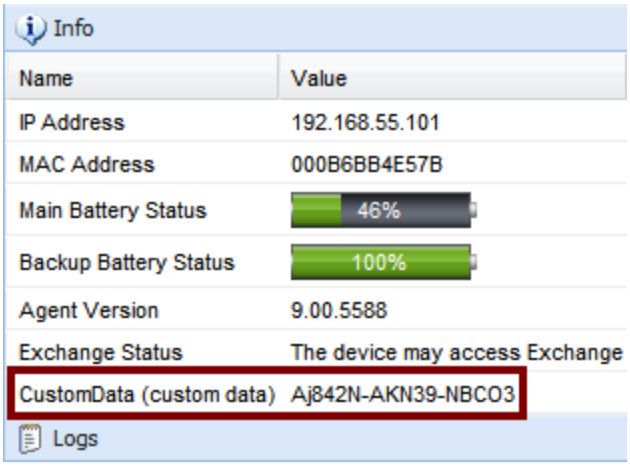
Custom Data

The custom data feature in MobiControl allows users to create their own monitoring fields to be shown in the **Device Info** window. This can be useful for monitoring various aspects of third-party applications. Custom data values are refreshed from the device when the device reconnects to the MobiControl Deployment Server and periodically, while the device status is Online, based on the device update schedule.



Custom Data Manager

The Custom Data Manager is accessible by right-clicking on a device or group, then selecting **Configure Device(s)** and clicking **Custom Data**.



The Device Info panel in MobiControl Manager

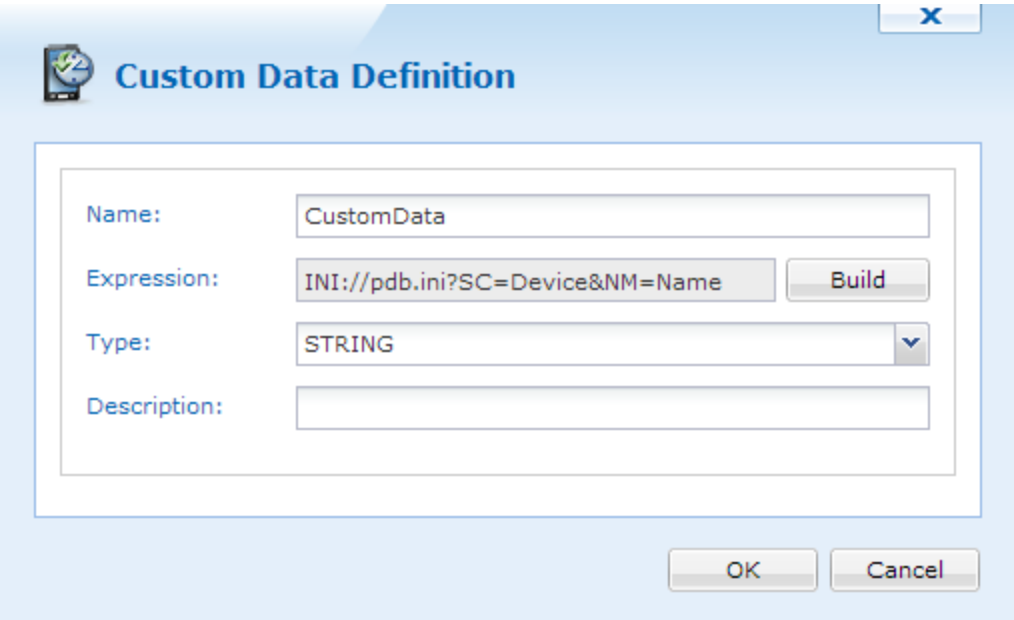
The following custom data types are available:

Type	Format and Description	Example
Text File	<Key>=TXT://\<FileName>?LN=<Value Number> Get the content of specified line of the text file (if LN is not specified, it assumes the first line)	TXT://\Device.log?LN=1
Registry	<Key>=REG://<GlobalKeyName>\<RegistryKey>?VN=<ValueName> Get a value from the registry. <GlobalKeyName> can be one of: • HKEY_CLASSES_ROOT • HKEY_CURRENT_USER • HKEY_LOCAL_MACHINE • HKEY_USERS	REG://HKEY_LOCAL_MACHINE\Software\Apps\SOTI\MobiControl?VN=Version
.INI File	<Key>=INI://\<FileName>?SC=<SectionName>&NM=<ValueName> Get a value from a Section in an .ini file.	INI://\SOTI\pdb.ini?SC=Device&NM=DeviceName
Exit Code	<Key>=EXE://\<Executable> [<ArgumentList>] Get the exit code of the executable	EXE://\windows\system32\calc.exe
STDOUT	<Key>=STDOUT://<Executable> [<ArgumentList>] Get the first line of STDOUT output of the executable.	STDOUT://cmd.exe /c dir
Static	<Key>=Text Enter the static value to display in the device info pane. This information is not based on any value on the device but based on user input.	OwnerName="X & Y Corporation, SalesDepartment"

Editing Custom Data

Configuration of custom data entries is performed through the Custom Data Manager which can be accessed by highlighting the device or the device group and selecting **Custom Data** from the **Configure Device(s)** option in the **Device** menu.

You can use the buttons in the **Custom Data Setting Manager** dialog box to add new entries, edit existing entries and change the order position of the custom data entries as displayed in the **Info** window.

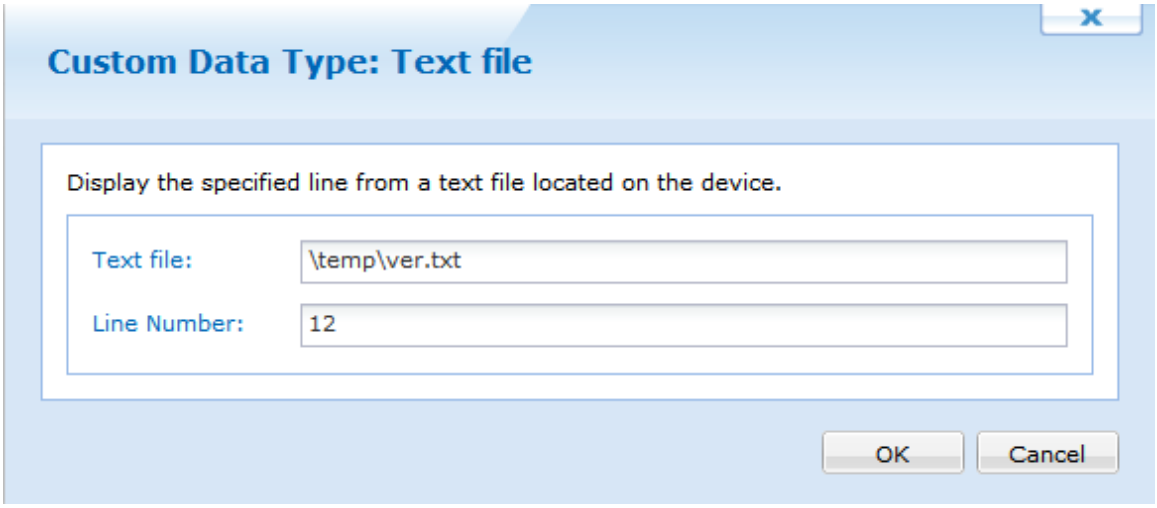


Custom Data Definitions window

The following table describes the fields in the **Custom Data Definition** dialog box.

Field Name	Description
Name	Name of the custom data field that you want to show in the device info pane
Expression	The build button can be used to create a definition which will be used to collect the custom data values.
Type	Default is set to "String." This setting is only recommended when doing custom data collection. Other options are "Float" and "Integer."
Description	A brief note describing the nature of the custom data query and its purpose. This description is shown in the device info pane when the custom data field is selected.

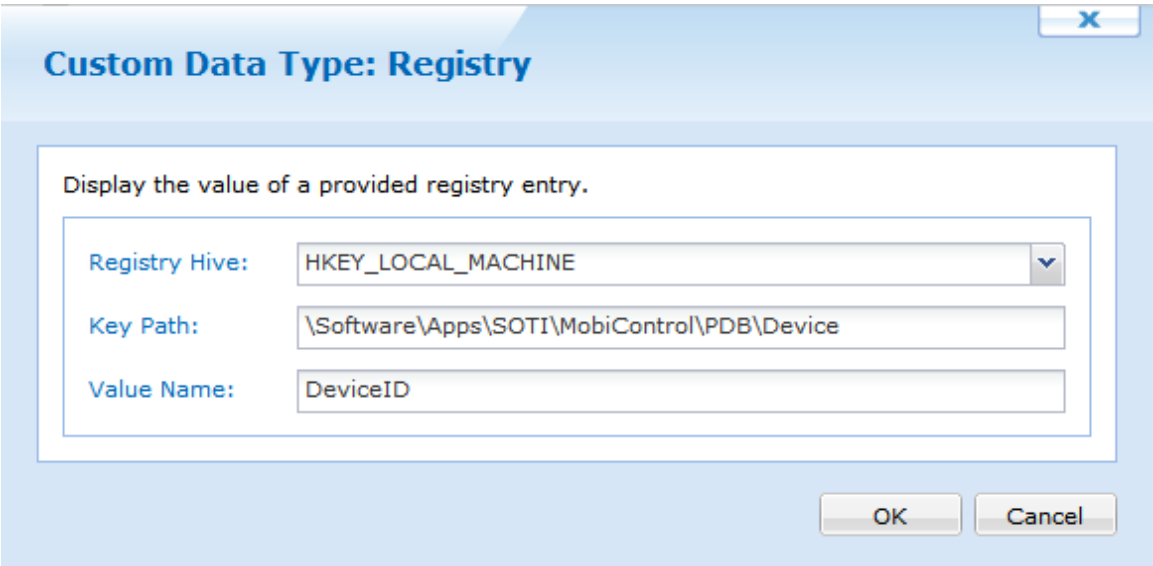
Custom Data: Text Files



The following table describes the fields in the **Custom Data Type: Text File** dialog box.

Field Name	Description
Text File Name	Specify the location of the text file on the mobile device.
Line Number	Specify the line number that should be read from the text file and displayed in the device info pane.

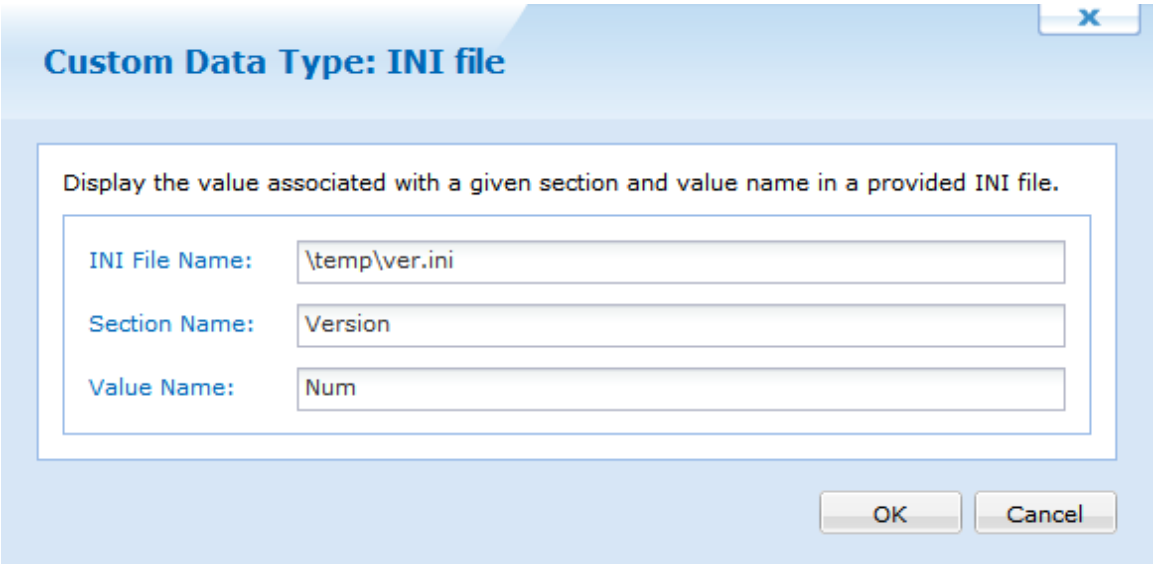
Custom Data: Registry



The following table describes the fields in the **Custom Data Type: Registry** dialog box.

Field Name	Description
Registry Hive	Specify the registry hive where the information is located.
Key Path	Specify the exact path of the value that needs to be read.
Value Name	Specify the name of the value that should be ready and displayed in the device info pane. **NOTE:** Only `REG_SZ` and `REG_DWORD` value types are supported.

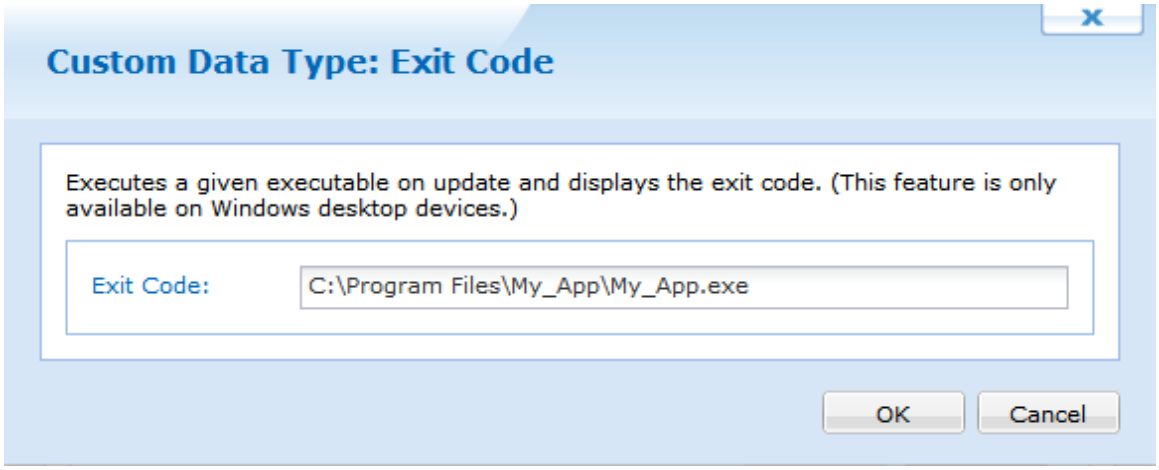
Custom Data: .Ini File



The following table describes the fields in the **Custom Data Type: INI File** dialog box.

Field Name	Description
INI File Name	Location of the `.ini` file on the mobile device
Section Name	Section from which the value should be read
Value Name	Value that should be read from the `.ini` file and displayed in the custom data field in the Device Info panel

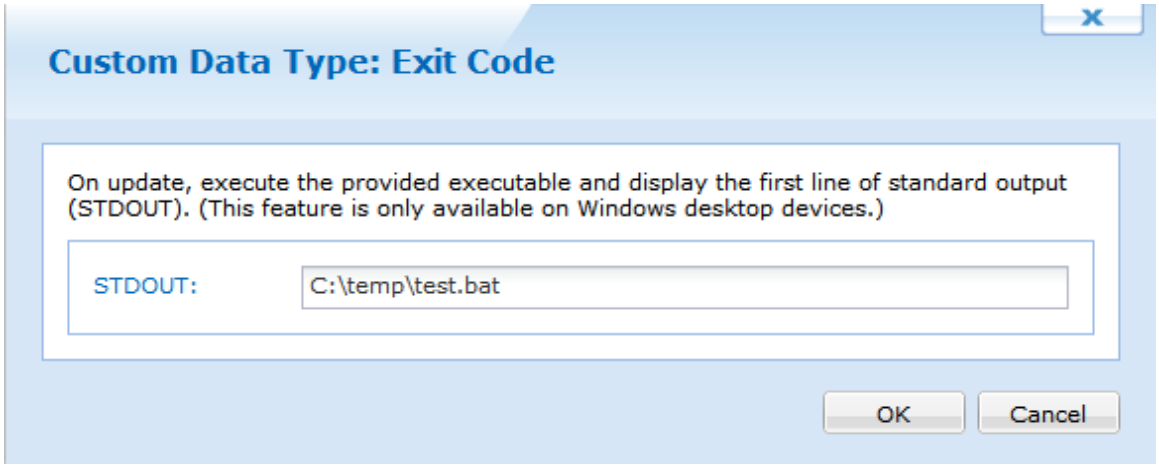
Custom Data: Exit Code



The following table describes the field in the **Custom Data Type: Exit Code** dialog box.

Field Name	Description
Command Line	Display the exit code of the application or command line instructions once they are executed.

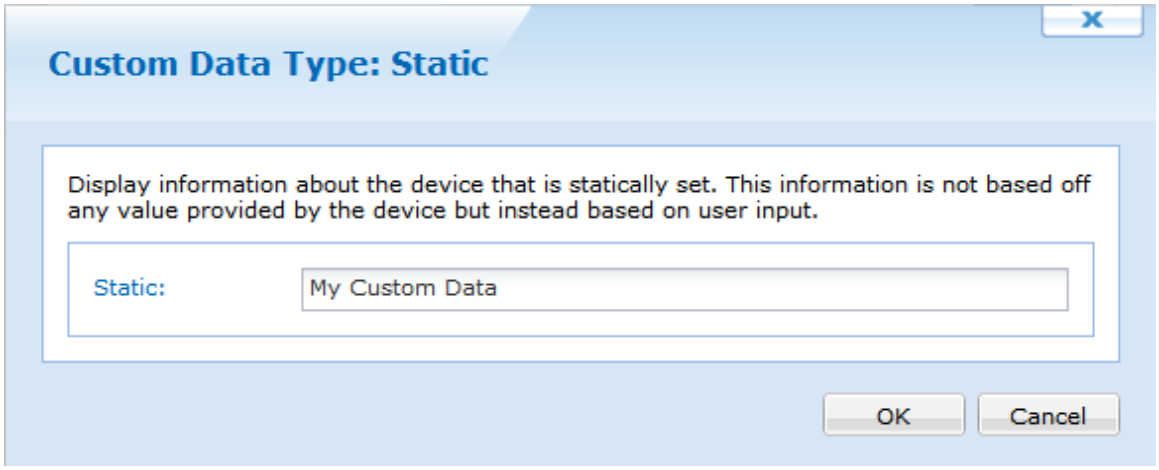
Custom Data: STDOUT



The following table describes the field in the **Custom Data Type: STDOUT** dialog box.

Field Name	Description
Command Line	Enter the command line instructions that should be executed and the first line of the return is displayed in the device info pane.

Custom Data: Static Data



The following table describes the fields in the **Custom Data: Static Data** dialog box.

Field Name	Description
Static Value	Enter the static value here to display in the device info pane. This information is not based on any value on the device but based on user input.

Embedded Query

A query string can be in another query string by using the format `%<KeyName>%`. The embedded query must be defined before the query. It works only in static type query and there has to be one static custom data type for every embedded query.

EXAMPLE:

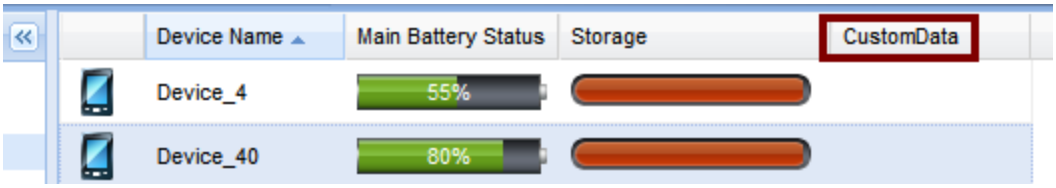
```
Key1=TXT://\RegLocationSSID.txt?LN=1
Key2=REG://%Key1%
```

Limitations

- All result values are limited to 250 characters. They will be truncated if this limit is exceeded.
- All Query Key Names are limited to 80 characters.
- All query strings (URLs) are limited to 250 characters.
- Typing "`STDOUT`" works on DOS and Desktop Agent. It doesn't work on CE and Pocket PC Agent.

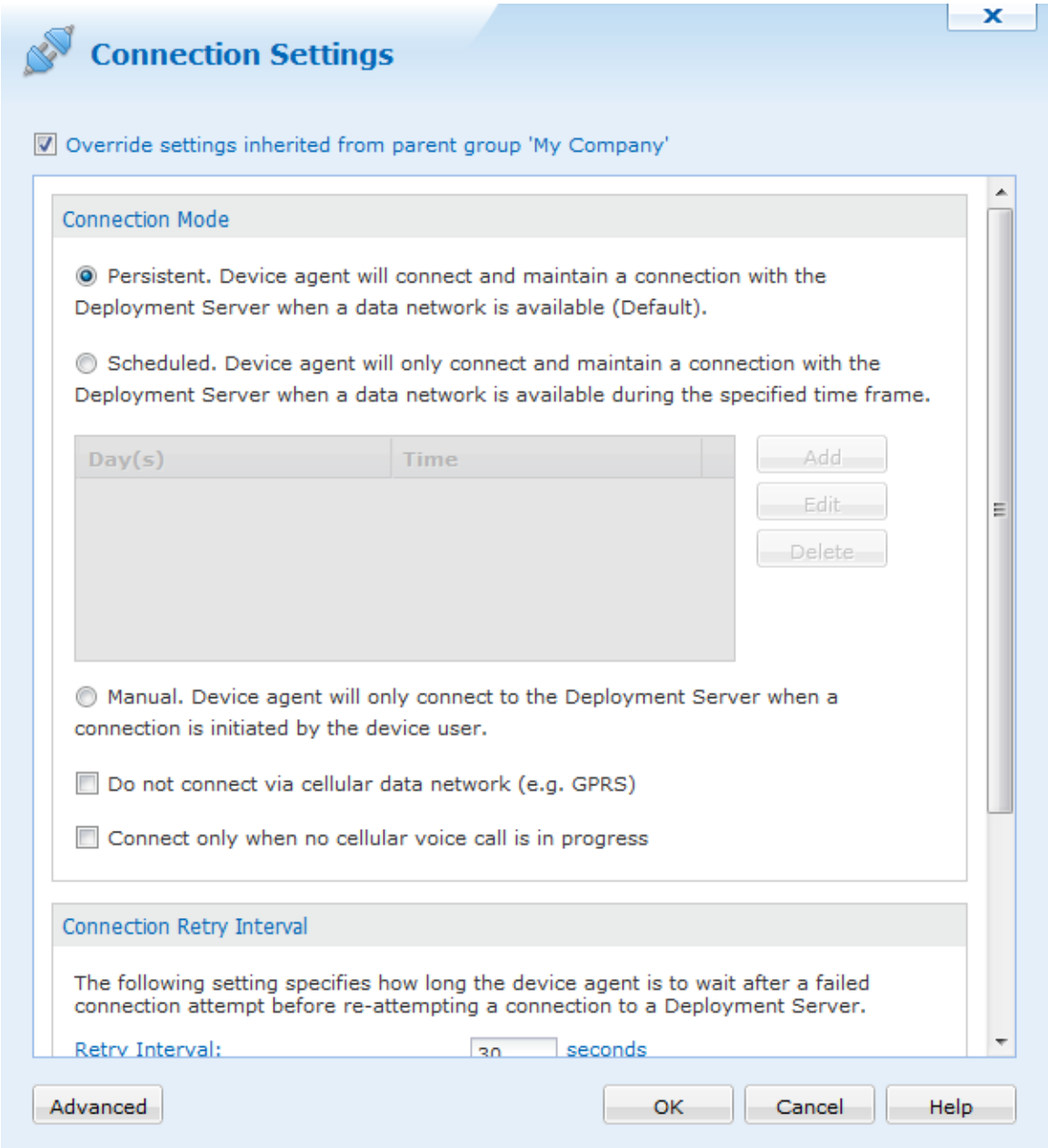
Custom Data Device Column

Once custom data has been configured, you can display or hide these custom data. Right-click on the device tree header or white space in the device tree and select **Custom Data**. You can also choose to display or hide the predefined data values displayed in the list.



Windows Mobile Connection Settings

To access the **Connection Settings** dialog box, right-click on a device or device group, point to **Advanced Settings,** and select **Connection Settings.**



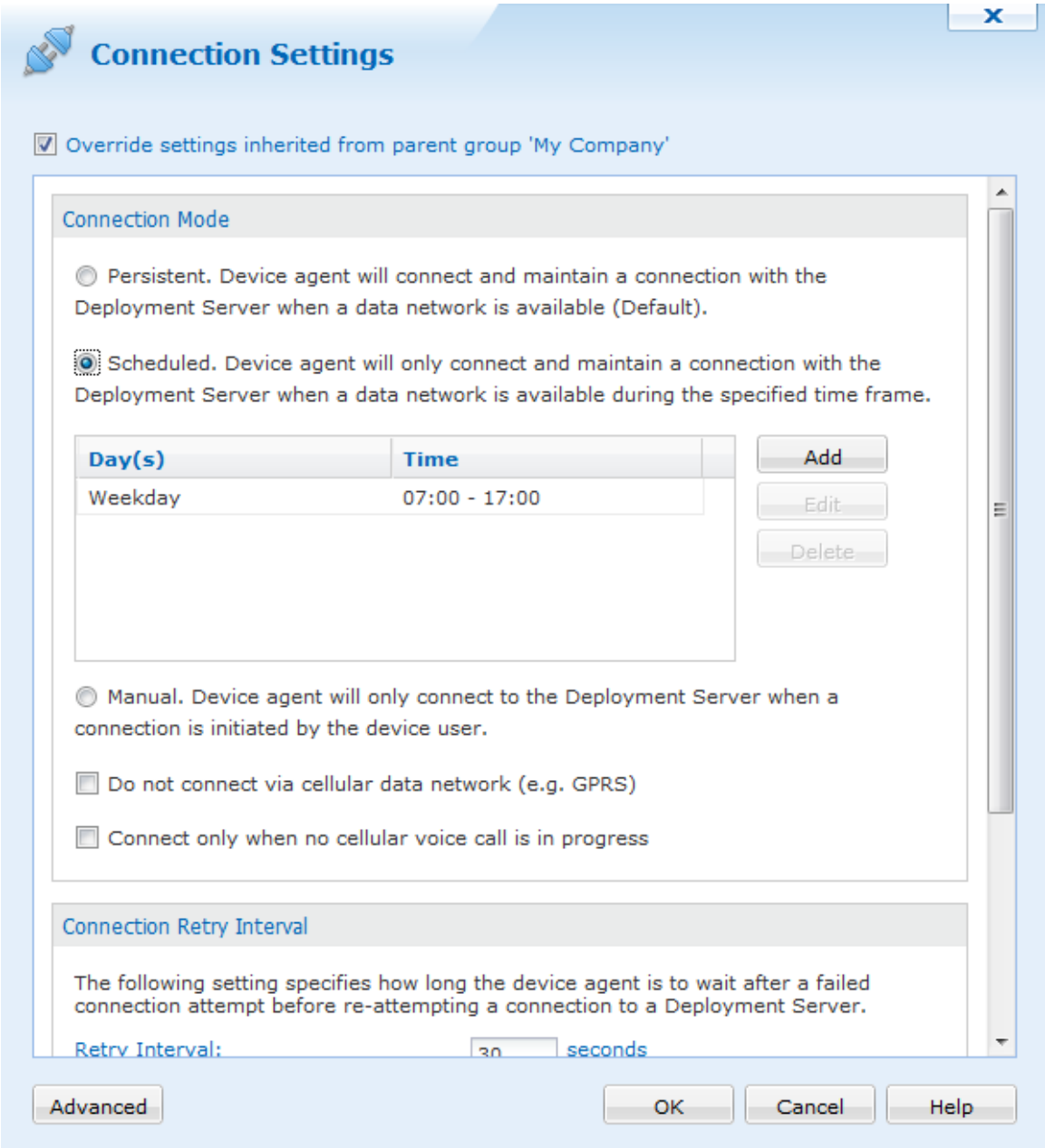
Connection Settings tab

Connection Mode

In any connection mode, the Device Agent does not force the mobile device to establish a network connection; it only takes advantage of an existing network connection.

Option	Description
Persistent	In this mode of operation the Device Agent will persistently try to establish and maintain a TCP/IP connection with the Deployment Server. This maximizes the amount

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>of time the device is connected to MobiControl, ensuring that it is able to quickly receive updates and available for remote control.
This is the recommended mode of operation for most installations.</td></tr>
<tr><td>Scheduled</td><td>In this mode of operation the Device Agent will only attempt to establish and maintain a TCP/IP connection with the Deployment Server during the defined time periods. Within the set time periods, the Device Agent operates in a "persistent" mode. Outside of the set time periods, the Device Agent will remain disconnected from the Deployment Server unless a connection is manually initiated by the device user.
This is the recommended mode of operation for installations where it is not necessary for the device to always be connected to the Deployment Server.
It is important that the time frame configured takes into consideration the device update schedule, and file synchronization schedules. These schedules can only be executed when the device is connected to the Deployment Server.
  TIP:
If you are experiencing aggressive battery consumption with the persistent connection mode, switch to the Scheduled mode, and specify a narrow time frame (e.g. 1–2 hours)</td></tr>
<tr><td>Manual</td><td>In this mode of operation the Device Agent will never automatically attempt to establish a connection to the Deployment Server. Connections must be initiated by the device user via the device configuration applet.
This is the recommended mode of operation for installations where only the remote help desk facilities of MobiControl are being used (not using deployment rules or file sync rules), and it is acceptable and/or required that the device user initiate the connection to the Deployment Server.
  NOTE:
The device must be connected to the Deployment Server in order for a remote help desk session to be established via the "TCP/IP(SERVER)" profile.</td></tr>
<tr><td>Do not connect via cellular data network</td><td>This option prevents the MobiControl Agent from connecting to the server via a data network on the device, e.g. GPRS. It can still connect using any other connection, e.g. Wi-Fi.
Don't use the Connect button on the Device Agent to test the device connection, since the MobiControl Manager (when the setting is implemented) will always allow a connection through GPRS. Instead you can use Disable device then Enable device on the MobiControl Manager to see if the device can connect through GPRS.</td></tr>
<tr><td>Only connect when no voice call in progress</td><td>When a voice call is in progress on a cellular phone device, the data service may or may not be available. To prevent the Device Agent from attempting to establish a connection while a voice call is in progress select this checkbox.</td></tr>
</table>



Add Schedule Entry settings dialog box

Connection Retry Interval

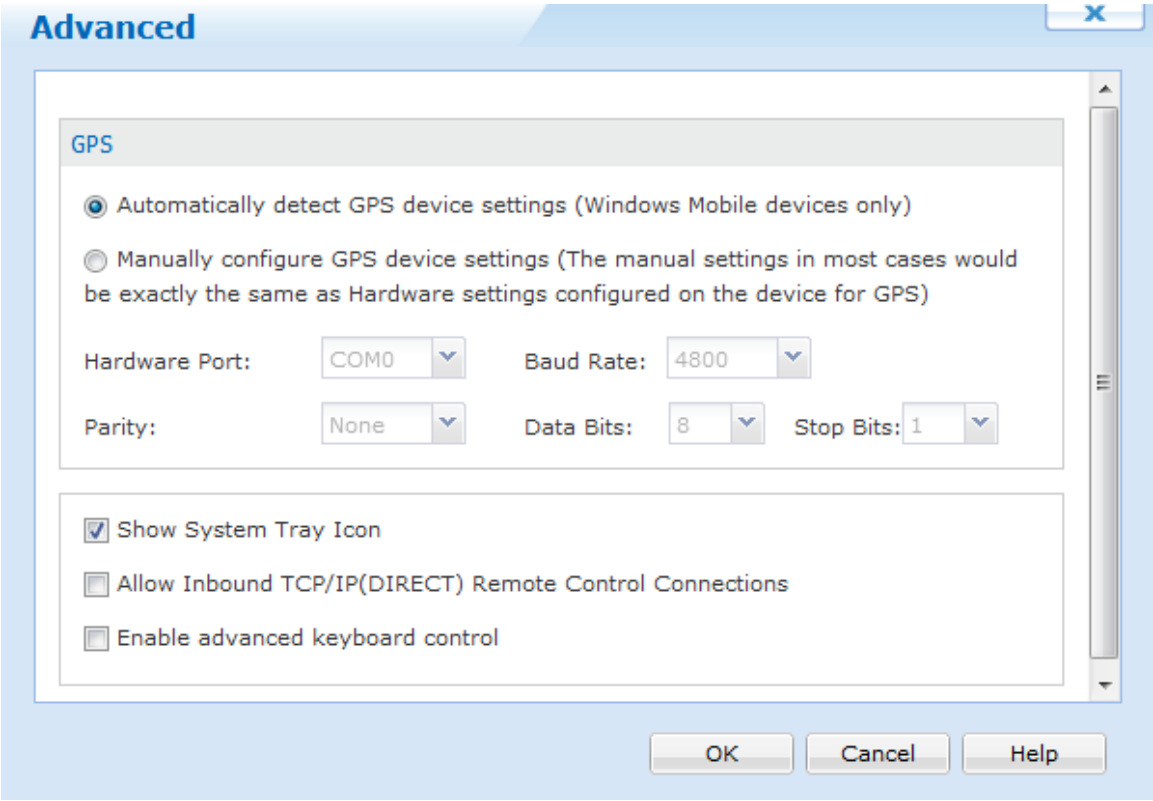
This setting determines how long the Device Agent should wait before trying to contact the Deployment Server again after a failed attempt. If your device will experience long periods disconnected from the Deployment Server, you should set this value high in order to prevent battery drain.

Log File Management

This set of options allows you to tune how the debug log files are managed on the device. Log management works by waiting for the log file to grow to a maximum threshold. Once the given threshold is met, the log file size is reduced down to the given minimum threshold by purging all the older entries.

Option	Description
Minimum Log File Size	Threshold size up to which the log file will be purged.
Maximum Log File Size	Threshold size, reaching which will trigger the log file to be purged to the minimum log file size
Enable Debug Logging (Normally Off)	Enables event logging on the mobile device. All MobiControl-related activity and events will be logged to a log file.The log file can provide vital information to IT support staff in diagnostics and resolving any issues that might have been reported for the mobile device with respect to MobiControl. The mobile device may operate more slowly with this option checked. **IMPORTANT:** Debug logs generate a large amount of file system traffic and as such, should only be enabled when you are debugging a problem. In particular, on Windows Mobile 5 devices, this intense logging activity can reduce the life of your flash memory if left on indefinitely.

Advanced Device Agent Configuration



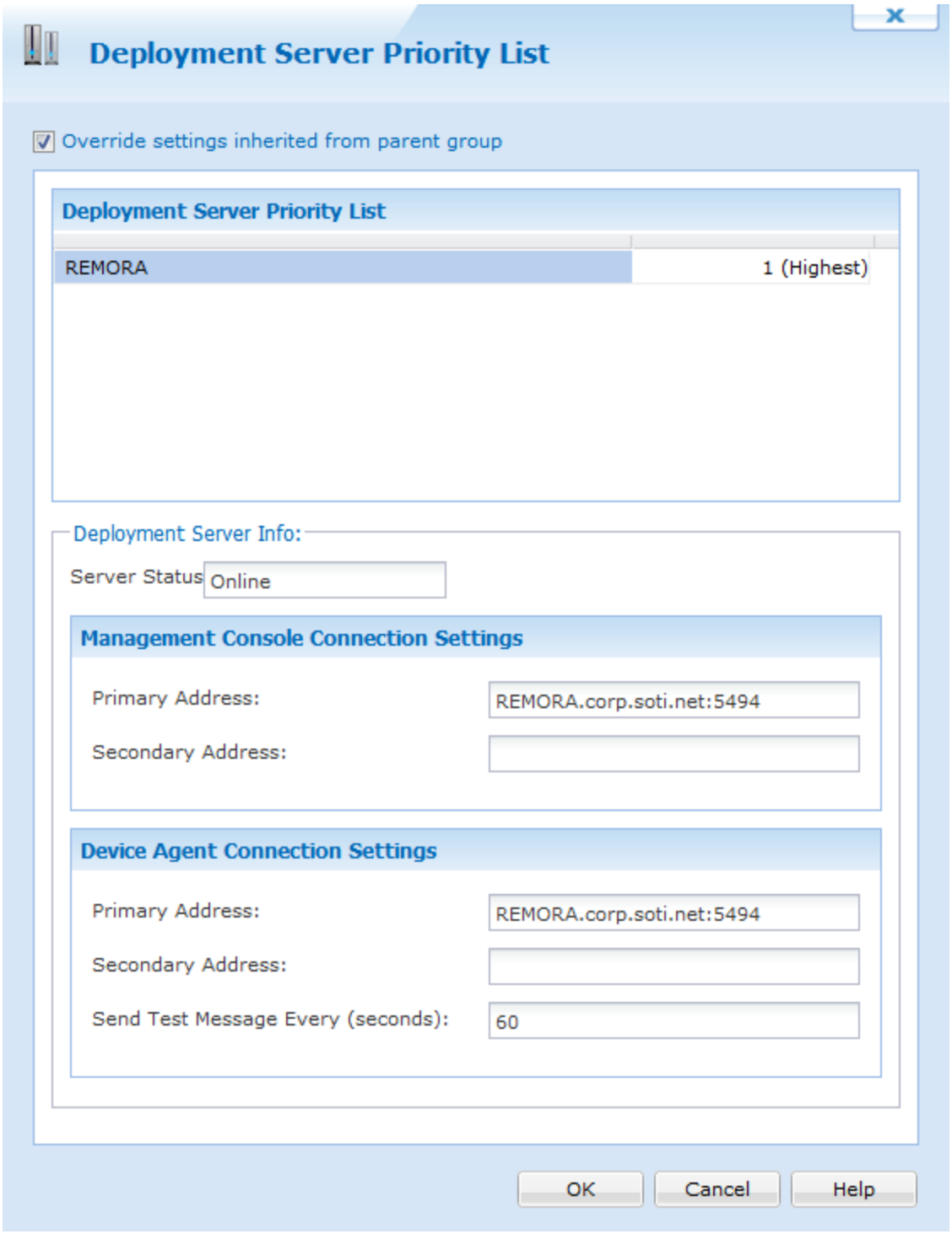
Connection Settings Advanced tab

The advanced settings allow us to configure GPS and other details on Windows Mobile.

Option	Description
Automatically Detect GPS Device	Automatically Detects the devices GPS settings, and uses those to locate the Device.
Manually Configure GPS Device	Enter the GPS Configuration settings for your specific devices. These settings can be obtained from the device manufacturer if you are un aware of them.
Show System Tray Icon	Enables the MobiControl Agent icon to be displayed on the device's system tray
Allow Inbound TCP/IP Connections	Enable the agent to listen and accept inbound TCP/IP remote control connections. When unchecked, you can remote control this device through "Remote Control Device via TCP/IP (SERVER)," but you cannot remote control this device by through "Remote Control Device via TCP/IP (DIRECT)."
Enable Advanced Keyboard Control	Enables the hardware keys on the device to be used by third party applications when the lockdown is engaged.

Deployment Server Priority

The **Deployment Server Priority List** dialog box allows you to specify the Deployment Server preferences for the devices. Priority one is the highest and five is the lowest. When a device is configured with more than one Deployment Server, it will try to connect to highest priority one first. If this server is not accessible, then it will try to connect to the next server available.



Deployment Server Priority List dialog box

Multiple servers may be assigned the same priority level to establish a pool of Deployment Servers to balance the load of a large number of devices.

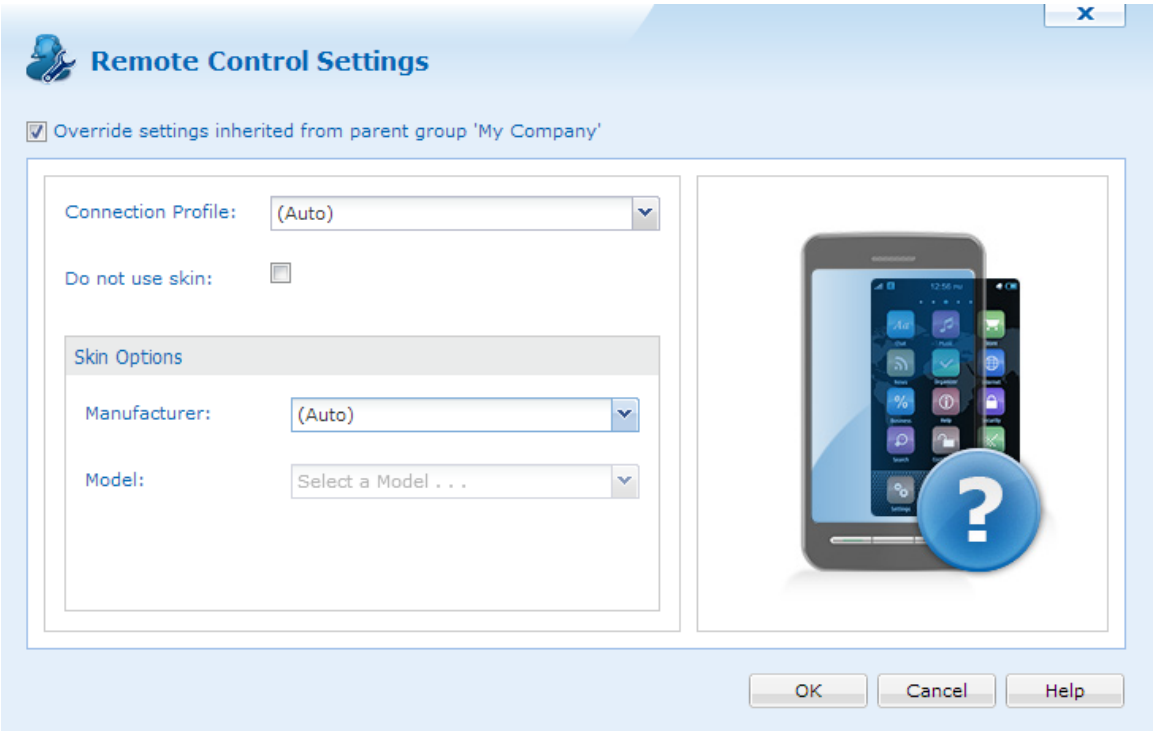
If you select "Not used," the selected devices will not connect to that Deployment Server.

We can also see the primary and secondary addresses for both the Management console and device agent connection setting here.

Deployment Server priority is only applicable when you have installed multiple Deployment Servers using the same site name. Please see the "Configuring MobiControl Manager" topic on page 399 for more information.

Windows Mobile Remote Control Settings

In the **Remote Control Settings** dialog box, it's possible to select a device skins and connection profiles. Skins for these devices should appear automatically depending on the device agent created.



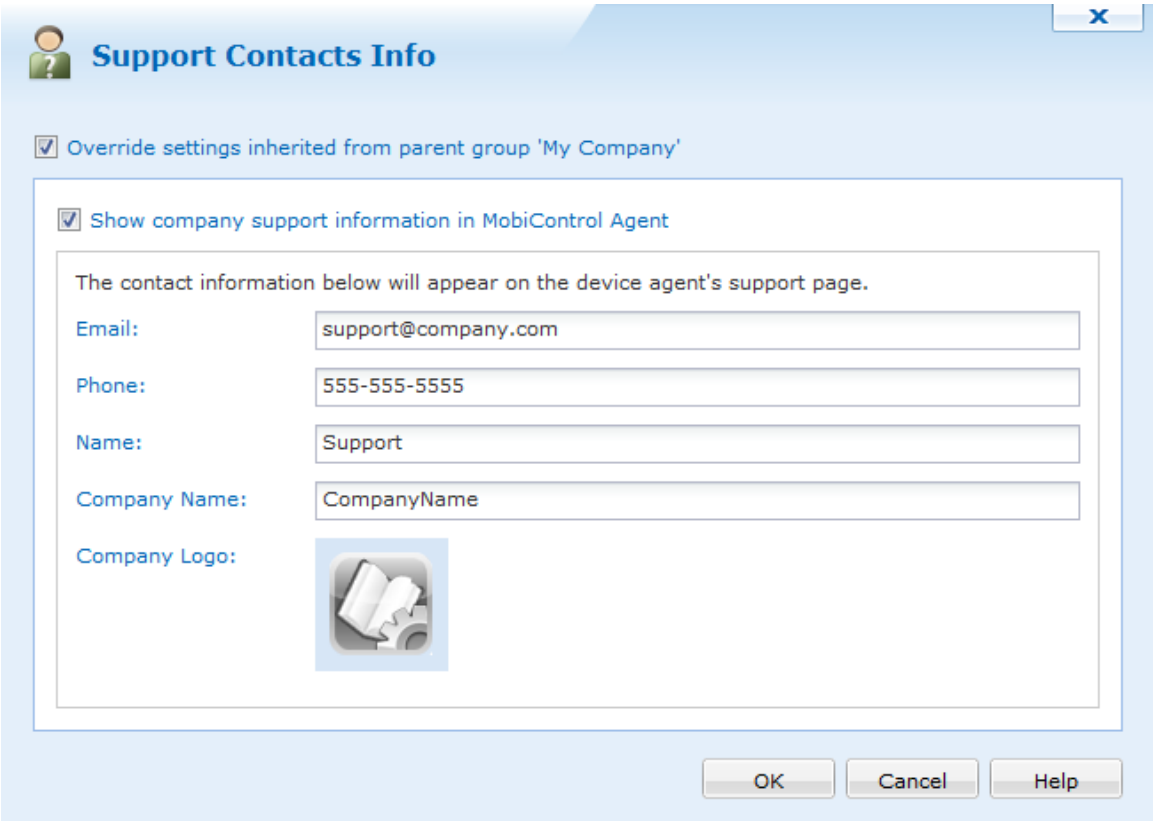
Remote Control Settings dialog box

The following table describes fields in the **Remote Control Settings** dialog box.

Field Name	Description
Connection Profile	This field allows the user to configure the type of connection that will be used for remote control sessions. The available connection types are TCP/IP(SERVER) **(recommended)**, TCP/IP(DIRECT), and <Prompt on Connect>. • The **TCP/IP(SERVER)** setting offers the broadest support for remote control connections. For example, situations where the mobile device does not have a public IP address. When a TCP/IP(SERVER) remote control session is established, the session is bridged through the MobiControl Deployment Server (i.e. The device connects to the MobiControl Deployment Server on TCP port 5494 and the desktop MobiControl Remote client connects to the Deployment Server on TCP port 5494). Since this connection goes through the Deployment Server the performance is generally not as fast as a direct TCP/IP connection, however, it offers improved security as it does not require the mobile Device Agent to accept unauthenticated remote control connections. An example of where this type of connection is required because of network topology is when the mobile devices are behind a firewall and do not have unique public IP addresses. • With the **TCP/IP(DIRECT)** setting, the MobiControl desktop software will open a direct Wireless/Wired TCP/IP connection to the mobile device (i.e. on TCP port 5494). A LAN-based wired/wireless TCP/IP connection generally provides the best performance, however it requires that the mobile Device Agent accept unauthenticated remote control connections unless SSL Security is enabled. Please see the "Windows Mobile Connection Security" topic on page 649.
Do not Use Skin	Checking this off will remove the skin from the device when remote controlling it.
Manufacturer, Model, and Skin Preview	A skin is an image of the body of your mobile device, which mimics the physical device on your desktop screen. Displaying your device in a skin gives you access to most of the physical buttons of the device. It can be useful in training or presentations. Skins should automatically be applied to devices depending on the device agent created. If another skin is wanted to be used, select the manufacturer and model of your device to have its skin be displayed in a remote control session. Skins for most Windows Mobile, Pocket PC and CE .NET based mobile devices are available. We are always adding new skins to our online collection, but if your device is not listed, please contact us to let us know which device you are using.

Windows Mobile Support Contacts Info

The Support Contacts Info panel allows us to set contact information when a user opens up the MobiControl agent on their device. Information that we are able to configure are Email, Phone, Name, Company name and a company logo.



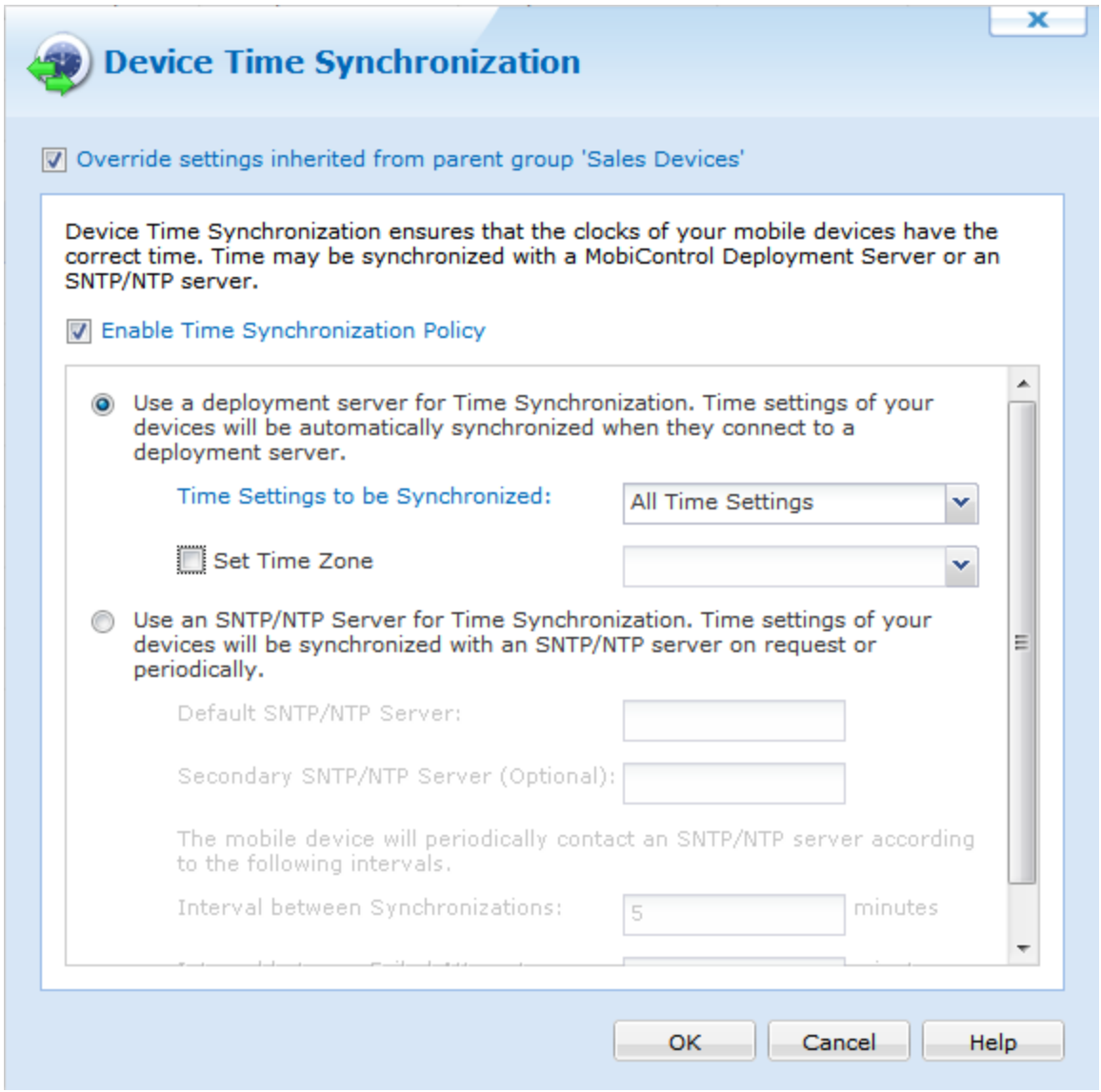
Support Contacts Info dialog box

When each of the fields are set and OK is pressed, this information will then be sent down to the devices where this was configured on. When a user opens up their MobiControl agent and goes to the support info tab, they will be able to see the appropriate information.

Windows Mobile Device Time Synchronization

This feature allows you to enable time synchronization for a mobile device, allowing the device to update its date and time settings by periodically synchronizing them with an SNTP/NTP time server or the MobiControl Deployment Server.

To configure the time synchronization settings for a device or device group, select the device or group in the device tree and click **Device,** click **Configure Device(s),** and click **Time Synchronization.**



Device Time Synchronization dialog box

Time Synchronization Settings

There are three different modes available for time synchronization:

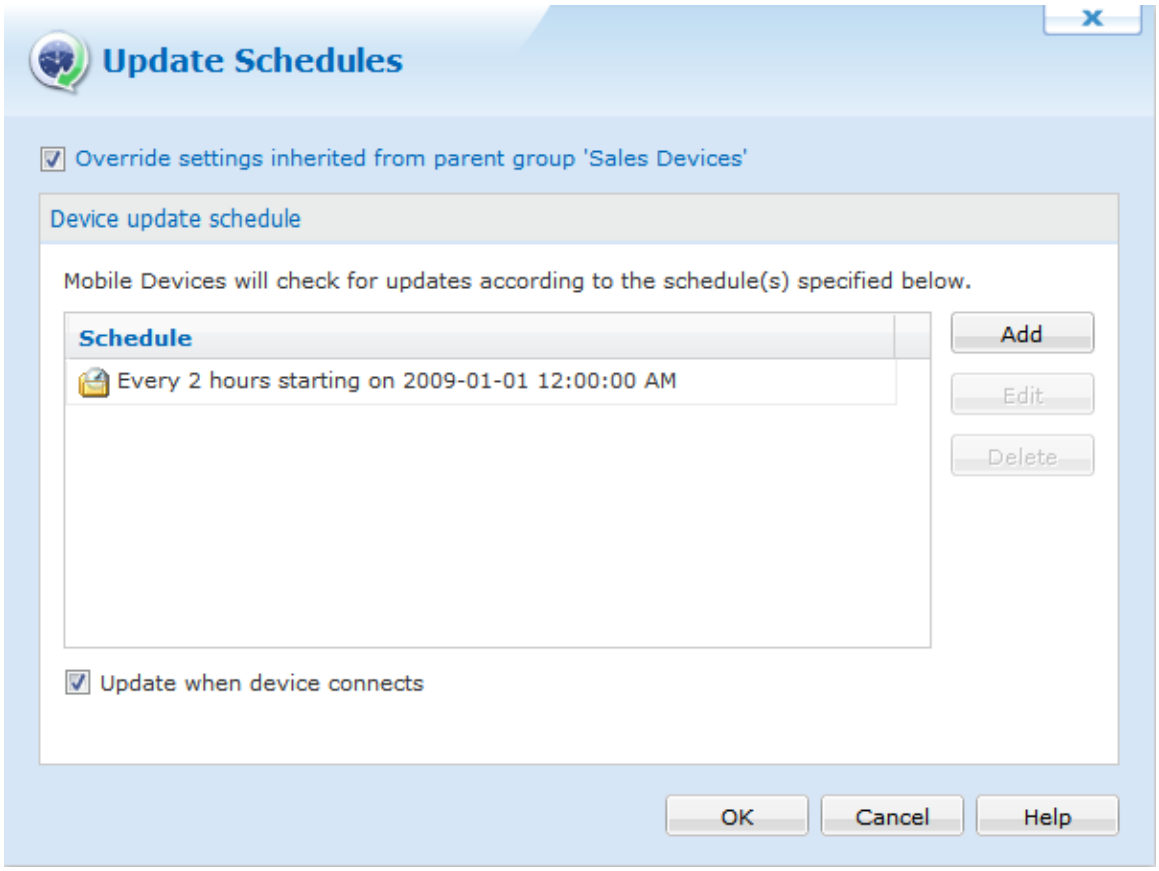
Option	Description
No Time Synchronization	The device time is not synchronized with any server.
Use a Deployment Server for Time Synchronization	The device will synchronize its time with a MobiControl Deployment Server when it connects to it. The time settings available for synchronization include Time Only, and All Time settings: • The **Time Only** option will result in the date and time being synchronized (but not the time zone) • The **All Time Settings** option will sync all of the time settings including DST, time zone, date, and time. • The **Set Time Zone** option to set the time zone for mobile devices which are in a different time zone than the Deployment Server. You can use this on device level or group level.
Use an SNTP/NTP server for Time Synchronization	The device will synchronize its time with the SNTP/NTP server(s) specified in the **Default SNTP/NTP Server** and **Secondary SNTP/NTP Server** fields. When this mode is selected, the option to synchronize automatically becomes available. With automatic synchronization enabled, the device will synchronize its time according to the interval specified in the **Interval between Synchronizations** field. If an automatic synchronization fails, the device will retry after the time interval specified in **Interval between Failed Attempts** has elapsed. **NOTE:** SNTP/NTP Server does not synchronize DST settings. It's similar to time only.

Windows Mobile Device Update Schedule

The device update schedule specifies when the device(s) should query the Deployment Server(s) for updates. Updates may include the addition, update, or removal of packages and modifications to device settings.

If the Deployment Server determines there are pending updates for the device, it immediately sends them to the device. The device also sends the Deployment Server a summary of its installed packages and settings. If the Deployment Server identifies an inconsistency, such as a previously-installed package that is missing on the device, the Deployment Server will re-install the package.

The initial device update schedule is specified by the add devices rule used to add the device(s) to the system. You may edit the schedule for an individual device or a group of devices that have been added to the system by selecting the target device or group in the device tree view in the main console window and selecting **Update Schedules** from the **Configure Device(s)** sub-menu.



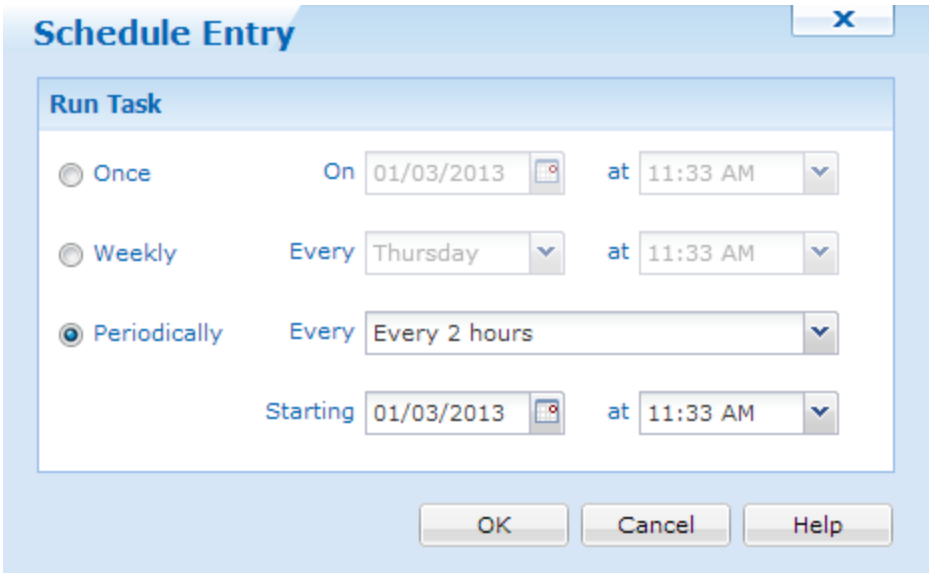
Device Update Schedules dialog box

The following table describes the **Device Update Schedules** dialog box:

Field Name	Description
Add	Select **Add** to specify additional update intervals. The **Schedule Entry** dialog box will be displayed. **EXAMPLE:** To sync a device twice a week, Monday at 06:00 and Friday at 19:00, create two weekly schedule entries.
Edit	Select **Edit** to modify an existing schedule entry. The **Schedule Entry** dialog box will be displayed.
Delete	Select **Delete** to permanently remove an update schedule entry from the dialog box.
Update when device connects	Select this check box to have the device(s) check for updates whenever they connect to a Deployment Server, that is, at every transition from offline to online. If this check box is not selected, the device(s) will only check for updates according to the schedule defined above.

Schedule Entry

The **Schedule Entry** dialog box allows you to specify schedule entries as one-time or periodic events.



Schedule Entry dialog box

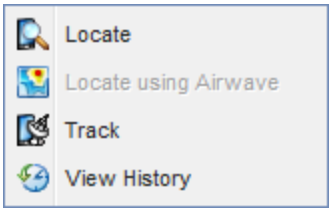
Field Name	Description
Once	The device will check for updates once at the specified date and time.s

Field Name	Description
Weekly	The device will check for updates once a week, on a specific day at a specific time.
Periodically	The device will check for updates periodically, at the specified interval from the set start date and time.

Windows Mobile Location Services

MobiControl's Location Services provides the ability to locate and track mobile devices that are equipped with a GPS receiver that is internal or external to the unit. In order to locate a device, the GPS must be enabled and correctly configured on your device. The GPS determines the current location based on its position relative to orbiting satellites. In order for this to happen, the device requires a clear view of the sky. Determining location may not be possible if the device is inside buildings or has an obstructed view of the sky.

You can activate Location Services for a device in MobiControl by right- clicking on a device and selecting the **Location Services** option from the menu. The first time you select an option from the Location Services menu for a device, it will automatically use the next available license. If there are no more licenses available, you will be notified to contact SOTI for information on acquiring additional licenses for Location Services.



Windows Mobile Location Services

Please See the "Contact Us" page to contact us for more details on acquiring additional licensing.

NOTES:

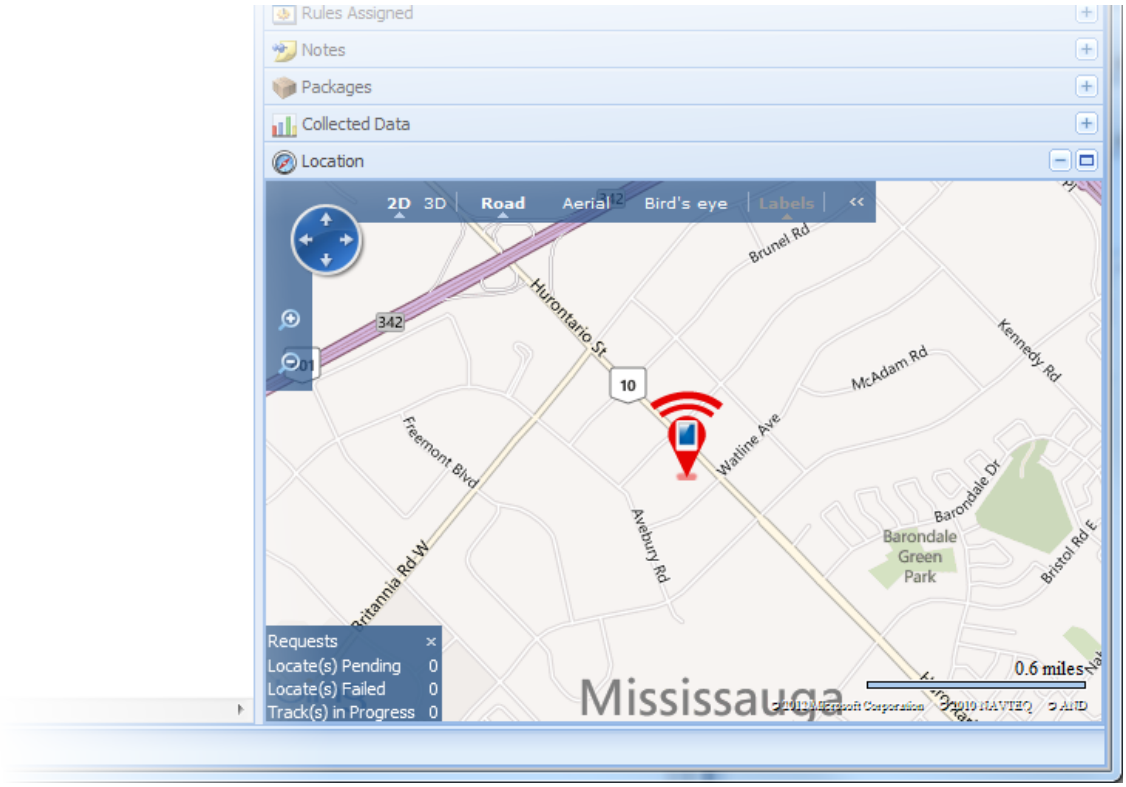
- When using Location Services in MobiControl to track devices, Internet Explorer 7 or higher is required.
- The Current Format for Regional and Language Options on your PC MUST be compatible with Bing Maps. Click here for a list of supported Bing Map control settings.

Windows Mobile Locate Feature

To use the Locate feature in MobiControl's Location Services, right-click on the device you wish to locate, select **Location Services,** and click **Locate.**

The locate feature will use the GPS unit associated with your mobile device to determine the current latitude and longitude of the device. These coordinates are returned to MobiControl and displayed in the Location panel using Microsoft's Virtual Earth. The coordinates plotted in the Location panel represent the exact position of the device at the time of the request. To follow the position of the device in real time, use the **Track** option under the **Location Services** menu.

You can locate the position of multiple devices at once: select the parent folder or hold the CTRL key and select all the devices you wish to locate, right-click, select **Location Services,** and click on **Locate.** In order to use the Locate feature, the device(s) must be online and communicating with the MobiControl Deployment Server. The status of the current (and completed) Locate and Track commands is displayed in the lower left hand corner of the screen.



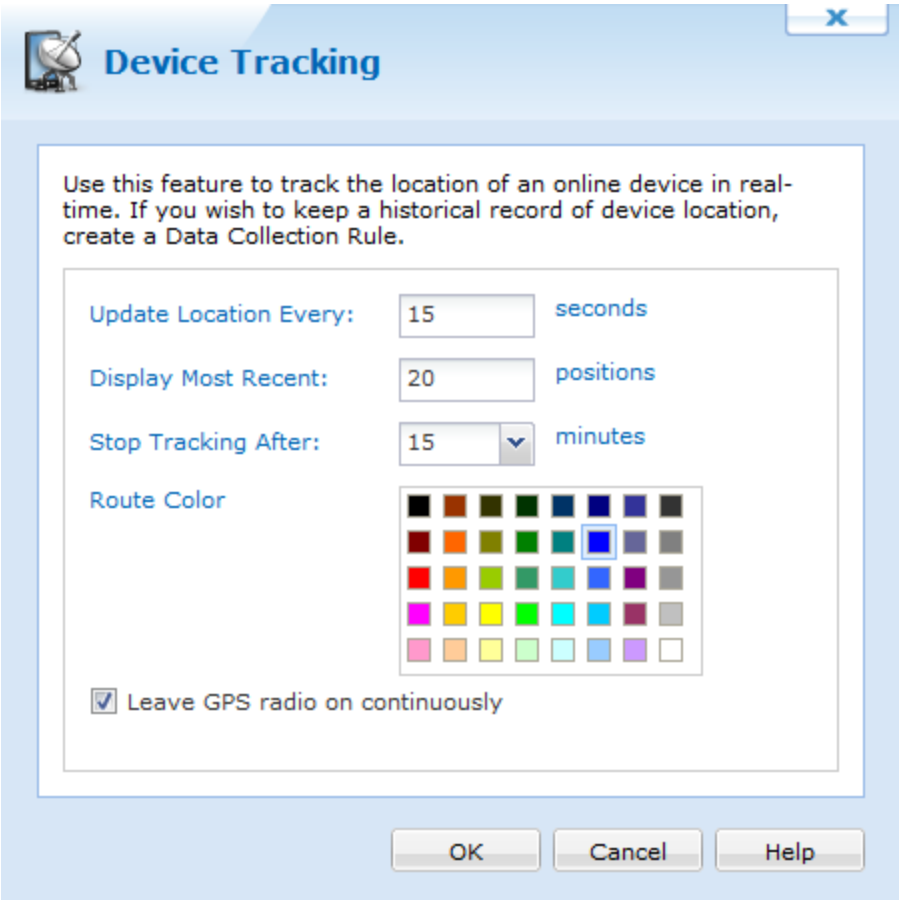
Location Services locate user interface

NOTE:

If the MobiControl Manager is behind a proxy server and you are unable to use Location Services, please run the following command through the **Start** menu then **Run**:
`netsh winhttp set proxy -server="http=<ProxyServerIP>: <Port>; https=<SSLProxyServerIP>: <Port>"` (on Windows Vista, **with no spaces between the quotation marks**.)
This command will update the WinHTTP service with the settings from Internet Explorer.

Windows Mobile Tracking

To use the Track feature in MobiControl's Location Services, right-click on the device you wish to track, select **Location Services,** and click **Track.**



Device Tracking dialog box

The track feature will use the GPS unit associated with your mobile device to determine the current latitude and longitude of the device at a given schedule and send the co-ordinates back to the MobiControl Deployment Server. These co-ordinates are then displayed in the Location panel using Microsoft's Virtual Earth. The co-ordinates plotted in the Location panel represent the exact position of the device at the time of the request along with where the device has been since the request was initiated. To view where the device has been in the past, you need to use the show history option within MobiControl's Location Services.

In order to use the track feature, the device must be online and communicating with the MobiControlDeployment Server.

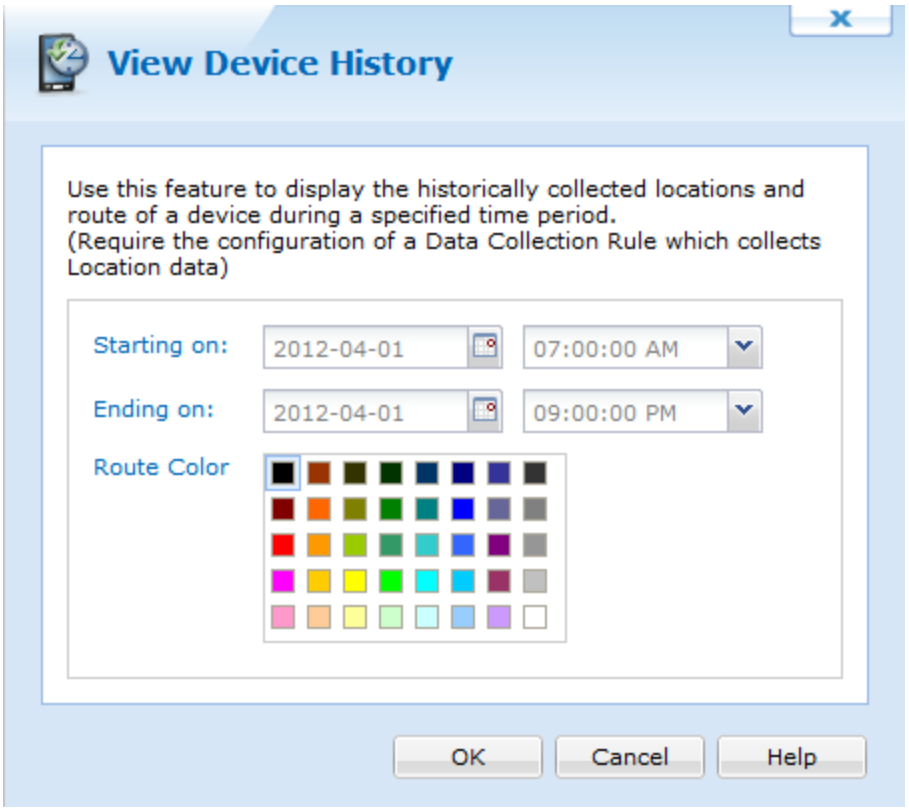
The following table describes each field in the dialog:

Feature	Description
Update Location Every	Set a time interval in seconds (5–86400) for how frequently you would like to have the device location reported.
Display Most Recent	Choose a value to represent the number of recent positions (maximum 100) that you would like to see plotted on the map of the device(s) that you will be tracking.
Stop Tracking After	Set the time interval in minutes (5– 60) for when you would like to end tracking the device.
Route Color	Identifies the device route you will be tracking
Leave GPS radio on continuously	For faster response time from the GPS radio on the device, you should enable this check box. The device's GPS radio will constantly be on.

Windows Mobile Show Tracking History

The show history feature will use the GPS unit associated with your mobile device, allowing you to view where the device has been over a given period of time. To use this feature, you need to set up a data collection rule that collects the location information from the device on a given schedule. The data will be sent back to the deployment server, or, if there is no active data connection on the device, it will be collected and stored in a temporary file and then sent back to the server the next time the device connects. The show history feature does not require the device to be online and communicating with the MobiControl Deployment Server. You can plot information from the history that has been transmitted back to the server during the last active connection.

To use the show history feature, right-click on the device you wish to view, select **Location Services,** and click **Show History.** You will then be prompted to enter the time period for which information is desired, and the route color. Once this is filled in, click **OK** and the path will be plotted.

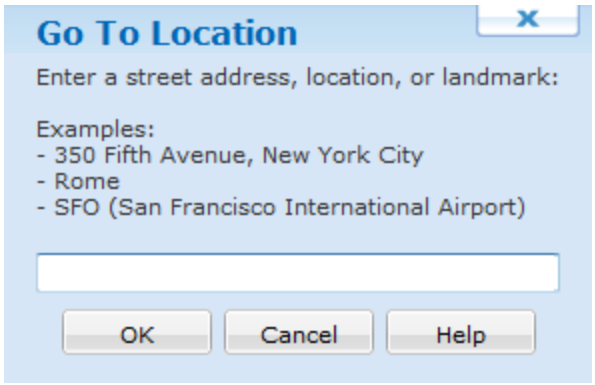


View Device History dialog box

Feature	Description
Starting On	Enter the date and time that you wish to start.
Ending On	Enter the date and time that you wish to stop.
Route Color	Select the color to be used on the map when connecting the co-ordinates.

Using Go To Location

Go To Location allows you to quickly centre and zoom the map to a specific location. Go To Location is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "Windows Mobile Location Services" topic on page 725 for more information.

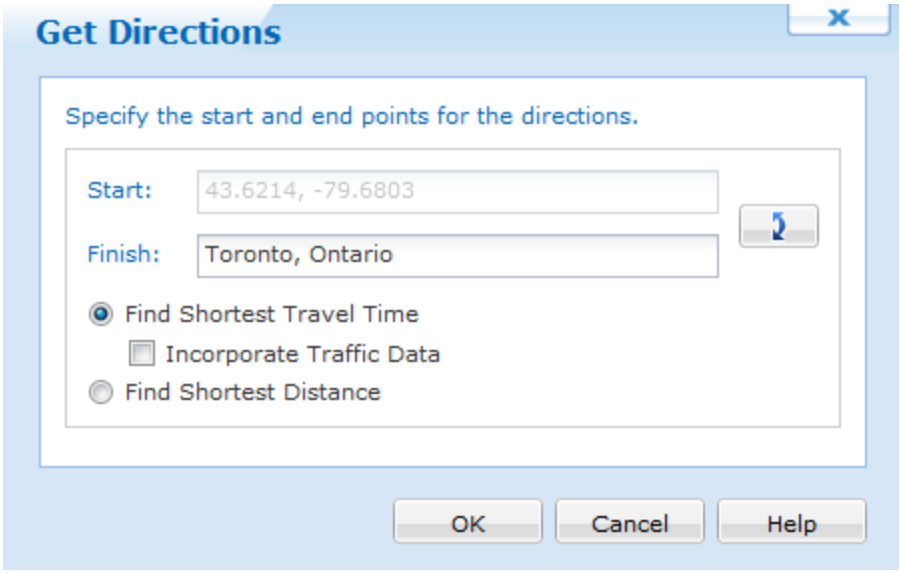


Go To Location dialog box

To use this feature, right click on the Location panel and select "Go To..." from the pop-up menu that appears to open the Go To Location window. You can then enter an address, location, landmark, or the name of an existing geofence. Once you have entered the location information, click the OK button and the map will reload centring on the information you provided. If you entered the name of an existing geofence, the map will change to the location of that geofence and display it on the screen in red.

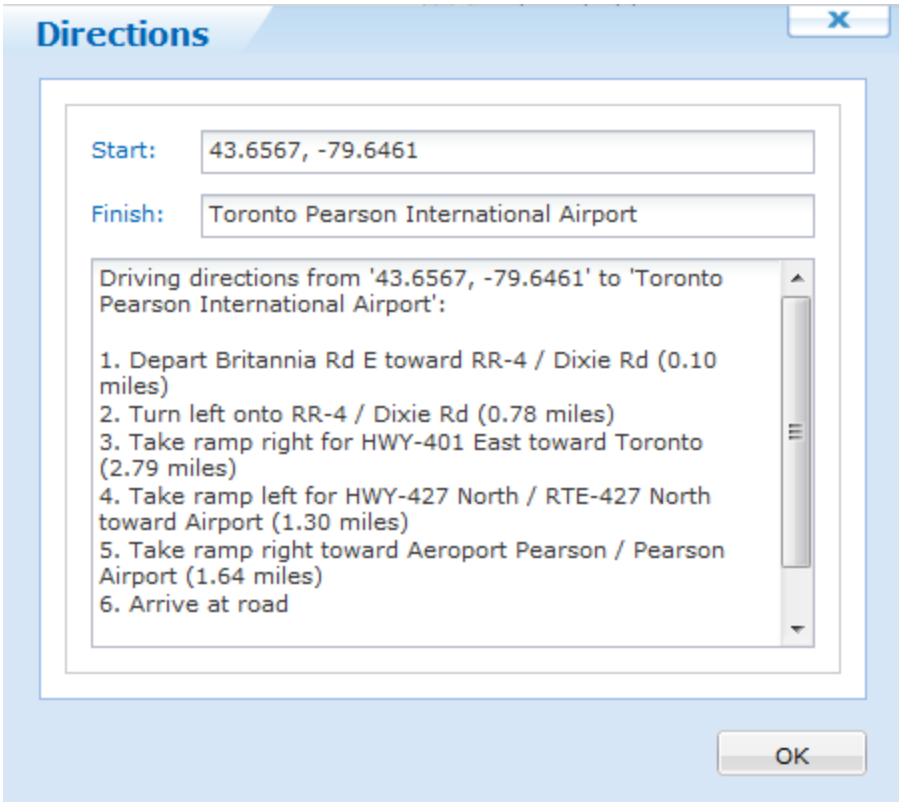
Get Directions

Powered by Microsoft's Bing Maps, MobiControl's Get Directions will return turn-by-turn directions between two locations on the map. These directions can be sent directly to the device, or they can be pasted into an email and sent to a larger group of people. Get Directions is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "Windows Mobile Location Services" topic on page 725 for more information.



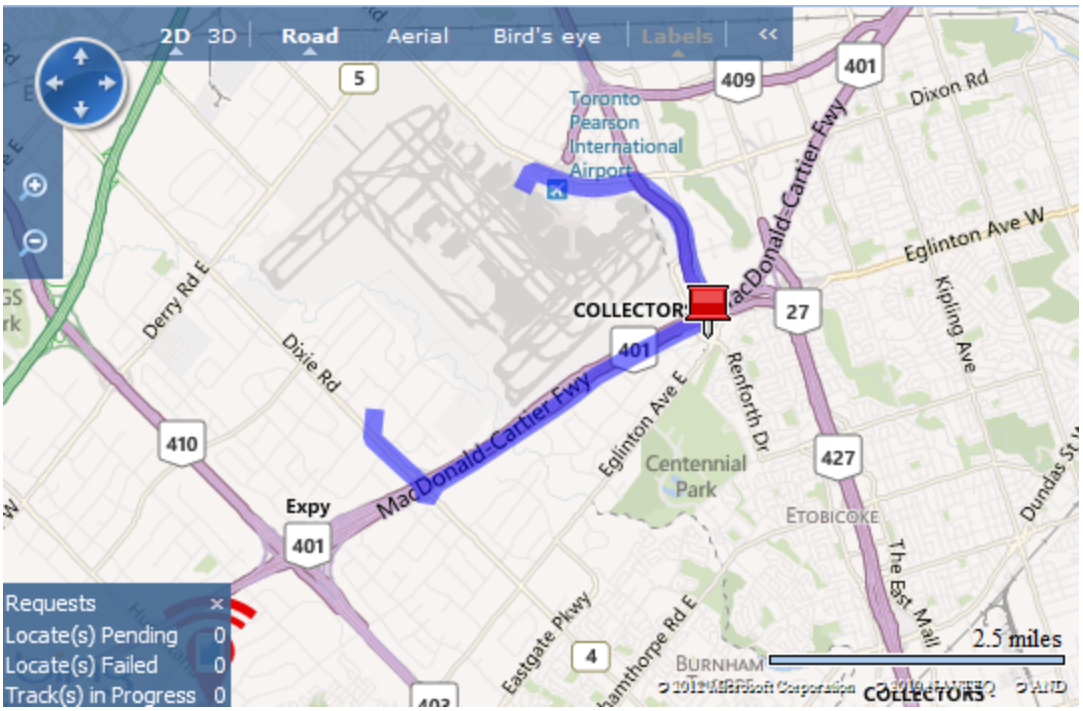
Get Directions dialog box

To use Get Directions, in the Location panel right click on any device or a point on the map and select "Get Directions" from the pop-up menu. The Get Directions dialog box will appear. Be default, the device or map location clicked on will be used as the starting point. To change this, click the double arrow button located to the left of the Start and Finish fields. You can enter GPS co-ordinates, landmarks, or an address. Directions can be optimised by selecting shortest travel time or shortest distance from the options list and press the OK button.



Driving Directions window

MobiControl will determine the turn-by-turn driving directions between the two locations you specified. The resulting directions will be displayed in the Driving Directions window. If you started by right clicking on a device, the "Send to Device" button will be enabled and you can send the instructions directly to the device. You can copy the directions from this window and paste them into an email or document or your choice.

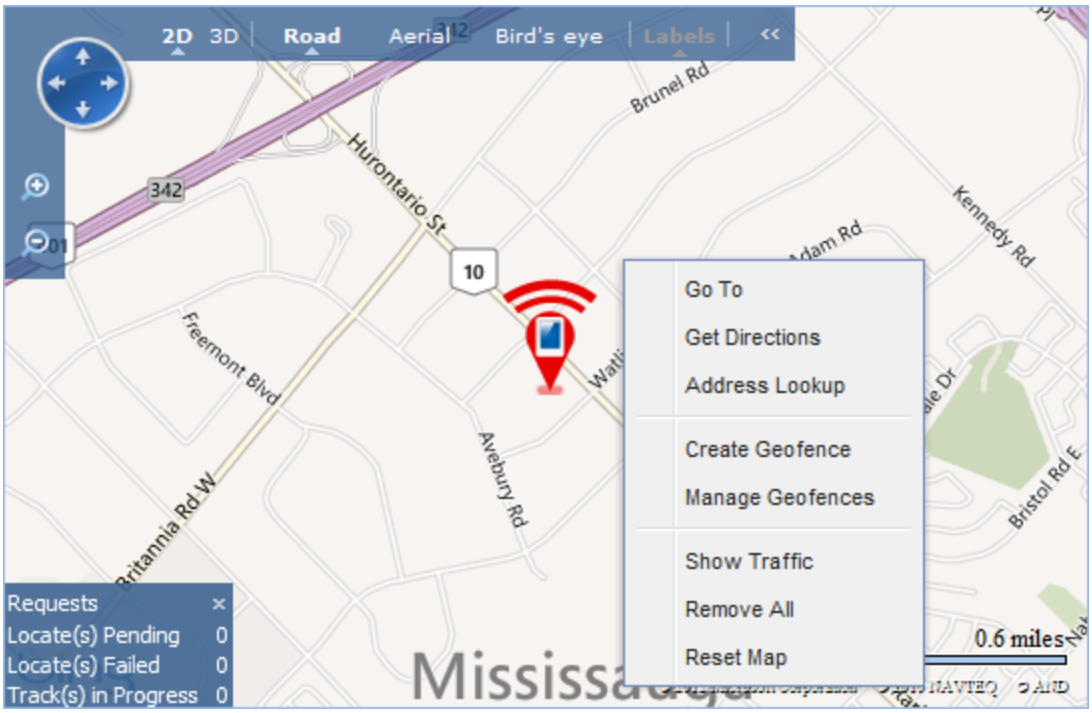


Driving directions displayed on the Map

The Location panel will reload the map to show the driving route highlighted. If the map is in Bird's Eye view, the highlight will not be displayed. Both Aerial and Road view will display the highlighted route.

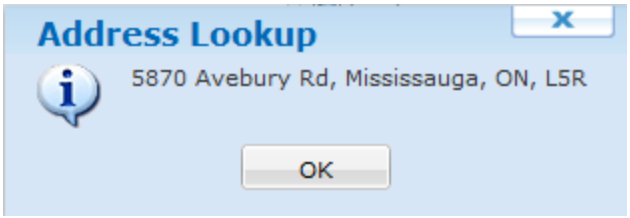
Windows Mobile Address Lookup

The Address Lookup feature allows you to determine the address of a specific point on the map displayed on the Location panel. Address Lookup is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "Windows Mobile Location Services" topic on page 725 for more information.



Location panel right click menu with Address Lookup option

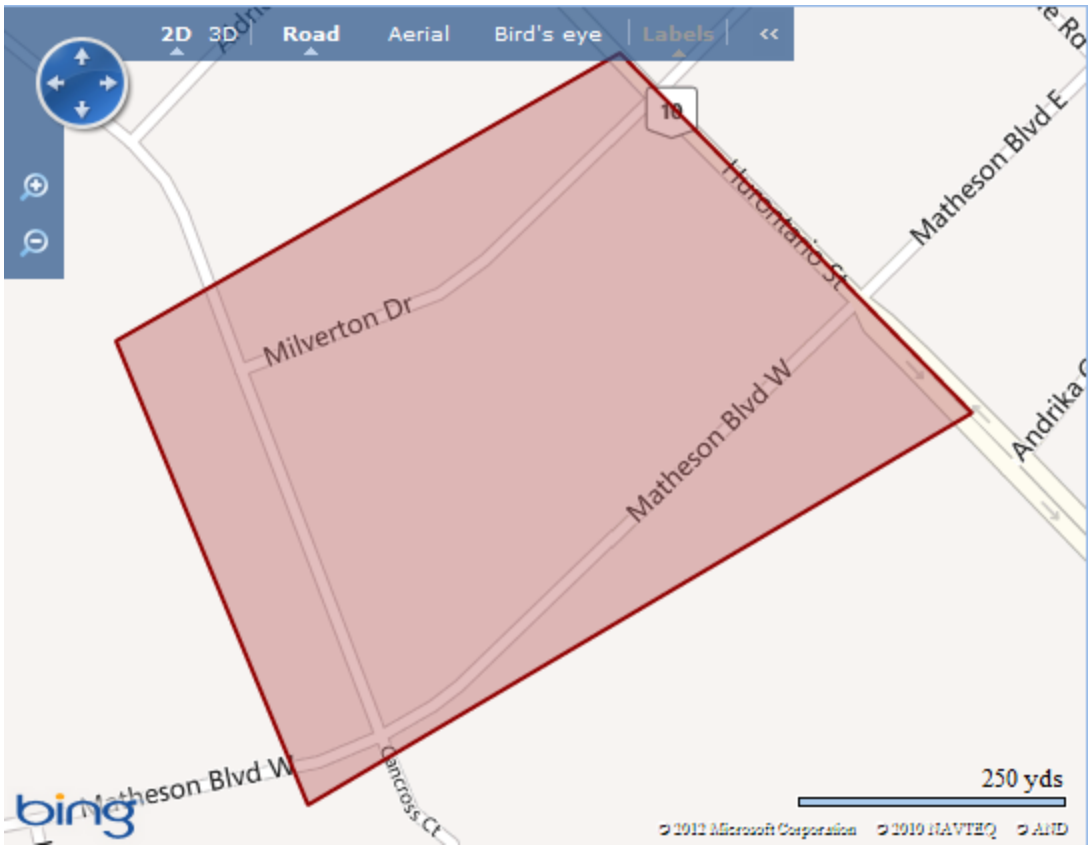
To use the Address Lookup feature, right click anywhere on the map in the Location panel and select the Address Lookup option from the menu that appears. The address of that location will be displayed in a new information window.



Address Lookup window

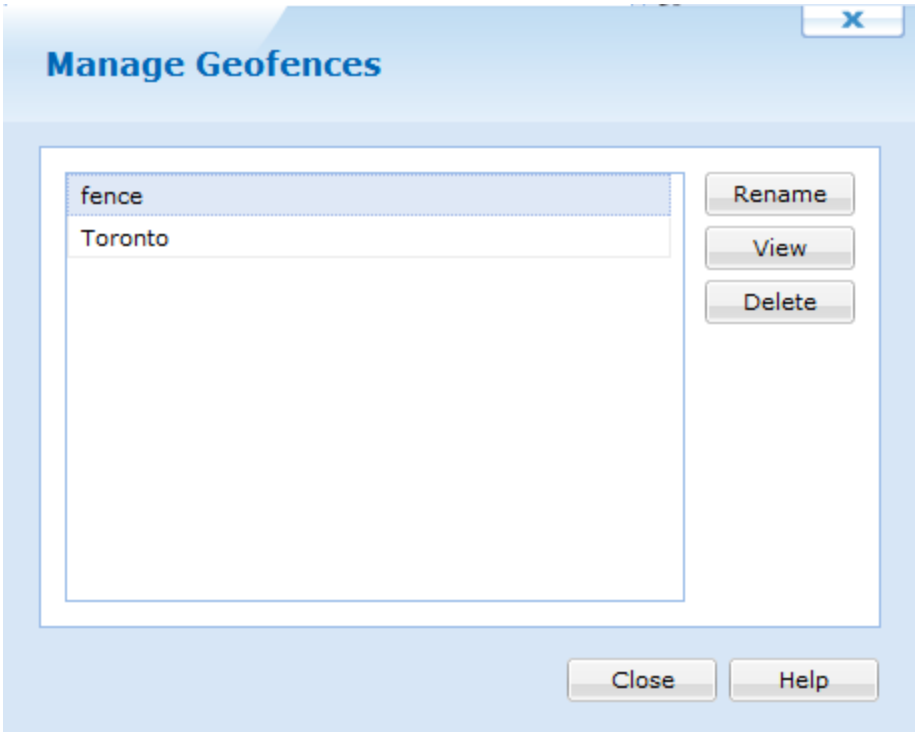
Manage Geofences

The Manage Geofences feature provides an area in which to rename, delete or view current created Geofences. You also have the option to create a new geofence from the drop down menu.



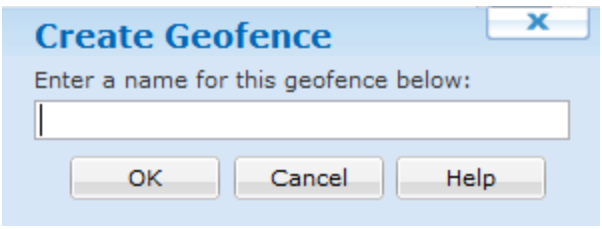
Location panel right click map and select Manage Geofence option

Selecting Manage Geofence brings up the following window.



Field Name	Description
Rename	Allows you to rename a Geofence
View	Allows you to view an already created Geofence on the map
Delete	Allows you to delete a Geofence **NOTE:** In order to Delete the Geofence, no Geofence Event can be associated with it

The **Create Geofence** option allows you to begin drawing on the map. The area drawn on the map will be defined as the Geofence. The defined area must be a complete geometric shape, which means the Start Drawing point will be the same as the End Drawing point. When you have completed a proper geometric shape you be asked to name your geofenced area.



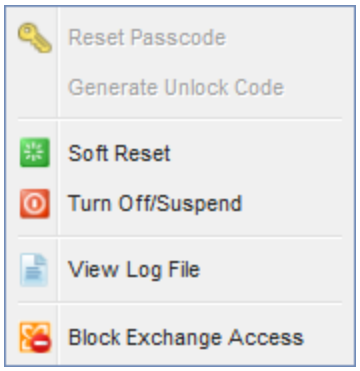
Windows Mobile / CE Actions

MobiControlallows you to reset passcodes, generate an unlock code, soft reset, turn off/suspend and block/unblock Exchange access on a group or an individual device level. These options can be viewed when you right click a device group/device and go to **Action**.

Device Level Actions

Selecting actions on a device level allows you to specifically send actions to that particular device. From here you can reset passcodes, generate an unlock code, soft reset, turn off/suspend, view the device log file and block/unblock Exchange access. To successfully use the Block/unblock Exchange Access action, you must have the Exchange ActiveSync filter installed on your Exchange Server. For more information on how to install this, please Skin/Formats/CrossReferencePrintFormat(See "Secure Email Access Install The Secure Email Access Filter allows you to achieve greater control with devices receiving email from your Exchange Service. When the filter is installed, you can block access to Exchange on certain devices as well as other controls. To successfully install the Exchange ActiveSync Filter, the MobiControl Root CA must be installed on the server that is publishing the Exchange ActiveSync Service. Below shows how to install the filter on your Exchange Server. Prerequisite StepsInstall MobiControl's Secure Email Access filter(Optional) 3rd party Exchange ActiveSync Filter Configuration Prerequisite StepsThe prerequisite steps show how to install the MobiControl Root CA on the Exchange Server. Go to the MobiControl Administration Utility and go to Certificates. The MobiControlAdministration Utility (MCAU) Click the Export button at beside the MobiControl Root Certificate label. Export the MobiControlRoot CertificateSave the exported certificate in a directory that is easy to remember. Next we need to go to the server with the Exchange ActiveSync Service.Open the Microsoft Management Console (MMC) by opening up the run command and typing mmc. Open the Microsoft Management Console. In MMC, click File then Add/Remove Snap In...Adding Snap-insSelect the Certificates snap-in and click Add >. Adding the Certificates Snap-inA new window will appear asking to select an account. Select the Computer account and click Next. Select the Computer Account. On the next screen select Local Computer and click Finish. Select ComputerAfter clicking Finish, click OK in the Add or remove Snap-ins window. Expand the Certificates (Local Computer) tree on the left side and go to Trusted Root Certification Authorities, then Certificates. Right click the Certificates folder and go to All Tasks then Import.Importing a new CA Follow the steps in the Certificate Import Wizard leaving all settings default. After the wizard has finished you will see the MobiControl Root CA in your Trusted Root Certification Authorities. The MobiControl Root CAInstall MobiControl's Secure Email Access filterMobiControl's Secure Email Access Filter must be installed on the server that is publishing the Exchange ActiveSync service. Typically this is the same computer that is hosting OWA (Outlook Web Access). From the server where the Secure Email Access filter will be installed, open Internet Explorer and browse to the MobiControl Web ConsoleLog in to the Web Console as an Administrator based account that has the "Configure Deployment Servers" permissionSelect the All Devices tab at the top of the MobiControl Web Console and then select the Servers tab located along the bottom of the Web ConsoleRight click on the Secure Email Access filter listed under the Deployment Server, and select Install Exchange ActiveSync FilterSave and then run the ExchangeActiveSyncFilter.exe program. This will place the needed files onto the server. Note: Depending on your Internet Explorer settings, you may be prompted to allow file downloads from the web pageOpen IIS manager and select the web site that is publishing Exchange ActiveSync Select ISAPI filters and select Add from the list of actionsEnter MobiControl Secure Email Access as the filter name For the Executable, If the Exchange ActiveSync site is running in a 32-bit application pool, select \Program Files\SOTI\XAS\mcxas.dll or, if the Exchange ActiveSync site is running in a 64-bit application pool, select \Program files\SOTI\XAS\mcxas64.dllSelect OK to save the filterIn the

resulting list of filters, ensure that the MobiControl Secure Email Access filter is listed above the Microsoft Exchange ActiveSync filter. If this is not the case, select View Order List from the available actions, highlight MobiControl Secure Email Access and select Move Up to place it at the top Note: MobiControl's Secure Email Access required communication between the server that is publishing Exchange ActiveSync where the filter is installed, to the MobiControl Web Console. This communication happens over SSL on port 443.3rd party Exchange ActiveSync Filter ConfigurationBefore you begin, the following components must be installed/enabled.1. IIS 7 with ASP.NET role service enabled.2. URL Rewrite Module installed (version 2.0 is required)3. Application Request Routing version 2.5 (Link)The URL Rewrite Module and Application Request Routing version 2.5 are both installed at the same time. After installation, please follow these steps:Open the IIS managerSelect the server in the tree view on the left hand side and then click on the Application Request Routing feature.Application Request RoutingOn the right menu, click Server Proxy Settings in the Proxy SectionServer Proxy SettingsCheck the Enable Proxy check box. Leave the default values for all the other settings on this page. Click Apply on the right side to commit the change.Enable ProxyNext step is to add the HTTP_ACCEPT_ENCODING server variable and Inbound and Outbound rules. To do this, please go to the left hand panel and select the Default Web Site and then select URL Rewrite. URL rewriteIn the URL Rewrite page, select View Server Variables on the right hand side. View Server VariablesClick the Add... link on the right side of the page to add the HTTP_ACCEPT_ ENCODING variable. Click OK then Back to Rules. Adding a server variableClick the Add Rule(s)... link on the right side to add Inbound and Outbound rules. Add rule(s)...When creating the Inbound and Outbound rules, select Blank Rule under the respected heading and click OK.Adding a Blank Inbound or Outbound ruleOn the page shown below, the following fields need to have values entered (Please ensure that you enter your appropriate owa address):NameReverseProxyInboundRule1Pattern^(.*)Rewrite URLhttps://owa.myDomain.com/{R:1} Inbound Rule creation pageAfter the values have been entered, the server variable needs to be added. To do this, expand the Server Variables panel. Click Add and choose HTTP_ACCEPT_ENCODING from the drop down menu. Under value, enter 0, then click OK. Set Server VariableAfter entering all required values, click Apply.Apply Inbound RuleCreate a new blank rule to create an Outbound Rule. Please see below for what values to set on this page: Outbound rule pageUnder precondition, you will need to create a new condition. To do this, select <Create New Precondition...>. When the pop up window appears, click Add... to add a pattern:Add PreconditionAfter entering all required values, Click OK then click Apply.Apply Outbound RuleAfter the rules have been created, click the IIS server, and restart. To confirm that everything has been configured properly, go to C:\inetpub\wwwroot and open the web.config file in notepad. Your file should look similar to this: <?xml version="1.0" encoding="UTF-8"?> <configuration> <system.webServer> <rewrite> <rules> <rule name="ReverseProxyInboundRule1"> <match url="^(.*)" /> <serverVariables> <set name="HTTP_ ACCEPT_ENCODING" value="0" /> </serverVariables> <action type="Rewrite" url="https://owa.soti.net/ {R:1}" /> </rule> </rules> <outboundRules> <rule name="ReverseProxyOutboundRule1" preCondition="ResponseIsHtml1"> <match filterByTags="A, Form, Img" pattern="^http (s)?://owa.soti.net/(.*)" /> <action type="Rewrite" value="http{R:1}://owa.soti.net/{R:2}" /> </rule> <preConditions> <remove name="ResponseIsHtml1" /> <preCondition name="ResponseIsHtml1"> <add input="{RESPONSE_CONTENT_TYPE}" pattern="^text/html" /> </preCondition> </preConditions> </outboundRules> </rewrite> </system.webServer> </configuration>" on page 1)



Windows Mobile / CE Device Action Selections

Reset passcode becomes enabled when the administrator enabled standard user authentication and allows users to reset their passcode in the Authentication Policy.

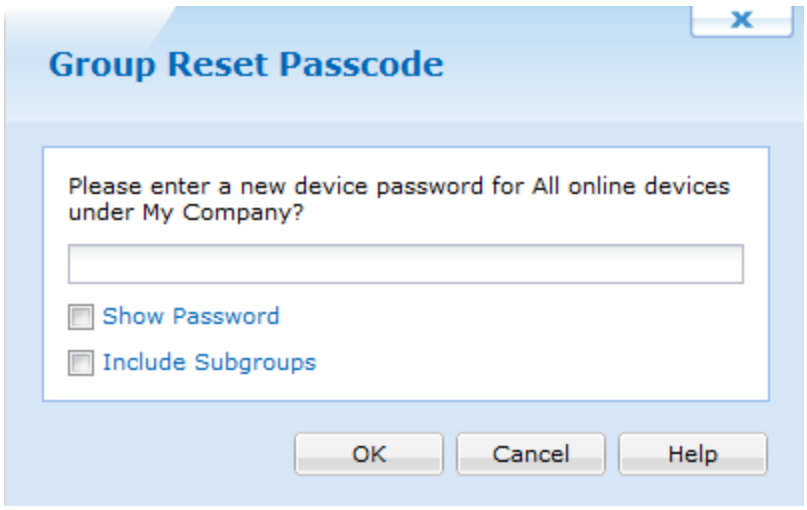
If the user has changed the passcode on the device and reset passcode is selected, the passcode changes back to the original passcode the administrator originally set. Please see the "Windows Mobile Authentication" topic on page 638 for more information on configuring user authentication.

Group Level Actions

With group level actions, you are able to reset passcodes, and Block/Unblock access to exchange.

Reset Passcode

Reset Passcode allows you to reset the passcode for every device in the group. This can be useful when you move multiple devices into a specific group for resetting passcodes.



Group Reset Passcode

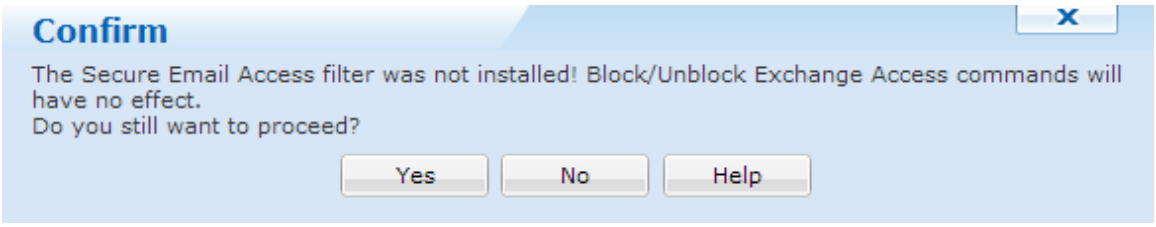
Block/Unblock Exchange Access

Using these options allow you to block and unblock Exchange access to every device in the group. To successfully use this action, you must have the Exchange ActiveSync filter installed on your Exchange Server. For more information on how to install this, please Skin/Formats/CrossReferencePrintFormat (See "Secure Email Access Install The Secure Email Access Filter allows you to achieve greater control with devices receiving email from your Exchange Service. When the filter is installed, you can block access to

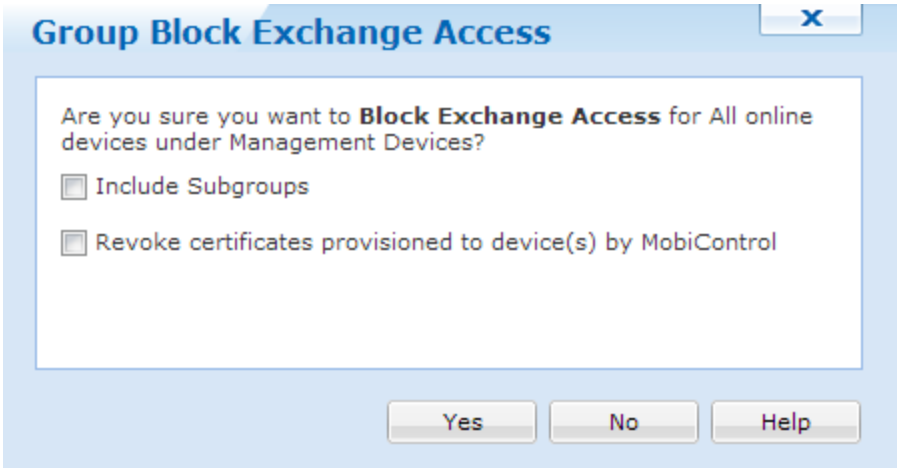
Exchange on certain devices as well as other controls. To successfully install the Exchange ActiveSync Filter, the MobiControl Root CA must be installed on the server that is publishing the Exchange ActiveSync Service. Below shows how to install the filter on your Exchange Server. Prerequisite StepsInstall MobiControl's Secure Email Access filter(Optional) 3rd party Exchange ActiveSync Filter Configuration Prerequisite StepsThe prerequisite steps show how to install the MobiControl Root CA on the Exchange Server. Go to the MobiControl Administration Utility and go to Certificates. The MobiControlAdministration Utility (MCAU)Click the Export button at beside the MobiControl Root Certificate label. Export the MobiControlRoot CertificateSave the exported certificate in a directory that is easy to remember. Next we need to go to the server with the Exchange ActiveSync Service.Open the Microsoft Management Console (MMC) by opening up the run command and typing mmc. Open the Microsoft Management Console. In MMC, click File then Add/Remove Snap In...Adding Snap-insSelect the Certificates snap-in and click Add >. Adding the Certificates Snap-inA new window will appear asking to select an account. Select the Computer account and click Next. Select the Computer Account. On the next screen select Local Computer and click Finish. Select ComputerAfter clicking Finish, click OK in the Add or remove Snap-ins window. Expand the Certificates (Local Computer) tree on the left side and go to Trusted Root Certification Authorities, then Certificates. Right click the Certificates folder and go to All Tasks then Import.Importing a new CA Follow the steps in the Certificate Import Wizard leaving all settings default. After the wizard has finished you will see the MobiControl Root CA in your Trusted Root Certification Authorities. The MobiControl Root CAInstall MobiControl's Secure Email Access filterMobiControl's Secure Email Access Filter must be installed on the server that is publishing the Exchange ActiveSync service. Typically this is the same computer that is hosting OWA (Outlook Web Access). From the server where the Secure Email Access filter will be installed, open Internet Explorer and browse to the MobiControl Web ConsoleLog in to the Web Console as an Administrator based account that has the "Configure Deployment Servers" permissionSelect the All Devices tab at the top of the MobiControl Web Console and then select the Servers tab located along the bottom of the Web ConsoleRight click on the Secure Email Access filter listed under the Deployment Server, and select Install Exchange ActiveSync FilterSave and then run the ExchangeActiveSyncFilter.exe program. This will place the needed files onto the server. Note: Depending on your Internet Explorer settings, you may be prompted to allow file downloads from the web pageOpen IIS manager and select the web site that is publishing Exchange ActiveSync Select ISAPI filters and select Add from the list of actionsEnter MobiControl Secure Email Access as the filter name For the Executable, If the Exchange ActiveSync site is running in a 32-bit application pool, select \Program Files\SOTI\XAS\mcxas.dll or, if the Exchange ActiveSync site is running in a 64-bit application pool, select \Program files\SOTI\XAS\mcxas64.dllSelect OK to save the filterIn the resulting list of filters, ensure that the MobiControl Secure Email Access filter is listed above the Microsoft Exchange ActiveSync filter. If this is not the case, select View Order List from the available actions, highlight MobiControl Secure Email Access and select Move Up to place it at the top Note: MobiControl's Secure Email Access required communication between the server that is publishing Exchange ActiveSync where the filter is installed, to the MobiControl Web Console. This communication happens over SSL on port 443.3rd party Exchange ActiveSync Filter ConfigurationBefore you begin, the following components must be installed/enabled.1. IIS 7 with ASP.NET role service enabled.2. URL Rewrite Module installed (version 2.0 is required)3. Application Request Routing version 2.5 (Link)The URL Rewrite Module and Application Request Routing version 2.5 are both installed at the same time. After installation, please follow these steps:Open the IIS managerSelect the server in the tree view on the left hand side and then click on the Application Request Routing feature.Application Request RoutingOn the right menu, click Server Proxy Settings in the Proxy SectionServer Proxy SettingsCheck the Enable Proxy check box. Leave the default values for all the other settings on this page. Click Apply on the right side to commit the change.Enable ProxyNext step is to add the HTTP_ACCEPT_ENCODING server variable and Inbound and Outbound rules. To do this, please go to the left hand panel and select the Default Web Site and then select URL Rewrite. URL rewriteIn the URL Rewrite page, select View Server Variables on the right hand side. View Server VariablesClick the Add... link on the right side of the page to add the HTTP_ACCEPT_ENCODING variable. Click OK then Back to Rules. Adding a server variableClick the Add Rule(s)... link on the right side to add Inbound and Outbound rules. Add rule(s)...When creating the Inbound and Outbound rules, select Blank Rule under the respected heading and click OK.Adding a Blank Inbound or Outbound ruleOn the page shown below, the following fields need to have values entered

(Please ensure that you enter your appropriate owa address):NameReverseProxyInboundRule1Pattern^(.*)Rewrite URLhttps://owa.myDomain.com/{R:1} Inbound Rule creation pageAfter the values have been entered, the server variable needs to be added. To do this, expand the Server Variables panel. Click Add and choose HTTP_ACCEPT_ENCODING from the drop down menu. Under value, enter 0, then click OK. Set Server VariableAfter entering all required values, click Apply.Apply Inbound RuleCreate a new blank rule to create an Outbound Rule. Please see below for what values to set on this page: Outbound rule pageUnder precondition, you will need to create a new condition. To do this, select <Create New Precondition...>. When the pop up window appears, click Add... to add a pattern:Add PreconditionAfter entering all required values, Click OK then click Apply.Apply Outbound RuleAfter the rules have been created, click the IIS server, and restart. To confirm that everything has been configured properly, go to C:\inetpub\wwwroot and open the web.config file in notepad. Your file should look similar to this: <?xml version="1.0" encoding="UTF-8"?> <configuration> <system.webServer> <rewrite> <rules> <rule name="ReverseProxyInboundRule1"> <match url="^(.*)" /> <serverVariables> <set name="HTTP_ACCEPT_ENCODING" value="0" /> </serverVariables> <action type="Rewrite" url="https://owa.soti.net/{R:1}" /> </rule> </rules> <outboundRules> <rule name="ReverseProxyOutboundRule1" preCondition="ResponseIsHtml1"> <match filterByTags="A, Form, Img" pattern="^http(s)?://owa.soti.net/(.*)" /> <action type="Rewrite" value="http{R:1}://owa.soti.net/{R:2}" /> </rule> <preConditions> <remove name="ResponseIsHtml1" /> <preCondition name="ResponseIsHtml1"> <add input="{RESPONSE_CONTENT_TYPE}" pattern="^text/html" /> </preCondition> </preConditions> </outboundRules> </rewrite> </system.webServer> </configuration>" on page 1) If the filter is not installed, a confirm message will appear.

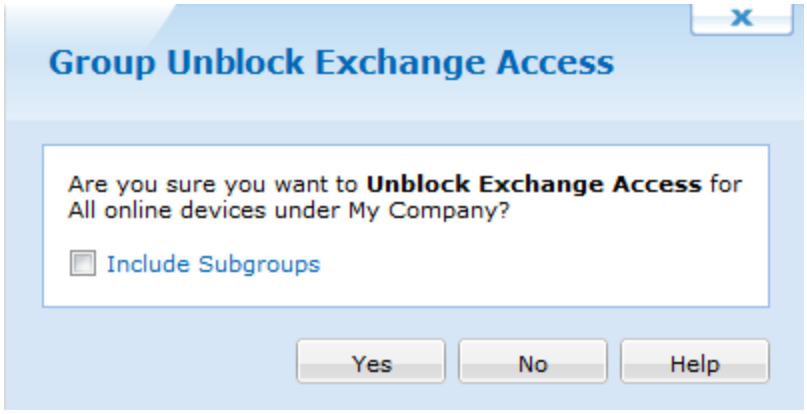
If any certificates were provisioned by MobiControl to devices, we can revoke them when we block Exchange access.



No Filter installed



Blocking Exchange Access



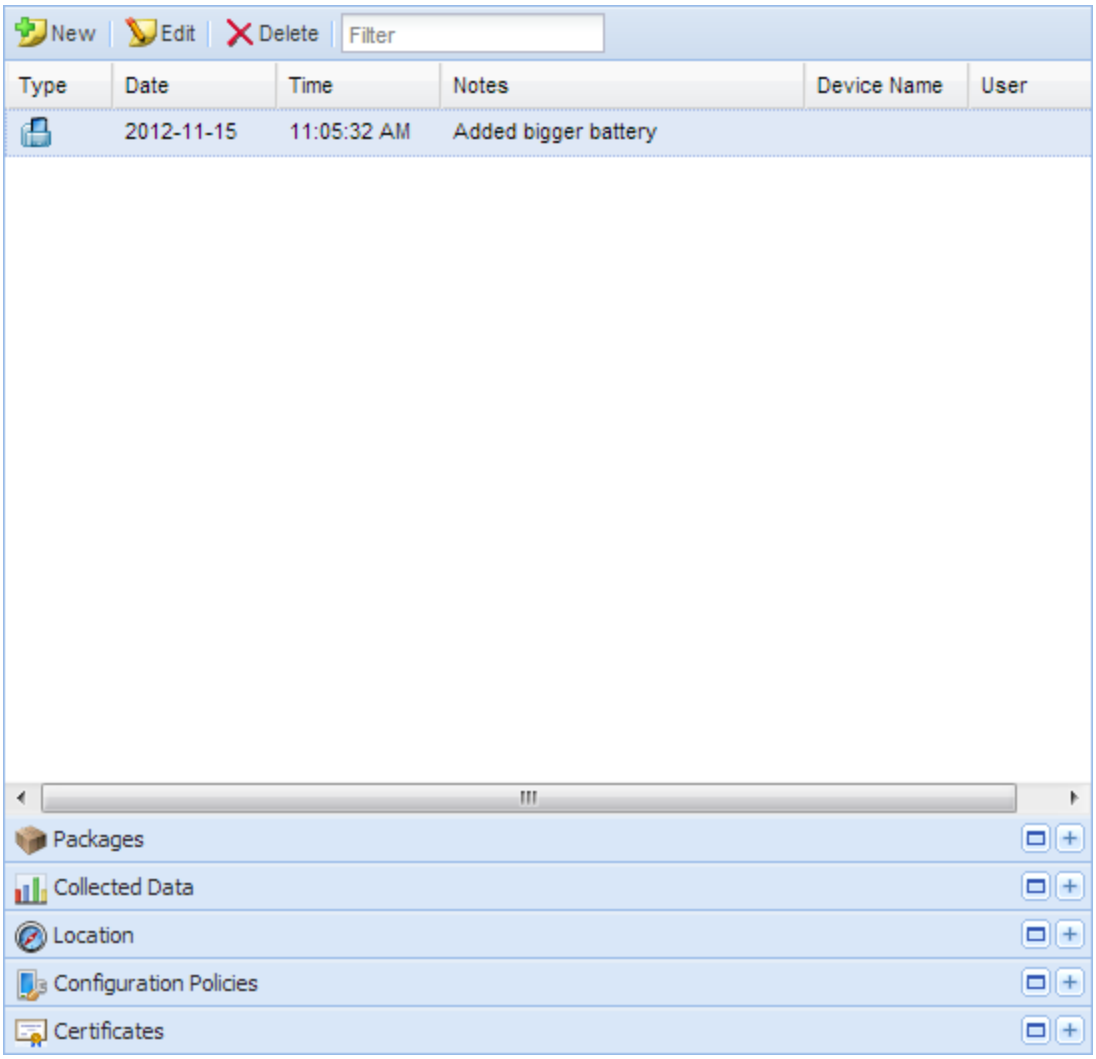
Unblocking Exchange Access

Device Notes

The Device Notes feature allows you to create a note for a device and archive it for future reference and tracking purposes. Each note is editable and includes the date and time when the note was added or edited. The note includes the name of the user creating the note and can be assigned different colors for color-coded categorization.

This feature is useful for creating a "trouble ticket" for help desk tracking in an end-user support or CRM (Customer Relationship Management) environment. It also allows users with access to the MobiControl Web Console to document a device-specific issue and share their comments and memos related to that device with other users of the MobiControl Web console.

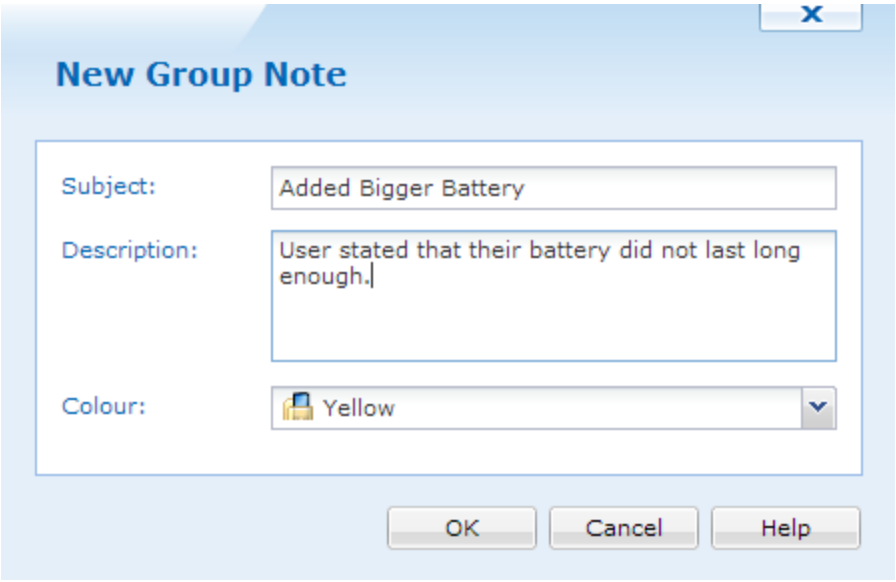
To view and edit notes for a device, select the Devices view (tab) in any of the All Devices, Windows Mobile, Windows Desktop, iOS, Android or Android Plus tab. Select a device and the notes for that device appear in the Notes panel.



Device Notes

Adding or Editing a Note

From within the Notes panel, click **New** to add a new note for the currently selected device or click **Edit** to make changes to an existing note.



Add Note dialog box

The following table describes the fields of the **Add Note** dialog box:

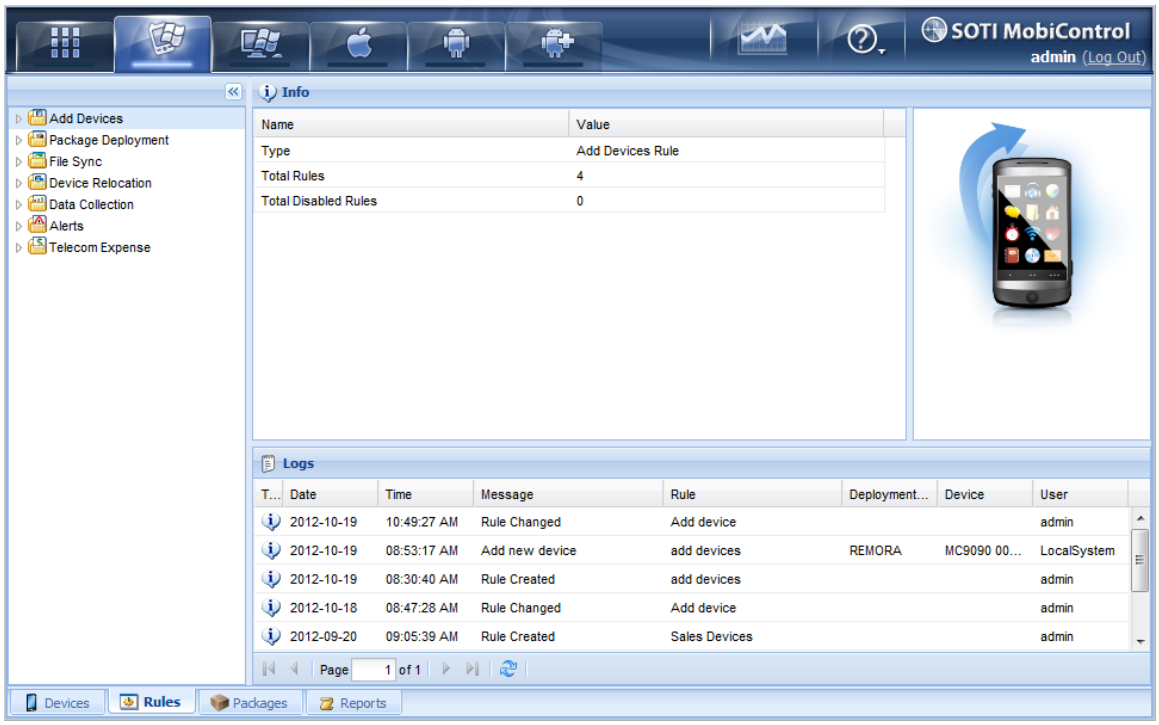
Field Name	Description
Subject	Text entered in the subject field appears in the Notes panel as the title of the note.
Icon	You can choose different colors for the icon to adopt a color-coding to indicate different priority levels or to distinguish between different departments or users creating the note. Notes can be sorted by icon color for a categorized view.
Description	The description field is available for viewing when the note is opened. This field can contain troubleshooting notes, administrative memos or any other device-specific information.

Device Group Notes

MobiControl now offers a way to place notes on a device group level. For example, if you are planning a roll out of devices across the country in phases based on location, you can add device group notes to state which phase each group is in. Therefore, when someone else logs into the MobiControl Web Console, they can see what part of the roll out each group should be in.

To create a device group level note, click a group on the left side of the MobiControl Web Console. After a group has been selected, expand the Notes panel on the right side, and click New.

Windows Mobile/CE Rules Tab



Windows Mobile/CE Rules Tab

MobiControl uses rules to simplify the tasks of device management and configuration. See Below for a description of each rule.

Add Devices

1. Create an add devices rule.

   An add devices rule allows you to configure the settings that MobiControl uses to set up and communicate with your devices. These settings include: the device group to which devices are added, how often the device is to check for updates, and the parameters to be used for remote control sessions. Please see the "Adding Windows Mobile Devices" topic on page 747 for detailed information about creating an add devices rule.

2. Create a Device Agent.

   The Device Agent is the MobiControl software that resides on mobile devices and communicates with MobiControl Deployment Servers. Device Agents execute instructions received from MobiControl Deployment Servers, report status information, and send real-time information to Deployment Servers. Device Agents also restore the device state after a hard reset, service remote control sessions, install or uninstall packages, and synchronize the device clock. Please see the "Windows Moible Device Agent Manager" topic on page 755 for detailed information about creating a Device Agent.

3. Install the Device Agent onto the devices.

   Once created, there are several options for installing the agent on to your devices. For example, installation can be accomplished via cradled ActiveSync, via a website download, via an SD card, or using an existing software distribution mechanism. Please see the "Windows Moible Device Agent Manager" topic on page 755 for detailed information about installing the Device Agent.

Package Deployment

1. Create a package.

   A package is a set of software and data files that have been packed into a single compressed file. MobiControl provides a tool called MobiControl Package Studio that allows you to quickly and easily create packages. For complex packages, Package Studio allows users to add scripts that get automatically executed at various points in the installation or un-installation of the package. Please see the "Creating Packages" topic on page 414 for detailed information about creating packages using MobiControl.

2. Create a deployment rule.

   To deploy a package using MobiControl, you need to create a deployment rule. When you create a deployment rule, you need to specify the package(s) to be deployed, the devices to which the package(s) will be deployed, and the installation time. Please see the "Windows Mobile Package Deployment" topic on page 764 for detailed information about creating a deployment rule.

3. Check the rule execution status.

   Once you have created a deployment rule, you may want to confirm that all devices have been provisioned with the specified packages. The execution status of the deployment rule is graphically represented in the execution chart in the Rules view (tab). MobiControl also provides a report called the 'Deployment Rule Execution Summary Report'. Please see the "Generate Reports" topic on page 390 for detailed information about MobiControl Reports.

File Sync

1. Create a file sync rule.

   A file sync rule allows you to schedule file(s) to be synchronized between a set of devices and the Deployment Server. When creating a file sync rule, you will need to specify the file(s) you want synced (both their original location and their destination), the interval in between the syncs and which direction the sync should go in (either device to server, or server to device) and which devices should be involved in the sync. Please see the "Windows Mobile File Sync" topic on page 769 for detailed information about creating a file sync rule.

2. Check the rule execution status.

   Once the file sync rule has been created, you may want to confirm that the scheduled syncs occurred. You can do this by looking at the rule execution status or by checking the rule execution report in the Reports view (tab).Please see the "Generate Reports" topic on page 623 for more detail about reports.

Device Relocation

1. Create a device relocation rule.

   A device relocation rule allows you to automatically move your mobile devices among different device groups in the MobiControl device tree, based on the IP address or other custom criteria. This is useful for managing mobile devices in a deployment where the device tree represents different physical locations (e.g. retail stores, warehouses, regional offices, etc). Please see the "Windows Mobile Device Relocation" topic on page 782 for detailed information about creating a device relocation rule.

2. Check the device relocation rule execution status.

   Once the device relocation rule has been created, you may want to confirm its execution. You can do this by looking at the rule execution status or by checking the rule execution report in the Reports view (tab). Please see the "Generate Reports" topic on page 390 for more detail about reports.

Data Collection

1. Create a data collection rule.

   A data collection rule allows you to set up rules to collect data from your mobile devices automatically. Please see the "Windows Mobile Data Collection " topic on page 786 for detailed information about creating a data collection rule.

2. Check the data collection rule execution status.

   Once the data collection rule has been created, you may want to confirm its execution. You can do this by looking at the rule execution status or by checking the rule execution report in the Reports view (tab). Please see the "Generate Reports" topic on page 623 for more detail about reports.

Alert

1. Create an Alert

   An Alert Rule allows Administrators and Users to be notified when events of interest arise on the system. Please see the "Windows Mobile Alerts" topic on page 575 for detailed information about creating an Alert Rule.

2. Check the Alert Rule execution status.

   Once the Alert Rule has been created, you may want to run a report to see what alerts have been generated. You can do this by looking at the Alert Rule Summary report in the Reports view (tab). Please see the "Generate Reports" topic on page 623 for more detail about reports.

Telecom Expense

1. Create an Telecom Expense Rule

   A Telecom Expense Rule allows Administrators and Users to be notified on current usage of company data and voice minutes. Please see the "Windows Mobile Telecom Expense Management" topic on page 807 for more information.

2. Check the Telecom Expense Rule execution status.

   Once the Alert Rule has been created, you may want to run a report to see what alerts have been generated. You can do this by looking at the Telecom Expense Rule Summary report in the Reports view (tab). Please see the "Generate Reports" topic on page 623 for more detail about reports.

Adding Windows Mobile Devices

Add devices rules allow MobiControl to name devices, place devices in the appropriate device group, and to generate a customized MobiControl Device Agent that, when installed onto devices, allows them to be managed by MobiControl.

When you generate a Device Agent for an add devices rule, MobiControl places an identifier for the rule (i.e. rule tag) into the `.cab` file for the generated agent. When the Device Agent is installed onto a device, it will connect to a MobiControl Deployment Server and supply the rule tag to the server. The server will then look up the add devices rule and configure the device accordingly.

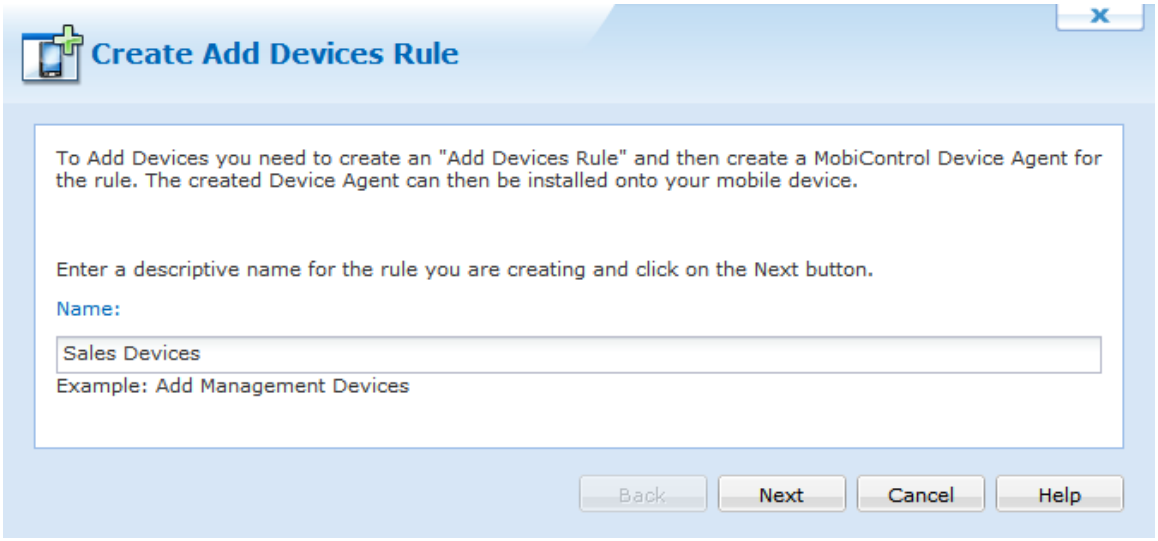
To create an add devices rule, select the Rules view (tab) within MobiControl Manager, then click the **Rule** menu, select **Create Rule**, and click **Add Devices Rule**. The Create Add Devices Rule Wizard will be displayed.

The six steps below describe how the Create Add Devices Rule Wizard can be used to create an add devices rule:

1. Start the wizard.

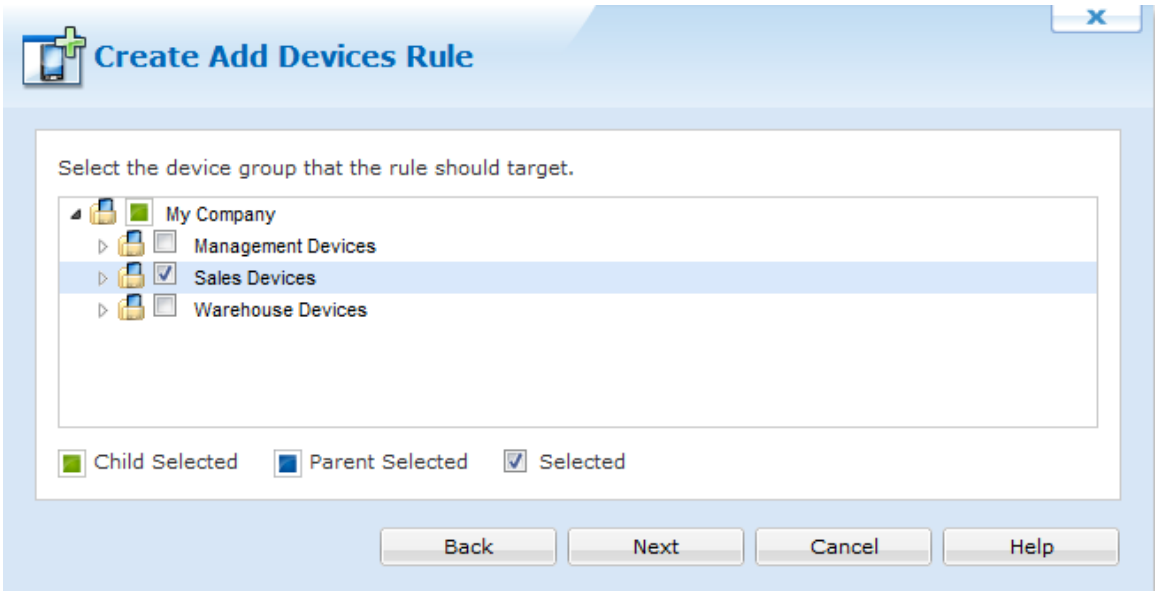
   Select the Rules view (tab), then click the **Rule** menu, select **Create Rule**, and click **Add Devices Rule**. The first page of the Create Add Devices Rule Wizard will be displayed.

   Enter a descriptive name for the add devices rule you are creating and click **Next.**



First page of the Create Add Devices Rule Wizard

2. Configure the device group.



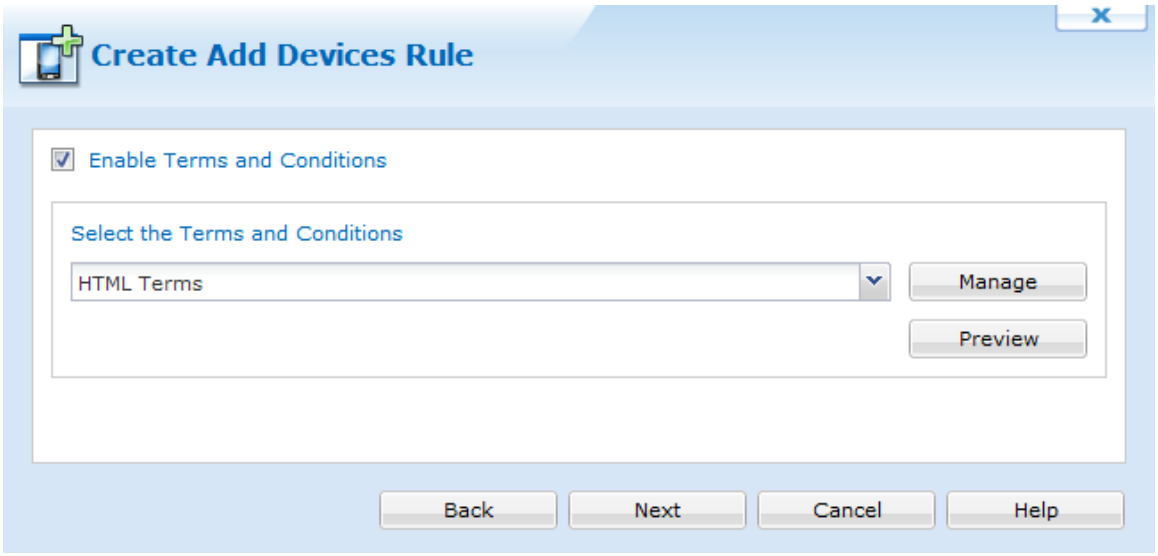
Device Group Selection page

First, select to which device group the devices configured by this rule will be added. The dialog box below displays the current device tree. Select the group where devices need to be inserted and then click **Next.** If you need to add a new group or change the structure of the device tree, exit the wizard, go to the Devices view (tab), edit the tree, and then begin the wizard again.

After selecting a device group click on the **Next** button.

3. Terms and Conditions

The terms and conditions page allows us to send terms and conditions to devices. Users must accept these terms before they are able to enroll their device to MobiControl. If they do not accept the terms and conditions, the device will not connect. If Terms and Conditions is required, click "Enable Terms and Conditions".



Terms and conditions

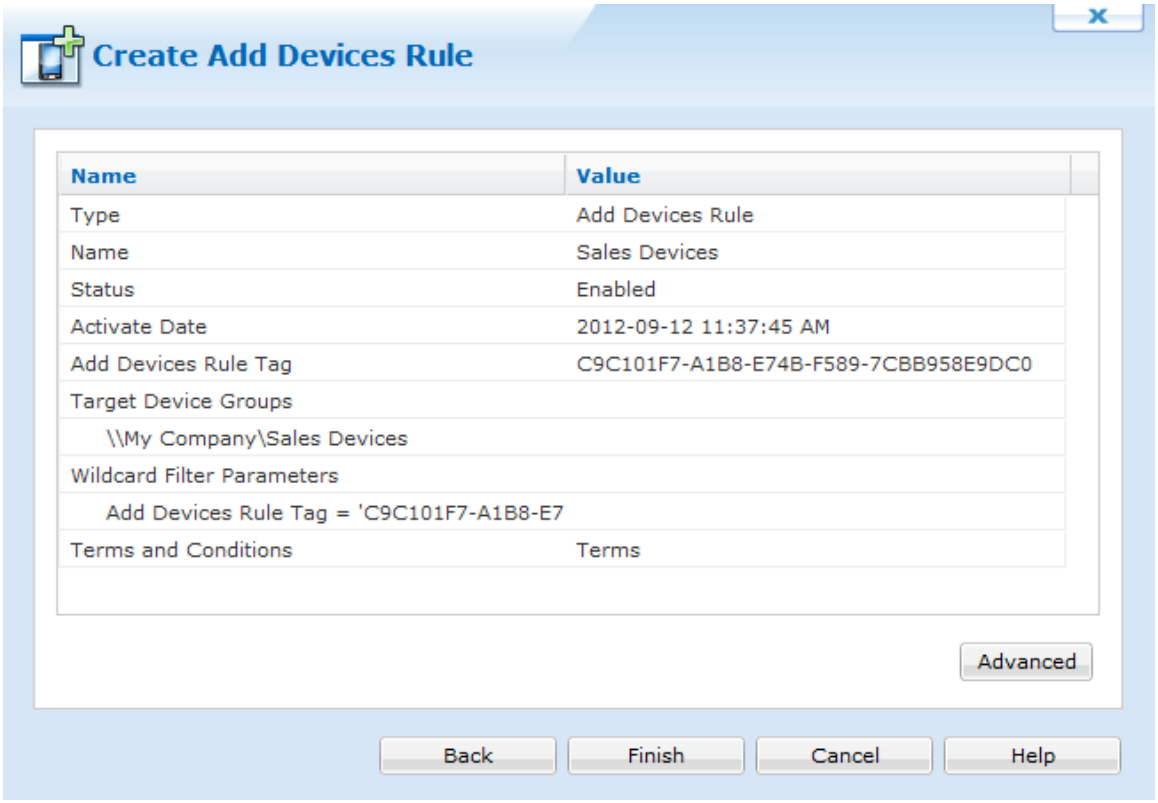
To add new Terms and Conditions to the Add Devices rule, click Manage. Once clicked, we can see the Terms and Condition Manager. Please see the "Terms and Conditions" topic on page 619 for more information.

After selecting the Terms and Conditions, click **Next** to continue the creation of the rule.

4. Review summarized information.

The **Rule Summary Information** page summarizes the settings configured on the previous pages of the wizard.

If you are satisfied with the configured settings, click on the **Finish** button to create the device rule, otherwise use the **Back** button to go to previous screens and make adjustments.

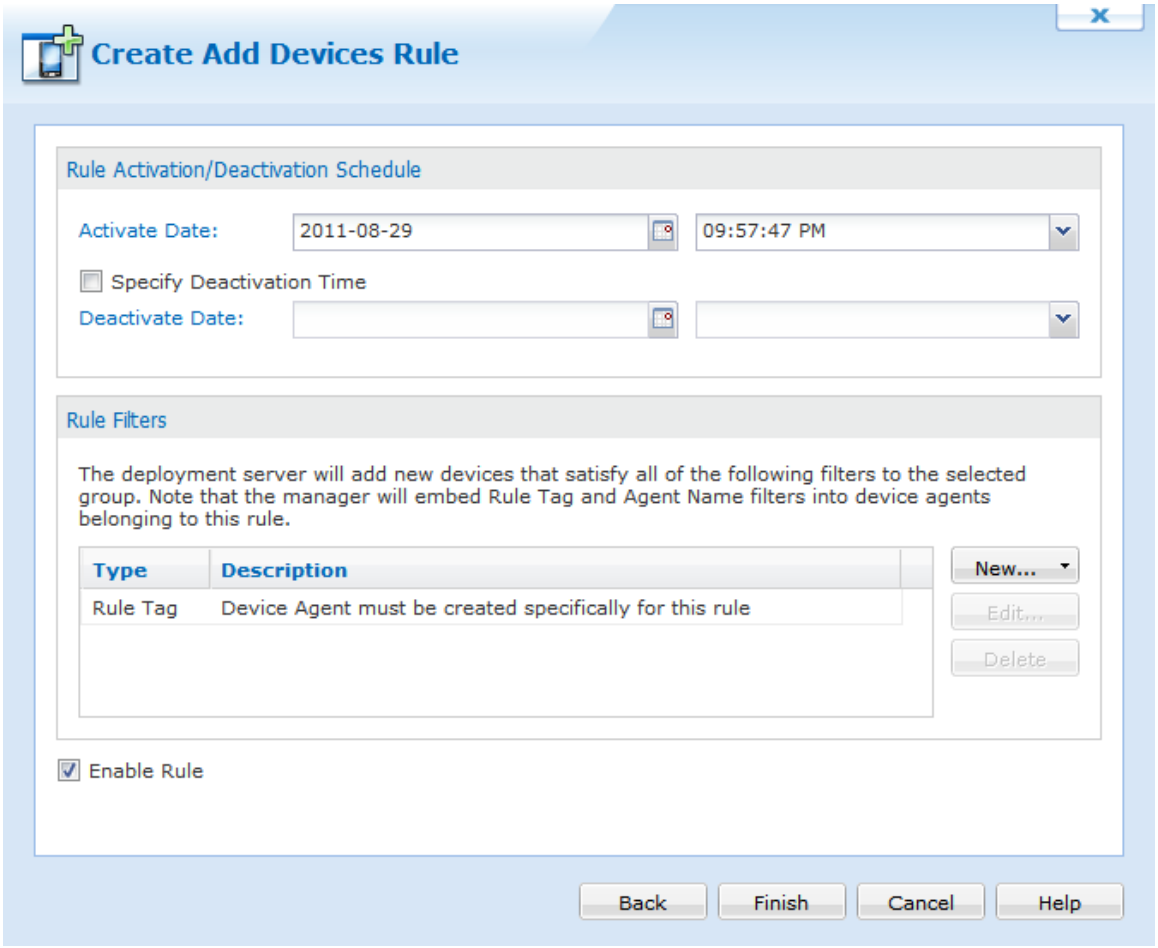


Rule Summary Page

5. Advanced Settings.

   The **Advanced Settings** button allows you to specify which devices are to be configured by this rule. By default, MobiControl will use this rule to configure only those devices that are running a Device Agent created specifically for this device rule. By using advanced settings filters, you can broaden or further restrict which devices get configured by this rule when they connect to MobiControl.

   Once you have made the changes, click **Next.**



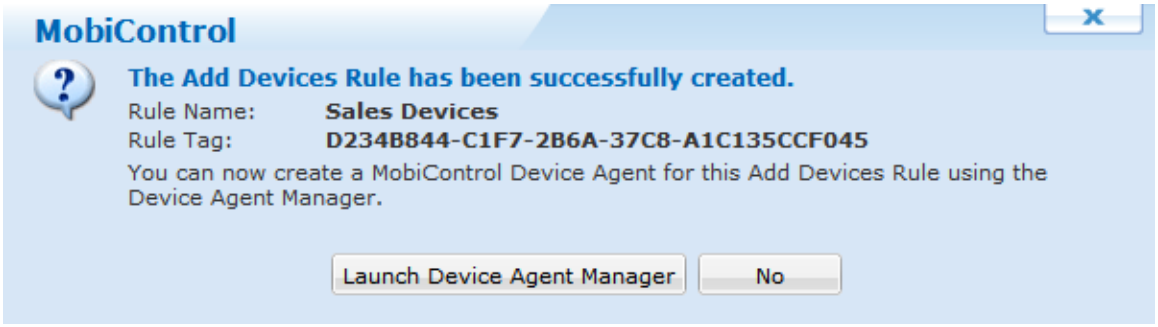
Advanced Settings Page

For additional information about **Rule Tags** see the appropriate section below.

6. Receive confirmation that the rule has been created.

   A notification of rule creation will be displayed once the device rule has been created. The message box confirms that the rule has been successfully created and allows you to immediately generate a MobiControl Device Agent for the rule.

   If you click the **Yes** button on the message box, the wizard to create a Device Agent will be launched. If you click on the **No** button, you can generate a Device Agent later.



Rule Creation Notification message box

NOTE:

You can access the Device Agent Manager from the Rules view (tab) in MobiControl Manager. Right-click on a specific add devices rule in the left pane, and then select **Device Agent Manager** from the pop-up menu.

Once you have created an add devices rule, the next step is to generate a MobiControl Device Agent. You can generate a Device Agent for an add devices rule immediately after creating the rule or at any time after creating the rule using the Device Agent Manager. The generated agent is customized for the specific add devices rule that you select. Please see the "Windows Moible Device Agent Manager" topic on page 755 for instructions on how to create a Device Agent using the Device Agent Manager.

Rule Tag Settings

The **Add Devices Rule Advanced Settings** are accessible from the Create Add Devices Rule Wizard by clicking the **Advanced Button** (Advanced Tab when editing a Rule.) This page allows you to specify which devices are to be configured by a specific Add Devices Ruleadd devices rule. By default when you create an Add Devices Rule, MobiControl will use the rule to configure only those devices that are running a Device Agent Device Agent created specifically for that Add Devices Rule. By using Advanced Settings filters, you can broaden or further restrict which devices get configured by a specific rule when they connect to MobiControl.

Types of Filters

- Rule Tag Filter

  The **Rule Tag filter** will cause the rule to configure only devices with a certain device rule tag. When a MobiControl Device Agent is generated, a unique identifier (rule tag) is inserted into the agent. When the Device Agent connects to a MobiControl Deployment Server, it presents the server with the rule tag. When this filter is used, the Deployment Server will only configure a device if there is a match between the rule tag presented by the agent and an add devices rule in the database. In this way, an add devices rule will be used to configure only those devices that are using an agent specifically created for that rule.

This is the default filter; it is automatically added when an add devices rule is created. If this filter is removed, then this rule can be used to configure devices that are using Device Agents created by third parties (i.e. When a MobiControl Device Agent is already installed on the device when it comes from the manufacturer) or Device Agents created for other device configuration rules.

- IP Address Filter

  The **IP address** filter causes the add devices rule to configure only those devices whose IP addresses are in the range specified. This rule is useful as an extra security blanket for limiting connections to only devices that have an IP within the authorized range of IP addresses. The rule may also serve as a means of segregating different sets of devices.

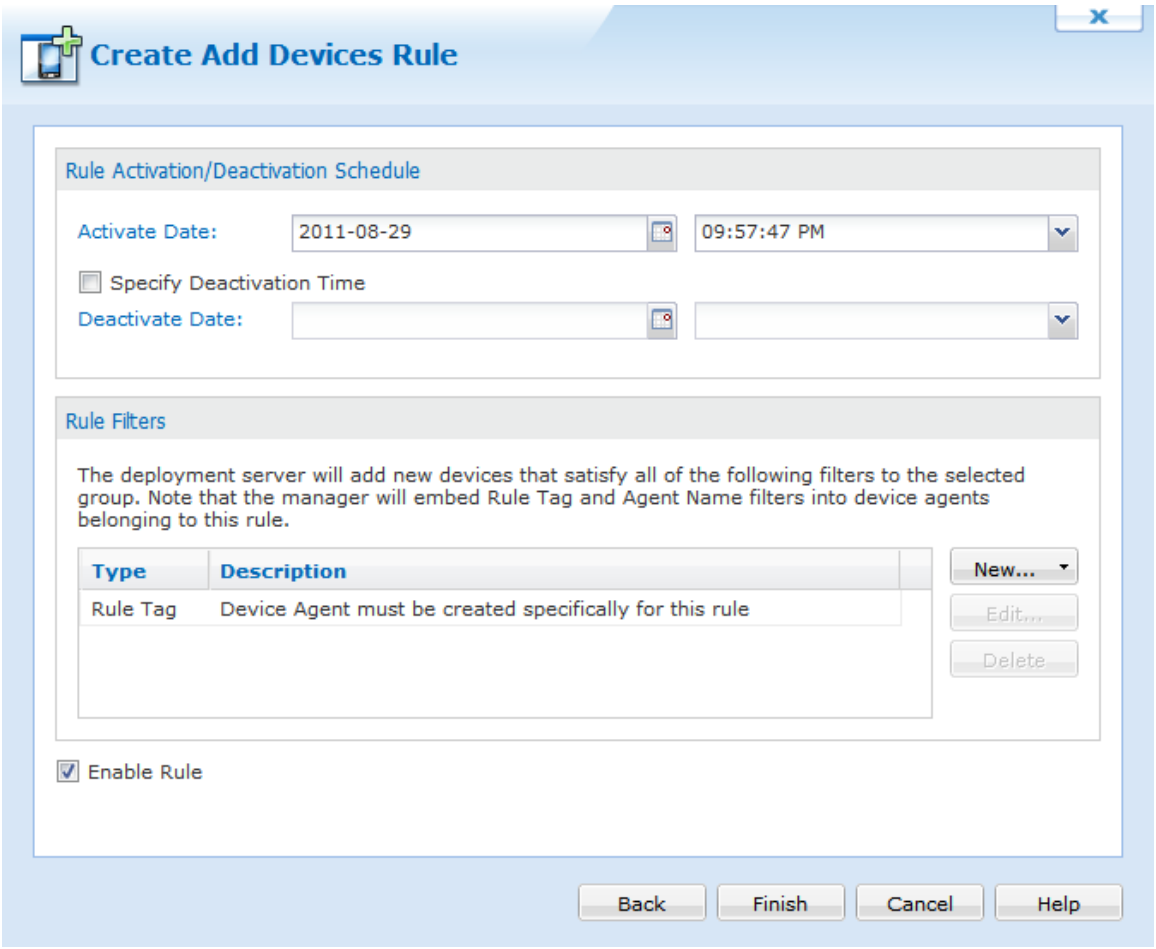
  EXAMPLE:

  If an IP address filter from 192.168.1.10 to 192.168.1.99 has been set, then only devices with an IP address in this range would be configured by this add devices rule. If a device with an IP address of 192.168.1.100 connects to MobiControl, it would not satisfy the IP address filter test for this rule and so, it would not be configured by this rule.

  The IP address filter is used for limiting connections to approved IP ranges. Please see the "Windows Mobile Device Relocation" topic on page 782 for dynamic relocation of devices from one device group to another and reconfiguring devices based on the IP address of the mobile devices (or other criteria).

- Agent Name Filter

  The **agent name filter** causes the add devices rule to affect only devices with the same agent name. When this filter is set, all agents generated for this rule will automatically be named appropriately. This rule is useful in the event you have a set of devices already equipped with Device Agents. Simply creating this rule will allow the Device Agents on those devices to connect to the Deployment Server.

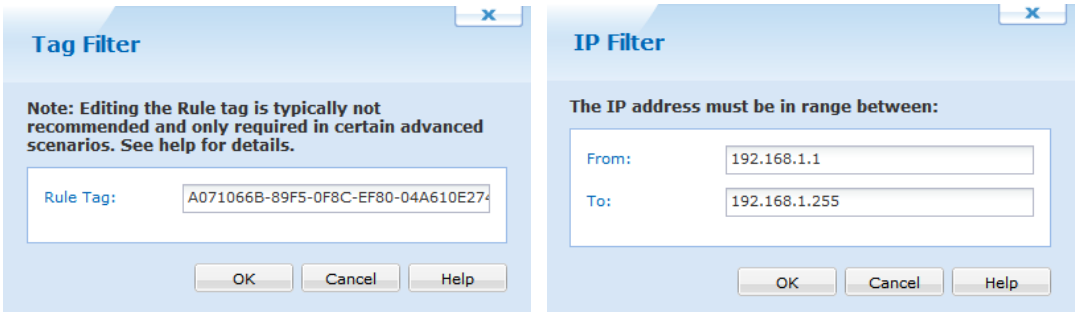


Add Devices Rule Advanced Settings dialog box

Adding a Filter

To add a filter, click the **New** button and select the appropriate filter type from the pop-up menu.

The dialog box displayed depends on the type of filter selected. If the **Add IP Address Filter** was selected from the menu, the **IP Address Filter** dialog box will be displayed. If an **Add Devices Rule** is created, the filter is automatically added. This option will not be available if this filter has already been added.



Rule Tag Filter and IP Address Filter dialog box dialog box

To complete the operation, fill in the information asked for in the dialog box and click the **OK** button.

Editing or Deleting a Filter

To edit or delete a filter, select the filter from the filter list and click the **Edit** or **Delete** button.

Windows Mobile Device Agent Manager

Deployment rules allow administrators to automatically provision mobile devices with packages that contain software or data. The following series of steps describes how to use the Create Deployment Rule Wizard to create a deployment rule.

Creating the Agent with Device Agent Manager

The Device Agent Manager is an interface that allows the user to manage the Device Agents that are installed to the devices. A Device Agent is a program that is installed on to the various devices that are to be managed by MobiControl. The software facilitates the server-client communications. The Device Agent Manager allows creation of custom Device Agents that have been specially configured to the settings of your MobiControl installation and the type of devices you have.

You can access the Device Agent Manager from the Rules view (tab) in MobiControl Web Console by right-clicking on a specific add devices rule in the left pane, and then selecting **Device Agent Manager** from the pop-up menu.

Once you have created an add devices rule, the next step is to create a MobiControl Device Agent. You can create a Device Agent for an add devices rule immediately after creating the rule or at any time after creating the rule using the Device Agent Manager. The created agent is customized for the specific add devices rule that you select.

The following steps outline how to create a Device Agent using the Device Agent Manager.

1. Create a Device Agent

Device Agent Managerdialog box

The MobiControl Device Agent Manager allows you to create a Device Agent for a specific add devices rule. The Device Agent Manager also allows you to view and copy files for Device Agents previously created. After creating a device rule, you can access the Device Agent Manager by clicking on the **Yes** button on the message box displayed immediately after the rule is created, or by going to the Rules view (tab) in MobiControl Manager, and then right-clicking on a specific add devices rule in the left pane, and then selecting **Device Agent Manager** from the pop-up menu.

The Device Agent Manager displays a list of the Device Agents that have previously been created for the selected device rule, and allows users to create new Device Agents, provision Device Agents onto devices (by directly installing, exporting or generating barcodes) and to delete obsolete Device Agents. For newly-created add devices rules, the list will be empty until an agent is created.

If an agent has been already created, select the Device Agent and click on **Provision Device**

The following methods can be used to provision the Device Agent on the devices.

You can download the agent installer by clicking on **Self-Extracting Executable** button

You can publish the Device Agent to your deployment server's website by clicking on **Device Agent URL Address**

To delete an agent, select the agent from the list and click the **Delete Agent** button.

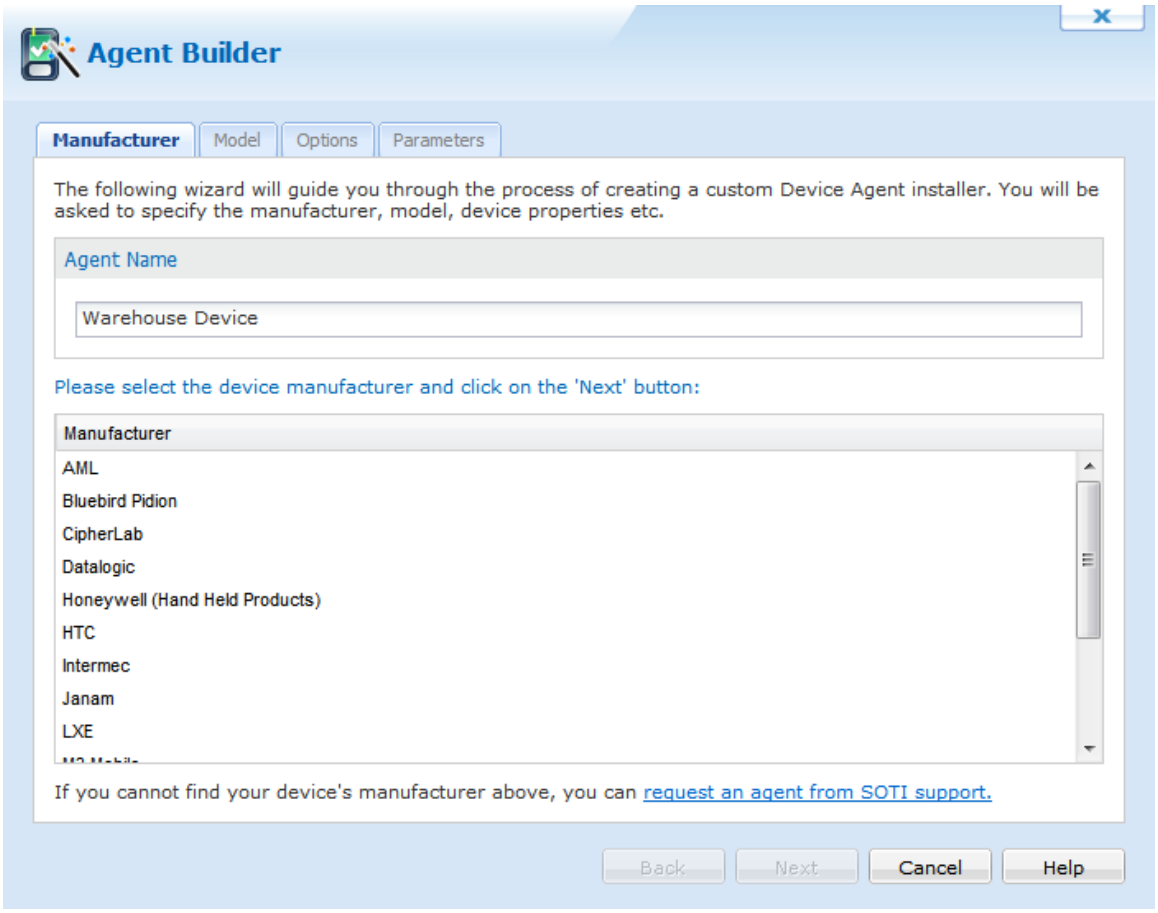
To create a new agent, click the **New Agent** button, the Device Agent Wizard will be displayed.

2. Name the Device Agent and specify the manufacturer.

This will allow you to add a custom name to the Device Agent, which will help to identify it.

Select the manufacturer of your device and click the **Next** button. If the manufacturer of your device is not listed you can try selecting the **Other Manufacturers** option and click the **Next** button or you can contact us to make sure that your device is properly supported.

After providing the device name and selecting the manufacturer, click the **Next** button.



3. Select the device model and configure device type

From the second page of the Device Agent Wizard you will be prompted to select the appropriate device model based on your previous selection. In previous versions of MobiControl where OS and Processor type had to be inserted, this is now done automatically

The **Device Type** dialog box allows you to configure platform, processor and operating system information about your devices. If you dock one of your devices via ActiveSync, and click on the **Detect Settings** button, the wizard can automatically detect most of the device settings. If your device is not docked you can enter the settings manually.

Manufacturer Selection page

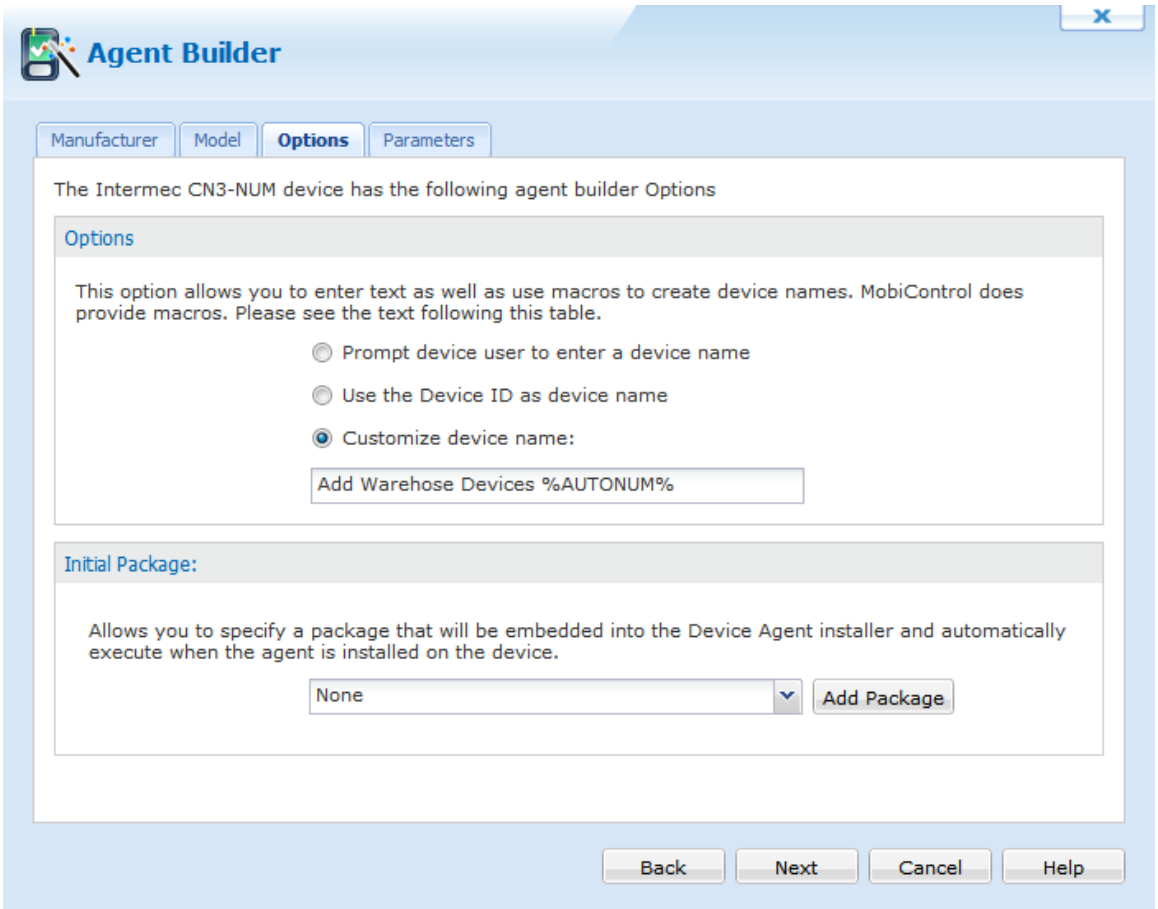
NOTE:

The OS version refers to the version of Windows CE or Windows Mobile. For example, if the version of the OS is 4.20, set the **OS Major Version** field to 4, and set the **OS Minor Version** field to 2. You can get information about the OS and the processor from the device. Typically, this information is available at the following locations for these mobile devices, however this may vary for some devices. If the device says Windows Mobile, and is a touch screen enabled device, select Pocket PC even though it says CE below on the CE OS Build. If the device is not a touch screen, select Smartphone.

Device type	OS or Processor Information
Pocket PC	Select **Start**, then click **Settings**, click **System**, and click **About** to view the information.
Smartphone	Select **Start**, then click **Settings**, and click **About** to view the information.
Windows CE	Select **Start**, then click **Settings**, click **Control panel**, and click **System** to view the information.

4. Configure the device identifier and specify an initial package

   The **Device Identifier Configuration** page allows you to select how devices are named and uniquely identified.



Method Selection page

The following table provides descriptions for the three device naming options:

Field Name	Description
Prompt Device User	When this option is selected, the Device Agent will prompt the user for a device name when it is first started.
Use the Device ID	When this option is selected, the device ID will be used as the device name. Since the device ID is a cryptic string that is not very readable (e.g. `0003000F-3EAC-0F94-0F00-0300AA3EE877`), we generally do not recommend this option.
Customize the Device Name	This option allows you to enter text as well as use macros to create device names. MobiControl does provide macros. Please see the text following this table.
Set Windows Device Name Checkbox	When this option is checked, MobiControl will set the Windows Device Name to be the same as the MobiControl Device Name configured above.

Macros

- **`%AUTONUM%`** allows you to automatically use a numbered sequence as part of the device name. For example, if the value of this field is set to `WH%AUTONUM%`, then the first device configured will be assigned a name of `WH00001`, the second device will have a name of `WH00002`, and so on. `%MAC%` expands to the MAC address of the device. This macro is suitable for use with devices that have a wireless or wired networking capability. The MAC address is a unique number that is built into the network hardware used on the device. In most cases MobiControl can retrieve the MAC address from the hardware. For example, if the value of this field is set to `DEV%MAC%`, then the device names configured would look similar to `DEV00A0F85324D4` and `DEV00A0F8533422`. When the MAC macro is used as the Device ID, the Wi-Fi radio must be enabled when the agent is installed in order for the macro to work.
- **`%HOSTNAME%`** expands to the local host name of the device. We recommend using this macro only in cases where unique hostnames have previously been assigned to devices before the MobiControl Device Agent software is installed.
- **`%IP%`** expands to the IP address of the device. We recommend using this macro only in cases where the mobile devices have wireless or wired networking capabilities and are using fixed IP addresses. The use of this macro is not suitable for situations in which the mobile devices are using dynamic IP addresses (i.e. DHCP) since when the IP address changes the device name will be incorrect.
- **`%PHONENUMBER%`** expands to the phone number of the device. We recommend using this macro only in cases where the mobile device is a Smartphone or Pocket PC Phone Edition. For some devices, the phone number may not be available.

- **%IMEI%** expands to the IMEI (International Mobile Equipment Identity) number of the device. We recommend using this macro only in case where the mobile device is a Smartphone or Pocket PC Phone Edition. For some devices the IMEI number may not available.
- **%ESN%** expands to the ESN (Electronic Serial Number) number of the device. We recommend using this macro only in case where the mobile device is a Smartphone or Pocket PC Phone Edition. For some devices the ESN number may not available.
- **%IMSI%** expands to the IMSI (International Mobile Subscriber Identity) number of the device. We recommend using this macro only in case where the mobile device is a Smartphone or Pocket PC Phone Edition. For some devices the IMSI number may not available.
- **%REG://%** expands to the registry in the device. This will allow custom names like serial number (read from registry key) to be used out of the box for device naming, e.g. `%REG://HKEY_LOCAL_MACHINE\Software\Apps\SOTI\MobiControl?VN=ESN%`
- **%TXT://%** will get the content of specified line of the text file (if LN is not specified, it assumes the first line), e.g. %TXT://\Device.log?LN=1%
- **%INI://%** will pull a value from a Section in an `.ini` file and make it the device name, e.g. `%INI://\pdb.ini?SC=Device&NM=DeviceName%`
- **%EXE://%** will get the exit code of the executable and make it the device name, e.g. `%EXE://\windows\system32\calc.exe%`
- **%STDOUT%** will pull the first line of STDOUT output of the Executable and make it the device name, e.g. `%STDOUT://cmd.exe /c dir%`

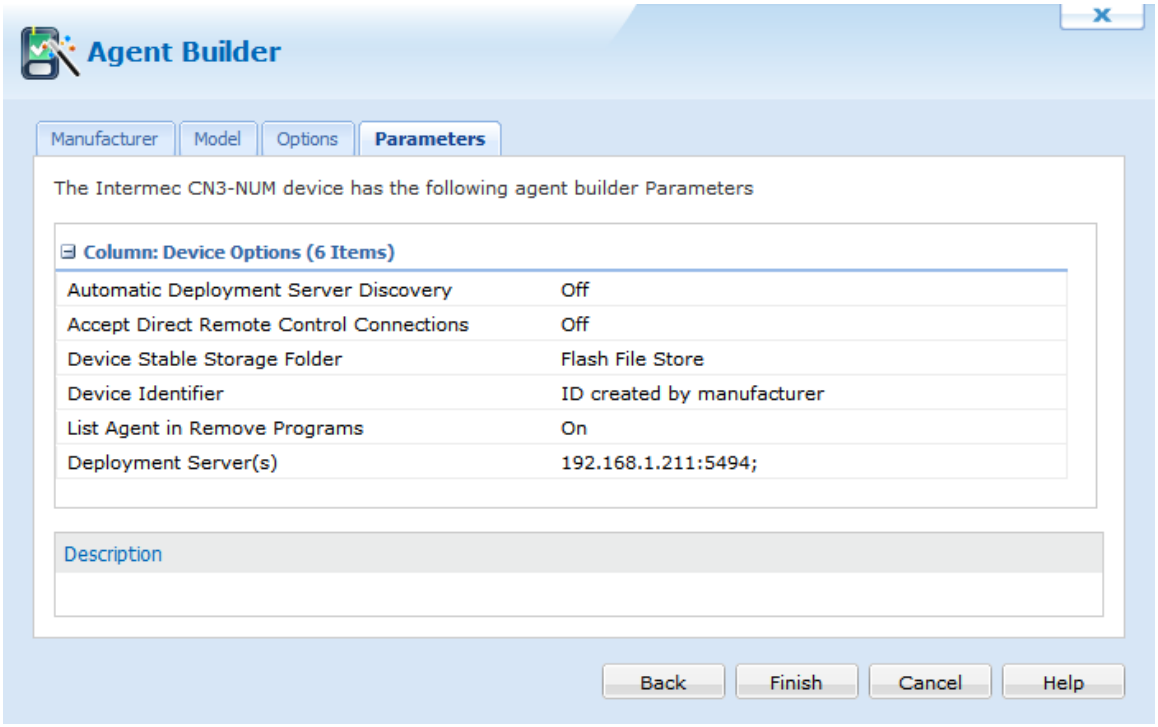
Include Initial Package

This feature allows you to specify a package that will be embedded into the Device Agent installer and automatically execute when the agent is installed on the device.

Click **Next** when you have completed the settings in this dialog box.

5. Configure software settings

The **Software Settings** page allows you to configure various parameters built into the agent. Click the **Next** button when you have completed the settings in this dialog box.

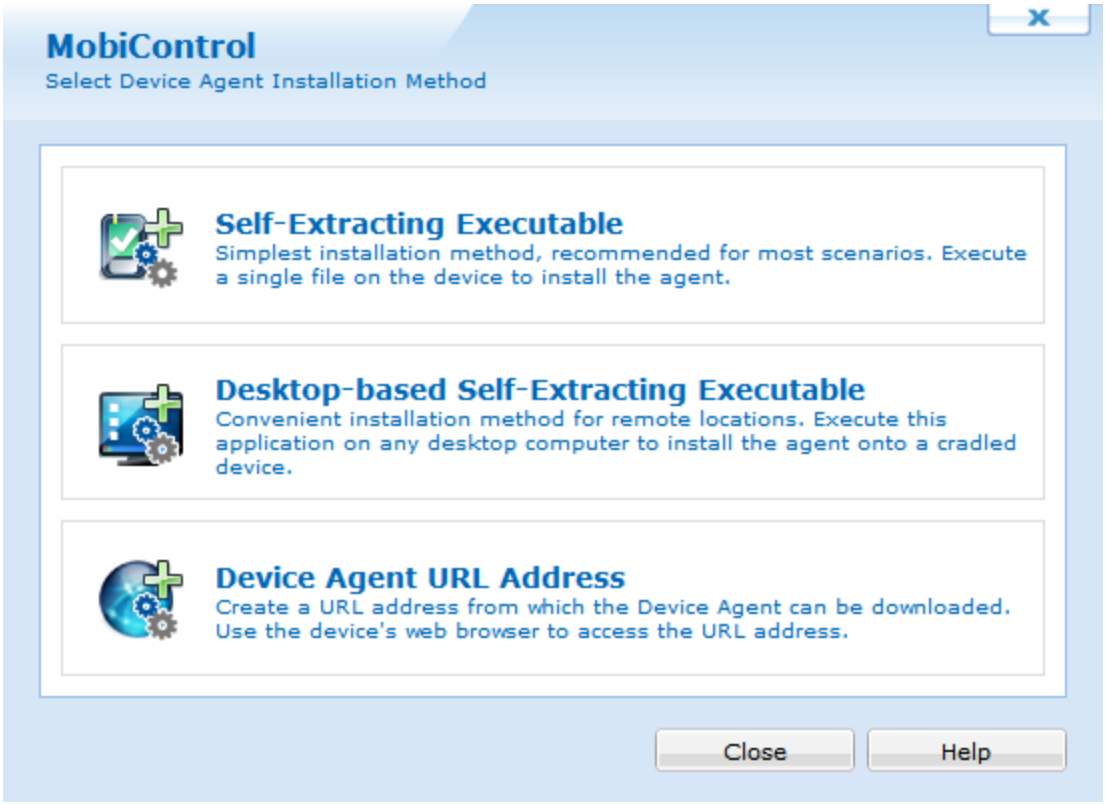


Device Agent Wizard - Software Settings page

Field Name	Description
Deployment Server(s)	Devices that have the MobiControl Device Agent software installed onto them connect to MobiControl Deployment Servers to receive configuration information as well as to get provisioned with software and data. It is crucial that the device is able to reach the IP address of the Deployment Server via the IP network to which the device is connected. If your device will be on a public network such as the Internet, you will need to setup an externally routable address for your Deployment Server. Please see the "Registering MobiControl" topic on page 608 for instructions on setting up an external IP address for the Deployment Server. **NOTE:** Configuration of the Deployment Server address should be performed before agents are created, as the address information will be embedded into the agent installer.

Field Name	Description
Automatic Deployment Server Discovery	When this option is enabled, MobiControl Device Agent(s) will attempt to discover Deployment Server(s) using UDP broadcasts when they cannot connect to configured servers. If you have multiple MobiControl installations on the same network, you need to set a unique site name for each installation so that the discovery process will not detect servers in a different installation.
Accept Direct Remote Control Connections	When this option is enabled, the Device Agent will accept direct remote control connections (TCP/IP remote control connection profile). A direct connection improves performance by reducing latency, however it requires the device to accept the connection without authentication unless SSL Security is enabled. (Please see the "Communication and Connection Security" topic on page 411 for more information about this.) Remote control is permitted via the TCP/IP(Server) remote control connection profile regardless of this setting.
List Agent in Remove Programs	When this option is disabled, no entry will appear for the agent in the Remove Programs settings applet on the device, thus preventing the agent from being uninstalled by the device user.
Device Stable Storage Folder	A stable storage folder is a special folder in the devices file system that is not erased when a device is hard reset. MobiControl uses the stable storage folder on the device to store data and packages so that MobiControl and packages and settings deployed via MobiControl can persist through hard reset.  **NOTE:** Stable storage folders do not exist on all devices. For devices that do not feature a stable storage folder, MobiControl will default to a standard folder in the file system. Optionally, you may use an external SD card as the stable storage folder. This option is not recommended in most scenarios, as removal of the SD card will severely impact the operation of the MobiControl Agent.

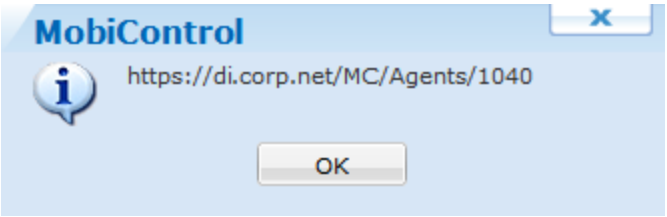
6. Provisioning agent on a device



Provision Device Page

After the agent is created, you have three installation options.

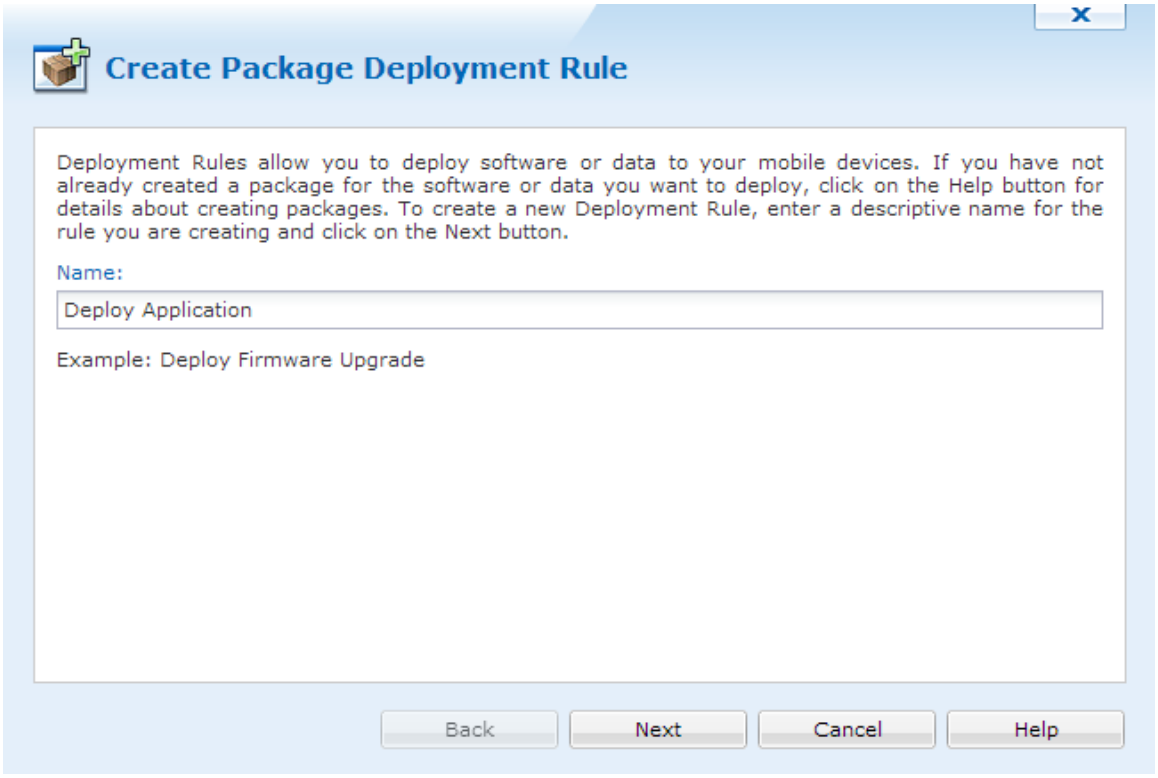
Option	Description
Self-Extracting Executable	This is the simplest installation method and is recommended for most scenarios. A single executable file (`*.exe`) will be exported. To install the agent, simply deliver this file to the device and execute it. The self-extracting executable contains the agent's installation `.cab` file, as well as any other supporting files that may be required for targeted device platform. **NOTE:** This method is not supported on Windows Mobile 5 Smartphone or Windows Mobile 6 Standard devices.
Desktop-based Self-Extracting Executable	Convenient installation method for remote locations. Execute this application on any desktop computer to install the agent onto a cradle synced device. This will open a light application that will install the agent on to the device via ActiveSync.

Option	Description
Device Agent URL Address	This option posts the device agent's `.exe` file in a special directory on the MobiControl Web Console allowing you to send the URL to the end user to have them download and install the MobiControl device agent quickly and easily. 

Windows Mobile Package Deployment

Deployment rules allow administrators to automatically provision mobile devices with packages that contain software or data. The following series of steps describes how to use the Create Deployment Rule Wizard to create a deployment rule.

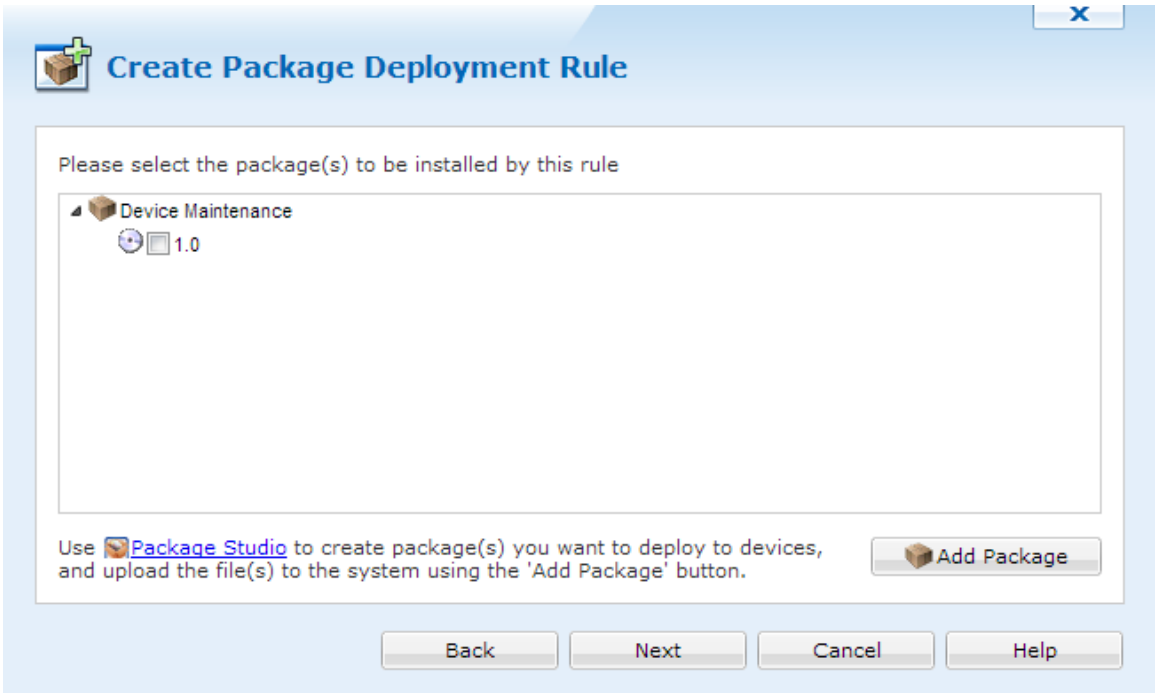
1. Start the wizard.



First page of the Create Deployment Rule Wizard

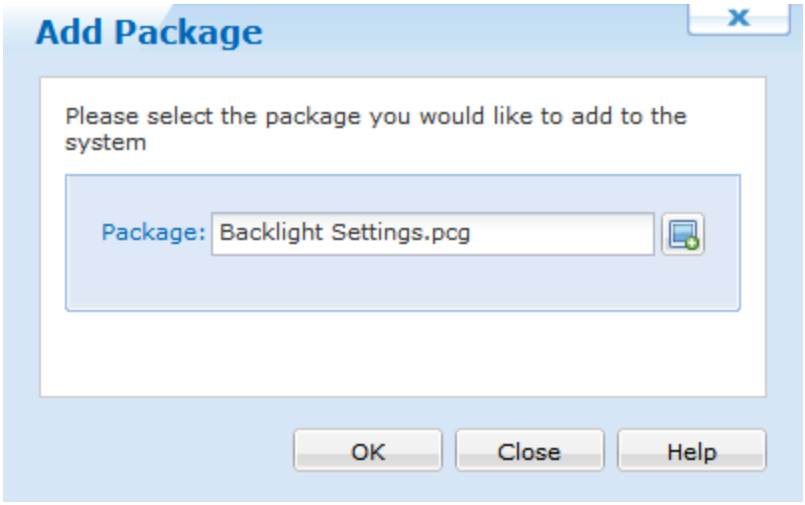
From MobiControl Manager select the **Rules view (tab)**, then click the **Rule** menu, click **Create Rule**, and click **Deployment Rule**. The first page of the Create Deployment Rule Wizard will be displayed. Enter a descriptive name for the deployment rule you are creating and click **Next**.

2. Select the package(s) to be deployed.



Select Package page

The dialog box displays a list of the packages that have been previously loaded into the MobiControl database. Select the relevant packages that need to be installed by this rule.

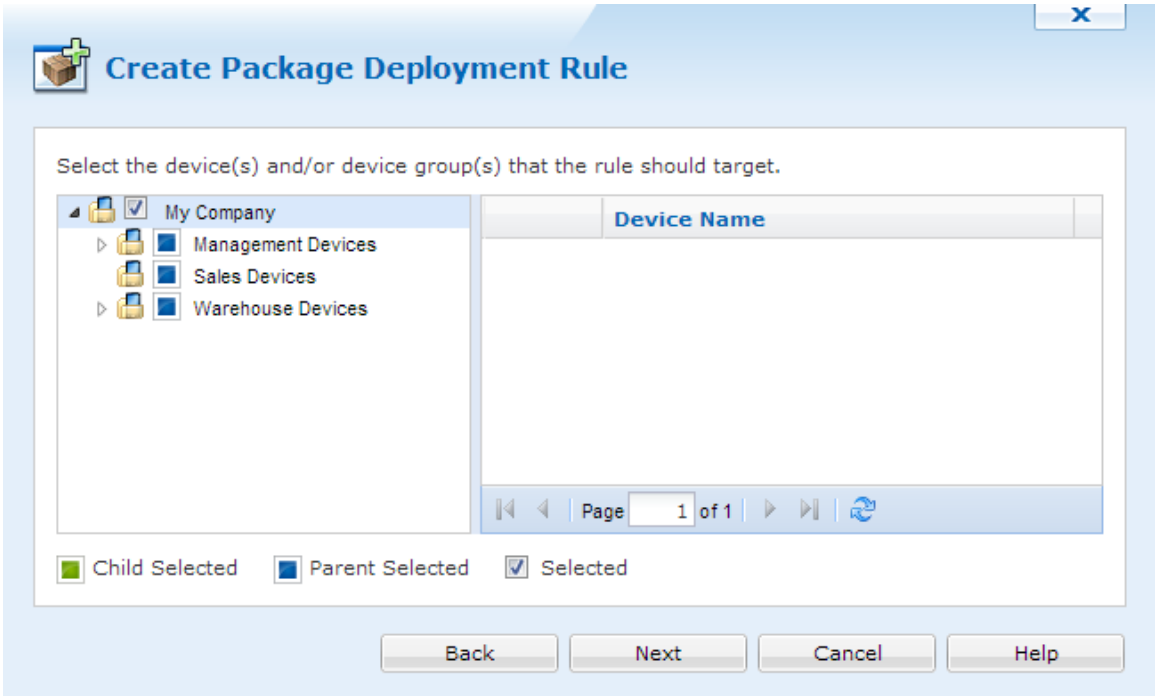


Add Package dialog

If the package to be installed has been created but not loaded into MobiControl, click the **Add Package** button and select the package file from the file system.

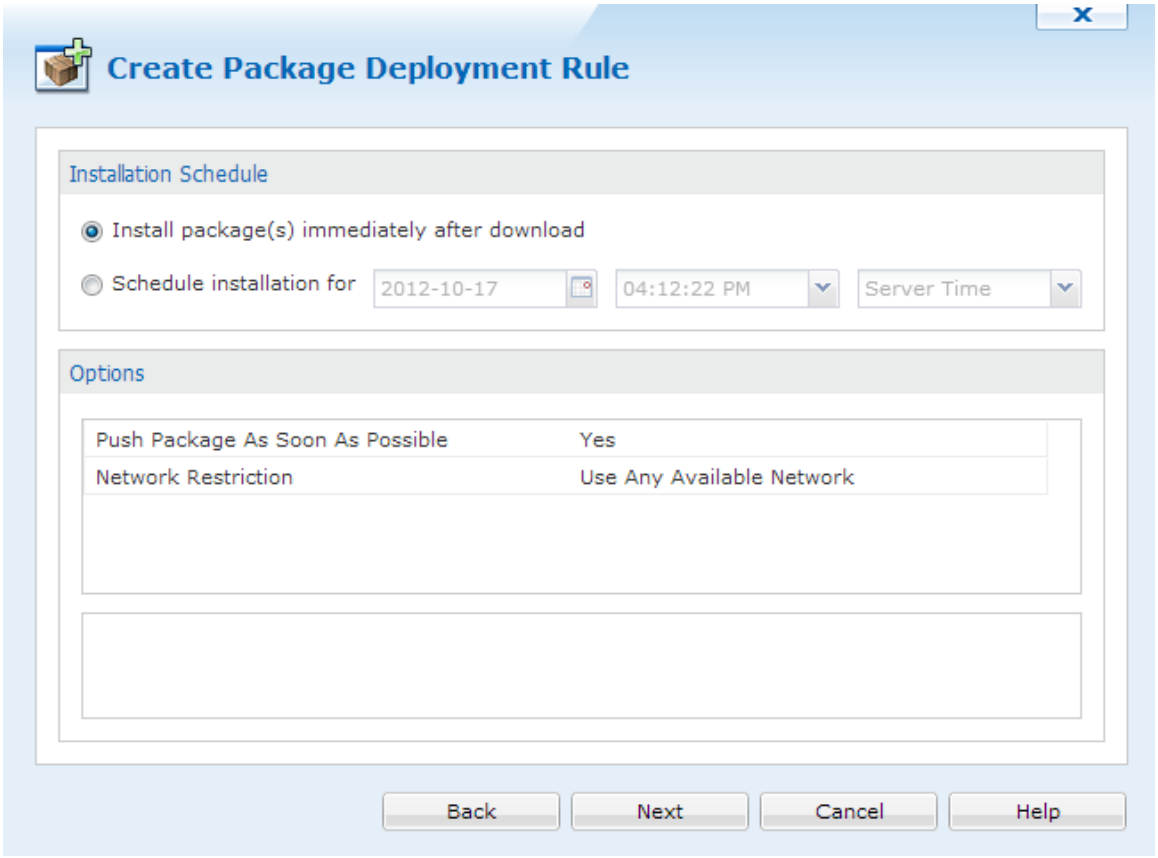
If the package has not yet been created, exit the wizard and use MobiControl Package Studio to create a package. (Please see the "MobiControl Package Studio" topic on page 413.)

3. Select where the package(s) will be deployed.
   Select the device(s) or group(s) to which the package(s) will be deployed and click the **Next** button.



Device Group Selection page

4. Configure deployment rule activation schedule and optional settings.



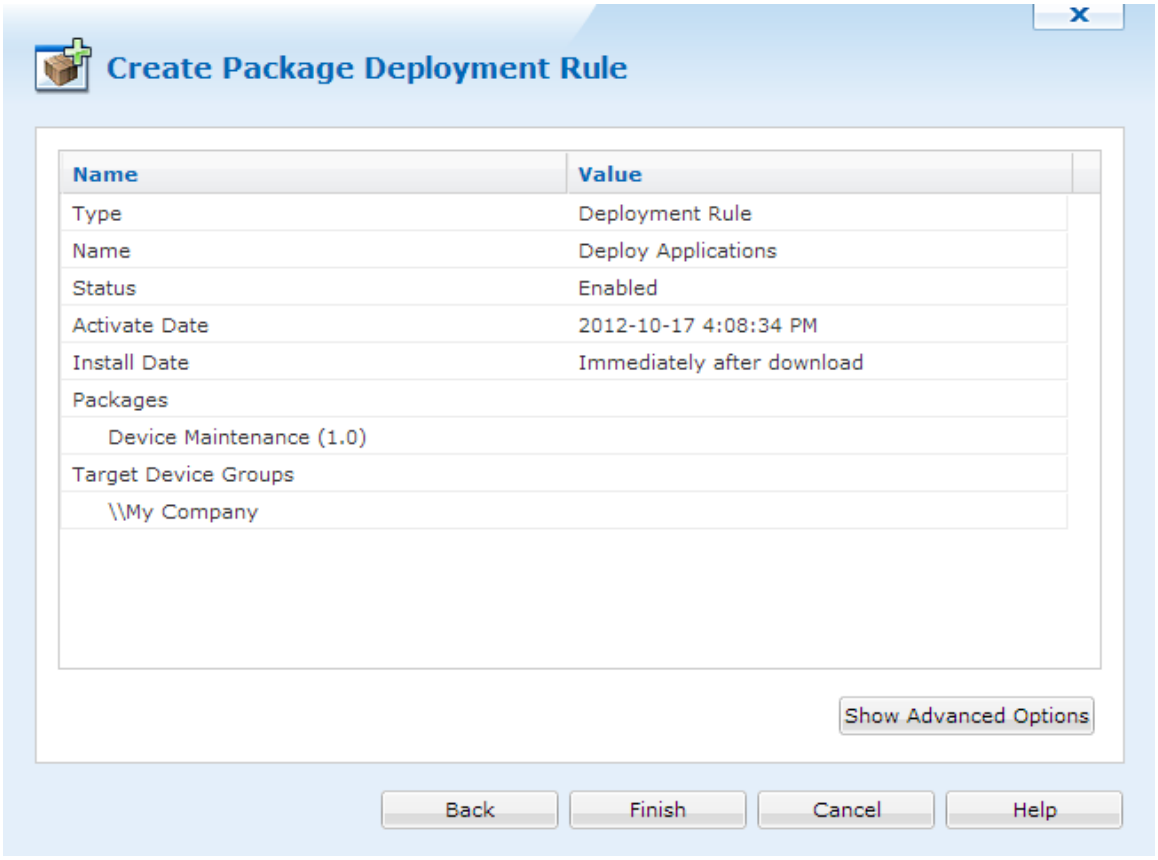
Device Settings Configuration page

The deployment rule can be deployed at real-time or at a pre-set time. The deployment rule, although set to be activated at a scheduled time, can also be set to be deactivated. The deactivation setting is optional.

Field Name	Description
Install immediately after download	If this checkbox is cleared, the installation of a downloaded package will be delayed till the specified Installation Date. The Installation Date must be after the Activate Date. If a package depends on another package that is scheduled to install at a later time, then the Deployment Server will not push the package unless it is also scheduled to install at the same time or later.
Push Packages As Soon As Possible	By default, packages will be deployed to the devices according to the device synchronization schedule. The device synchronization schedule is specified by the add devices rule used to add the device to MobiControl. If this option is selected, package(s) will be deployed to the target devices immediately. If the devices are currently offline, the package(s) will be deployed as soon as the device connects to MobiControl.
Network Restriction	Restrict whether package deployment should take place over cellular data networks.
Persistently Store Package(s)	For devices with stable storage, persistently storing packages allows them to be reinstalled after a hard reset, without needing to connect to the Deployment Server.
Uninstall Contents upon Rule Deletion	This is relevant when the rule has been deleted or is no longer assigned to a device, for instance because it was moved to a new group or the rule was edited to target a different group. • If **Yes** is selected, the package will be removed from the device, and the uninstallation logic of the packages will be executed. • If **No** is selected, the package will be removed from the device, but no uninstallation logic will be executed. The uninstallation logic depends on what the package contains, for example, when a rule that deploys a package containing a `.cab` file is deleted. • If the **Uninstall Package(s) upon Rule Deletion** option is set to **Yes,** the application installed by the `.cab` file will be removed. • If the **Uninstall Package(s) upon Rule Deletion** option is set to **No**, the application installed by the `.cab` file will remain installed.
Always Force Reinstall	Packages will be reinstalled on to the device regardless of whether they are already installed.
Rule Priority	This option allows you to prioritize the deployment of the package(s). Package dependencies (introduced in version 3.06) are the recommended means to ensure the order in which packages are installed on the devices.
Enable Rule	If you wish to activate the rule, that is, to install the package(s), then this field needs to be checked. This option is also made available by right-clicking the rule in the Rules view (tab). When you disable a deployment rule, MobiControl will attempt to uninstall the packages that were being deployed by that rule. If the package(s) that were being deployed contained `.cab` files, MobiControl will try to uninstall the `.cab` files as well.

5. Review the summarized information.

   A **summary** of the deployment rule is displayed. Review the settings you have chosen and click **Finish** to complete the wizard.



Summary page

NOTE:

After five unsuccessful attempts to deploy the package, deployment to that device is temporarily deferred. In order to start deployment of that package again, you must right-click the package from the Package panel and select **Force Re-install**.

Creating File Sync Rules

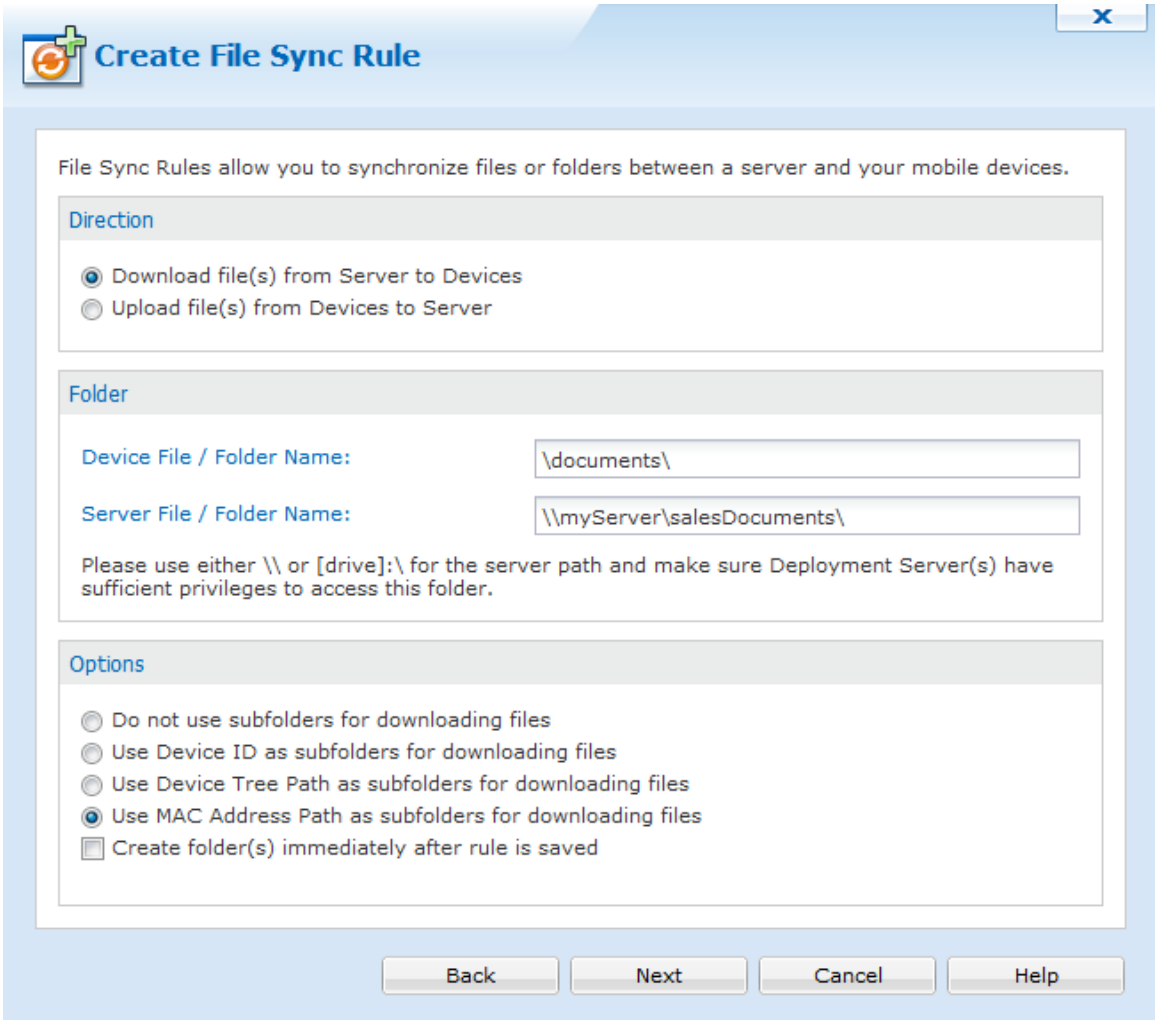
File sync rules allow you to synchronize files and folders between your devices and a server. File collection, also referred to as file uploading, is a very convenient method for gathering information from devices, for example a transaction log file. File dissemination, also referred to as file downloading, is a quick and easy way to send one or more files to a set of devices such as an updated product listing or configuration file.

1. Start the wizard.

   Select the Rules view (tab), then click **Rule,** point to **Create Rule,** and click **File Sync Rule.** Enter a meaningful name for the rule.

First page of the Create File Sync Rule Wizard

2. Configure file synchronization source and destination.



Configure file sync source and destination

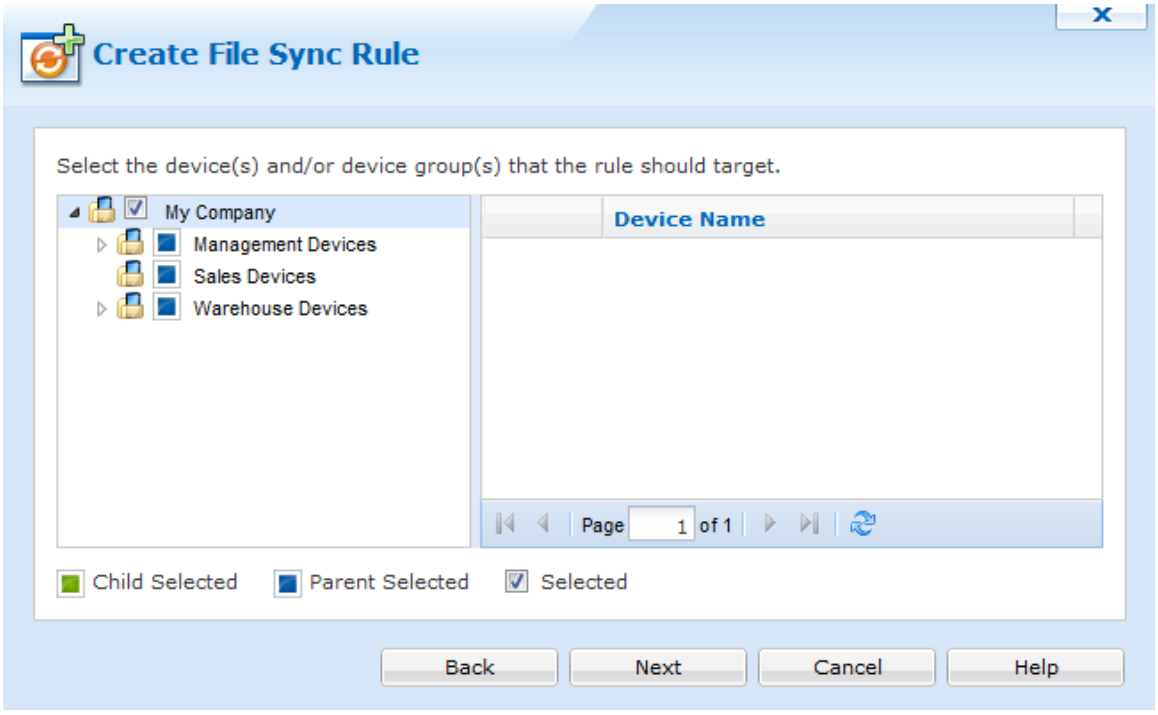
The following table describes the fields of this page of the wizard:

Field Name	Description
Direction	• **Upload** (File collection) The rule will be used to upload files from the devices to a server. • **Download** (File dissemination) The rule will be used to download files from the server to devices.
Device File/Folder	Specifies the complete file system path to the files or folders being synchronized on the device

Field Name	Description
Server File/Folder	Specifies the complete file system path to the files or folders being synchronized on the server It is strongly recommended that a UNC (Universal Naming Convention) path be used. A local path (i.e. `C:\MyFiles`) can be used if only one Deployment Server is being used and the local path is on the computer running the Deployment Server. **NOTE:** It is important that the Deployment Servers have sufficient permission to read and write to the source or destination UNC path. Best practice is to run the Deployment Server under its own Active Directory user profile.
Server-side Folder Options	For **upload rules,** files collected from the devices can be written to: • A single shared folder, meaning files could potentially be overwritten if they have the same name. • A per-device subfolder, named using the device ID (i.e {00135304-41D7-019E-5800-0050BF3F5173}) • A per-device subfolder, named using the device tree path (i.e. `.\Management Devices\Device 0001`) • A per-device subfolder, named using the device MAC address (i.e. 0020E0401234, without colons) For **download rules,** files disseminated from the server can be read from: • A single shared folder, meaning all devices get the same file(s). • A per-device subfolder, named using the device ID (i.e. {00135304-41D7-019E-5800-0050BF3F5173}) • A per-device subfolder, named using the device tree path (i.e. `.\Management Devices\Device 0001`) • A per-device subfolder, named using the device MAC address (i.e. 0020E0401234, without colons) When the **Create folder(s) immediately after rule is saved** option is enabled, the server-side folders will be created immediately after the file sync rule is saved. This allows adding files to the folders on the servers that are synchronized with the devices when the file sync event occurs.

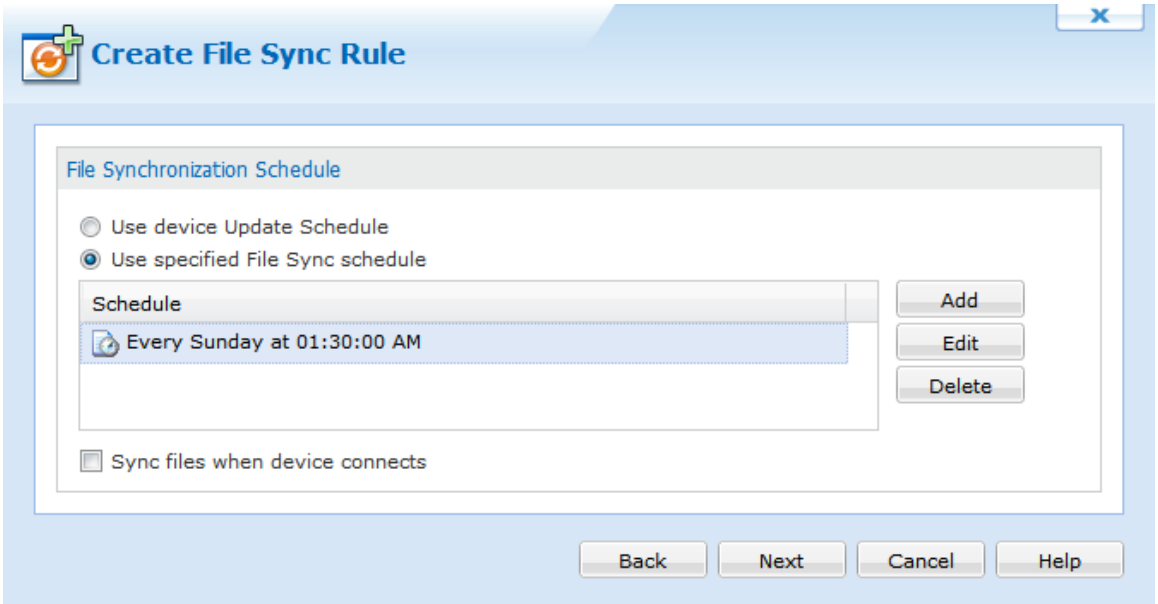
3. Select devices.

   Select the device(s) and group(s) for which the file sync rule will apply.



Device Group selection page

4. Specify the synchronization and activation or deactivation schedule.



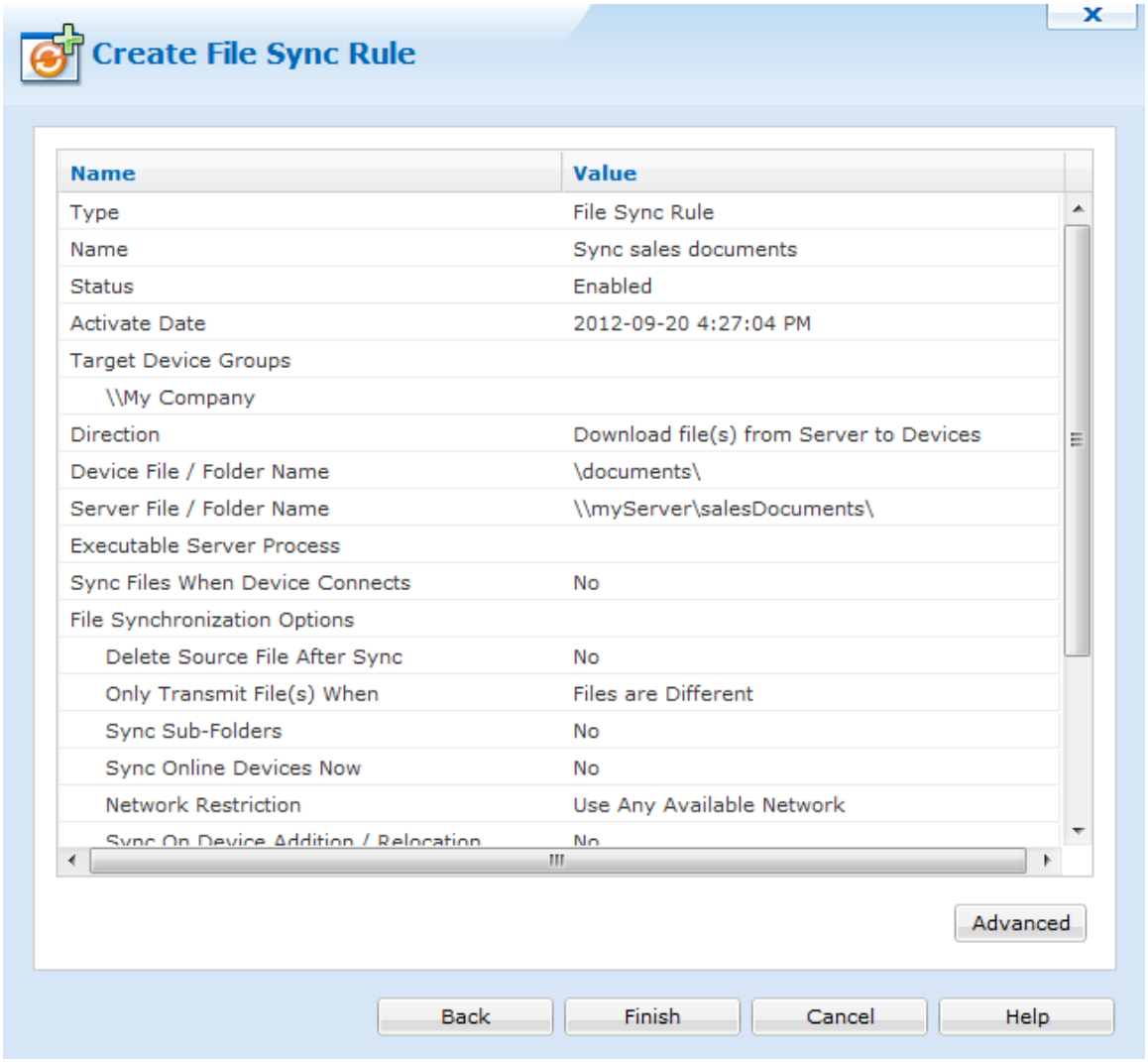
Rule activation schedule

Field Name	Description
Use Device Update Schedule	By default, the device update schedule (specified by the file sync rule used to add the devices to the system) triggers file synchronization
Use Specified File Sync Schedule	If you specify a file synchronization schedule in this dialog box, only that schedule will be used, and the device synchronization schedule will not trigger file synchronization. To Specify the custom schedule click the **Add** button.

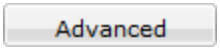
By default, the will be activated immediately upon completion of the wizard. If you wish to delay the activation you can modify the activate date. A deactivate date can optionally be entered to specify a date from which the rule will be disabled. A can also be explicitly disabled by clearing the Enable Rule check box.

5. Review the summarized information and advanced settings.

   Review a summary of information presented by the file sync rule.



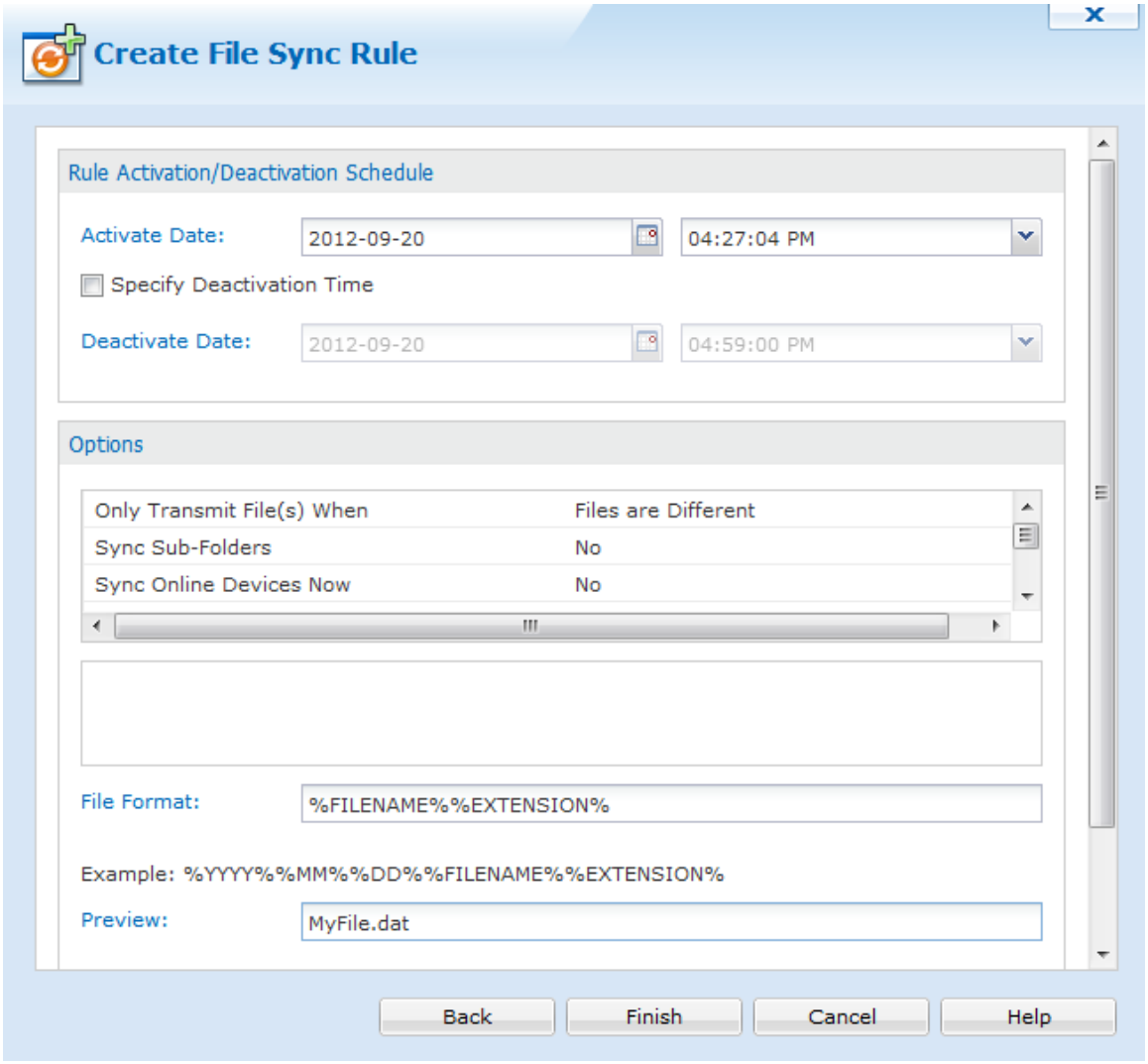
Summary page

Clicking  brings up the advanced settings page. Here we can specify additional options.

The following table describes the file synchronization options on the advanced page of the Create File Sync Rule Wizard:

Field Name	Description
Delete Source File After Sync	(This applies only to upload rules.) When selected, the source file(s) on the device are transmitted to the server and then deleted from the device.

Field Name	Description
Only Transmit File (s) when	• The **Always Transmit** option will cause file(s) to be uploaded or downloaded regardless of whether or not the source and target are different or the same. • The **Files are different** option will cause file(s) to be uploaded or downloaded only if the source file is different from the destination file. • The **Source file is newer** option will cause file(s) to be uploaded or downloaded only if the source file has a more recent date-time stamp. • The **Destination file does not exist** option will cause file(s) will cause file(s) to be uploaded or downloaded only if the destination file does not exist.
Sync Sub-Folders	Synchronize files in sub-folders in addition to the files located in the target folder
Sync Online Devices Now	File synchronization will be executed immediately following the completion of the wizard for online devices.
Sync On Device Addition or Relocation	Perform file synchronization when a device is added or relocated to a device tree group for which this rule has been configured This setting is useful to easily invoke file synchronization when a device is moved from one group to another in the device tree.
Network Restriction	Restrict whether file synchronization should take place over cellular data networks (i.e. GPRS)
Upload File Name Format	Allows you to customize the names of the files that are uploaded from the devices For example, you can augment a file name with the date-time stamp of when it was uploaded. These are available file-name macros: • **%YYYY%** is for the year (e.g. 2006). • **%MM%** is for the month of year (e.g. 12 is December). • **%DD%** is for the day of month (e.g. 31). • **%H%** is for the hour in the 24-hour format (e.g. 14). • **%M%** is for the minutes (e.g. 30). • **%S%** is for the seconds (e.g. 55). • **%FILENAME%** is for the original file name (e.g. `mylogfile`). • **%EXTENSION%** is for the original file extension (e.g. `.txt`).
Use Common Cache Mode	The option to use the new, advanced caching mode of the files being disseminated is applicable only when syncing files from the server to the device. This option is set to **Yes** by default. When enabled, a single, shared, cached copy of each file being disseminated is stored on the Deployment Server. If you are experiencing issues with file synchronization, set this option to **No.**



File synchronization options

Click the **Scripts** button to configure file synchronization scripts.

File Synchronization Scripts

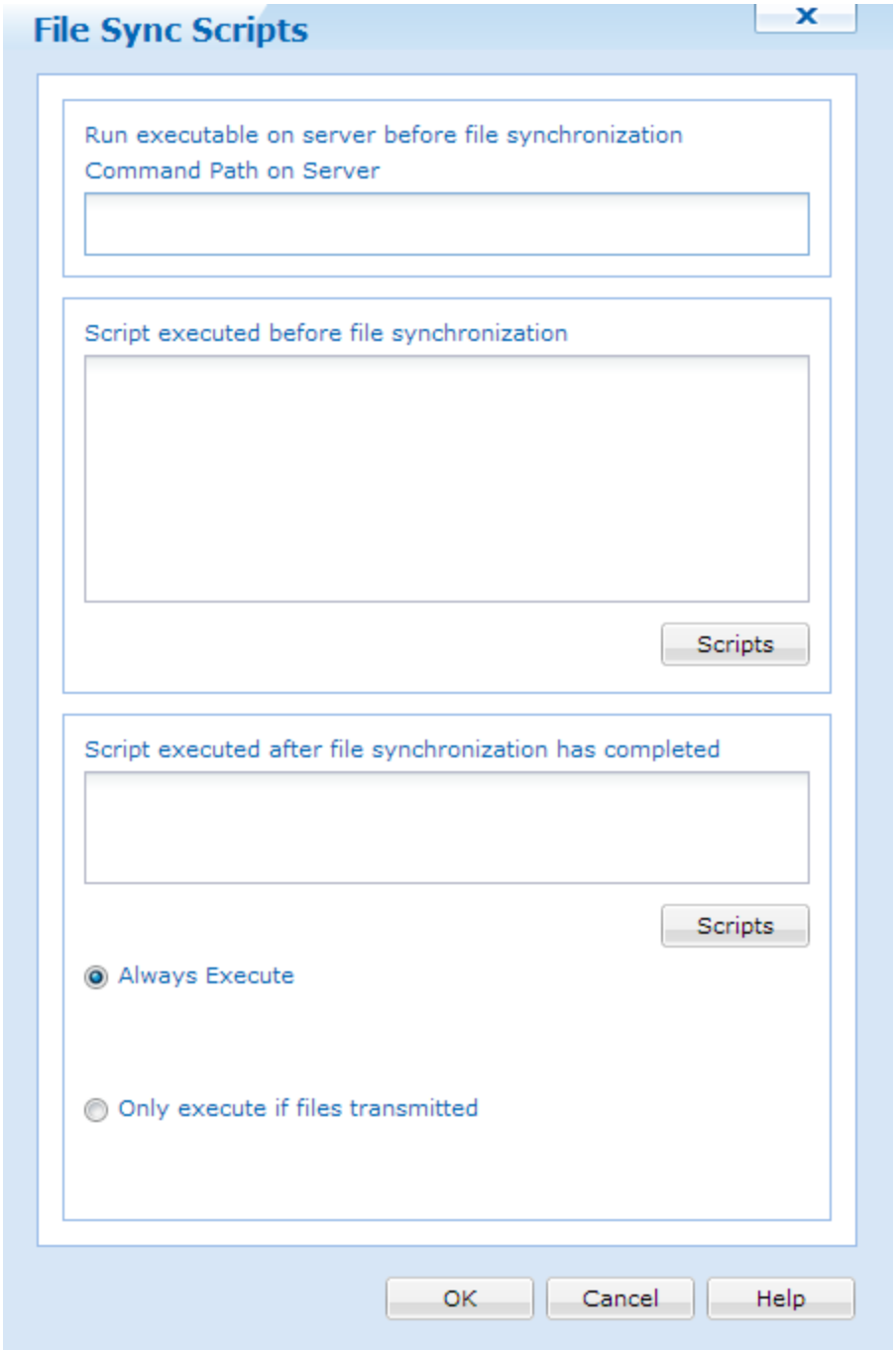
File synchronization scripts provide flexibility in automating actions on the server before the file sync or on the device pre or post file synchronization.

EXAMPLE: RUN EXECUTABLE ON SERVER

MobiControl contains plenty of server side utilities used to manage devices in the deployment server. One of these utilities is a device move. If this utility is ran before the file sync, we can ensure that all the devices are in the proper location before syncing the files down. For additional help with this utility and more, please contact us.

EXAMPLE: PRE AND POST FILE SYNC

Before collecting a log file from the device, stop a certain running process (e.g. `kill abc.exe`). After the file has been collected, restart the process (e.g. `start abc.exe`). Please see the "Script Command Set" topic on page 72 and the "Script Variables" topic on page 424.s



File synchronization advanced options

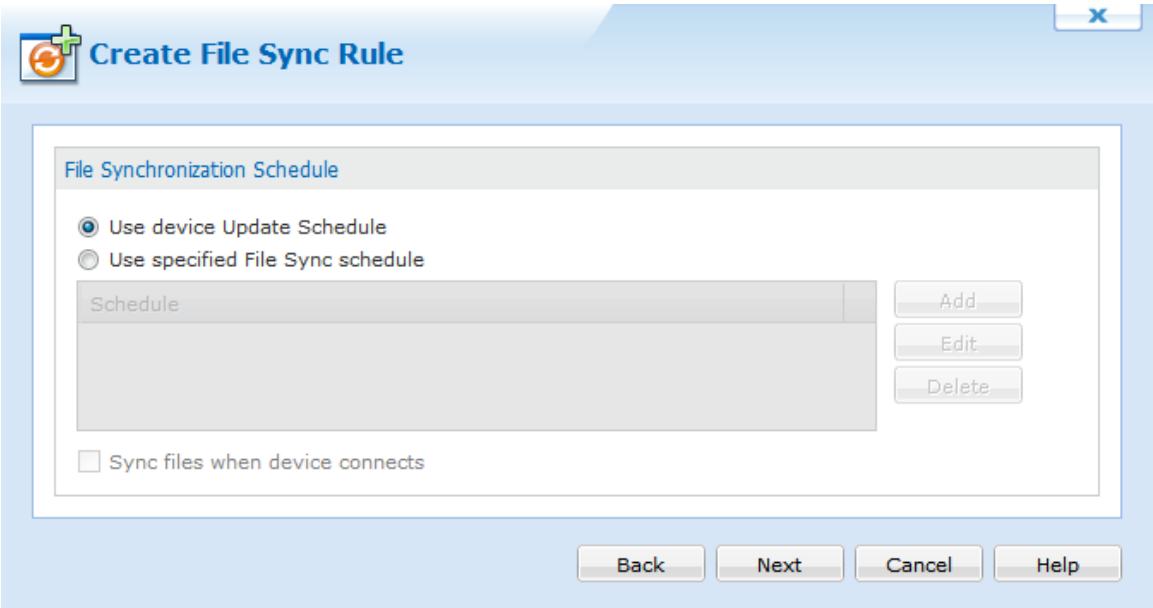
Field Name	Description
Always execute	Will execute the script every time there is a scheduled sync, even if the files are updated or not
Only execute if files transmitted	Will execute the script when files have been updated by the sync schedule
Scripts	Will allow you to import previously created scripts

File Synchronization Schedules

The file synchronization schedule specifies when the Deployment Server(s) should check device(s) for synchronization.

If the Deployment Server identifies an inconsistency, such as a mismatch in the file size or finds the new file, the Deployment Server will act according to the file sync rule.

By default, the device synchronization schedule, specified by the add devices rule used to add the devices to the system, is selected for file synchronization. You may add, edit or delete the custom schedule using the following dialog box.



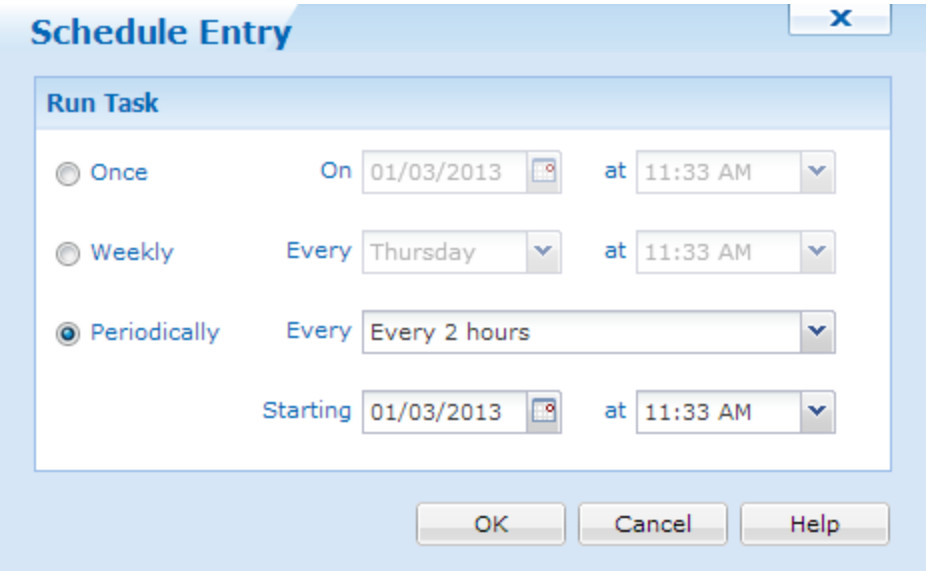
Create File Sync Rule Wizard dialog box

The following table describes the fields of the Create File Sync Rule Wizard dialog box.

Field Name	Description
Add	Specify your own file synchronization intervals. When you select **Add,** the **Schedule Entry** dialog box is displayed. **EXAMPLE:** To sync twice a week (Monday at 06:00 and Friday at 19:00), create two weekly schedule entries.
Edit	Select **Edit** to modify an existing schedule entry. The **Schedule Entry** dialog box is will be displayed.
Delete	Permanently remove a file sync schedule entry from the dialog box
Sync Files when device connects	Sync whenever devices under this rule connect to a Deployment Server (i.e. transition from offline to online)

Schedule Entry

The **Schedule Entry** dialog box allows you to specify schedule entries as one-time or periodic events.



Schedule Entry dialog box

Field Name	Description
Once	Device will check for file synchronization once at the specified date and time.
Weekly	Device will check for file synchronization once a week, on a specified day and time.
Periodically	Device will check for file synchronization periodically at the specified interval from the set, start date-time.

Creating Device Relocation Rules

Dynamic device relocation allows you to set up rules to move your mobile devices automatically between different virtual groups or device groups in the MobiControl device tree based on the IP address or other custom criteria. This is useful when managing mobile devices in a deployment where the device tree is set up to represent different physical locations (e.g. retail stores, warehouses, regional offices, etc.).

In a deployment that has mobile devices connecting from and moving frequently between several different sites, properties or regions, the administrator needs visibility over the movement of mobile devices across different locations. Dynamic device relocation allows the MobiControl device tree to be updated automatically when a device moves to a different location (e.g. a mobile device that has moved from a warehouse or site in Chicago to a site in New York will automatically be relocated in the device tree on reconnection and will appear in the device group for devices in New York based on the new IP address information). Additionally, the devices can also be automatically reconfigured and any modifications to the mobile device settings, specific to the new location, will be sent to the device automatically.

The devices are relocated based on the IP address ranges specified for each location. You can also create a custom data identifier which can be the criterion that will be utilized to relocate the devices to the appropriate device group. (Please see the "Windows Mobile Custom Data" topic on page 700 for detailed information on custom data identifiers.)

1. Start the wizard.

   From MobiControl Manager, select the Rules view (tab), then click **Rule,** select **Create Rule,** and click **Create Device Relocation Rule.** The first page of the Create Device Relocation Rule Wizard will be displayed. Enter a meaningful name for the rule and click **Next** to continue.

Create Device Relocation Rule Wizard startup dialog box

2. Review the device relocation mappings.

This page lists **device relocation mappings** that determine how the devices would be relocated and in which groups they would appear if the specified criteria is met. When a device connects to the MobiControl Deployment Server, its IP address and custom data information will be checked against all device relocation rules configured, and it will be moved to the appropriate device group based on the information in the relocation mappings.

NOTE:

Devices that are already connected and online in MobiControl will be relocated when they disconnect and re-connect to the MobiControl Deployment Server.

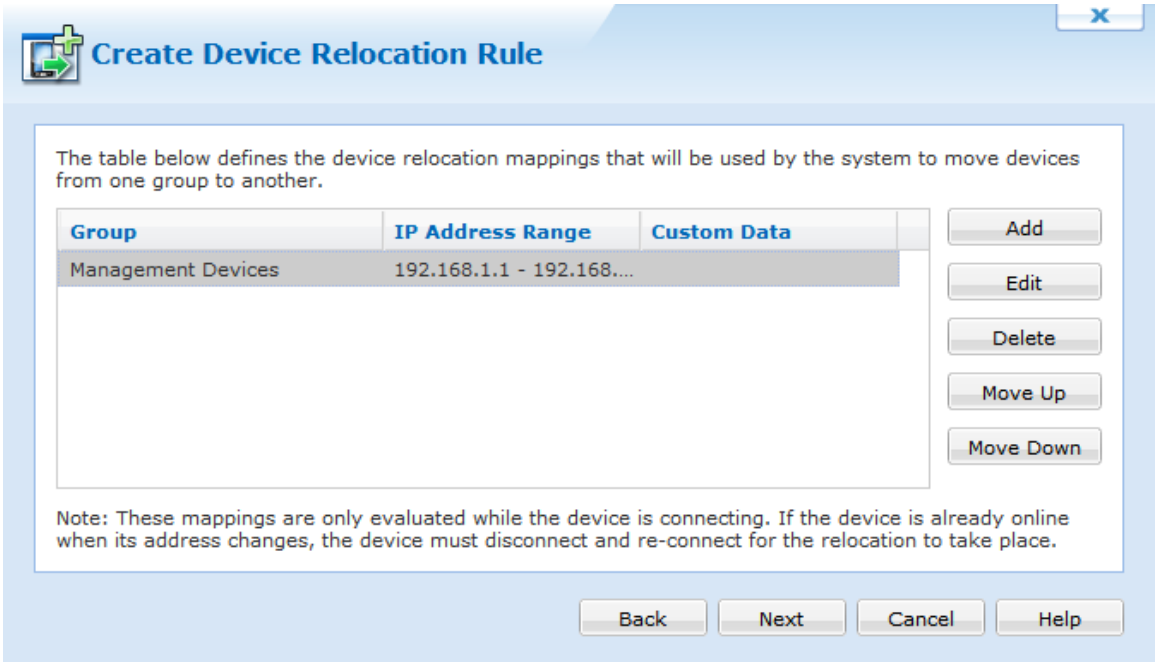
Edit Device Relocation Rule dialog box

The buttons on the **Edit Device Relocation Rule** dialog box are explained below:

Button Name	Description
Add	Click the **Add** button to add an entry for the relocation mapping.
Edit	Click the **Edit** button to change the settings for an existing relocation mapping entry.
Delete	Click the **Delete** button to delete a relocation mapping entry.
Move Up / Move Down	Click these buttons to change the order of the relocation mappings. The entry listed higher in the list have a higher priority and take precedence over entries listed lower in the list. For more details, read about relocation mappings priority below.

A relocation mapping can use just the IP address or the custom data entry to specify the relocation rule for mobile devices. If a relocation mapping has both the IP address and custom data entry specified as the criteria, the mobile devices would be relocated only if both these conditions are satisfied. If a device is affected by more than one relocation mapping, the one

higher in the list of mappings will have a higher priority and will be effective. You can use the **Move Up** and **Move Down** buttons to change the precedence of the relocation mappings if multiple mappings apply to a device.

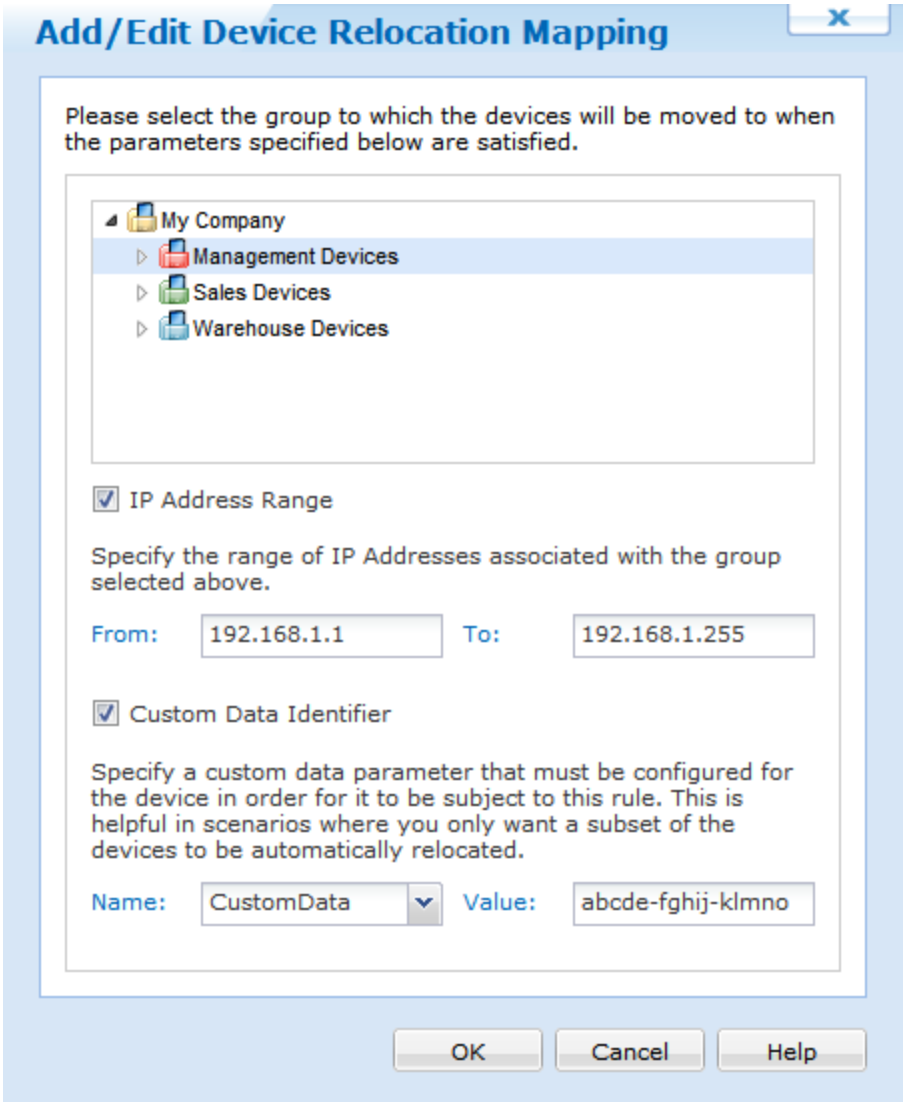


Device Relocation Mappings dialog box

The first two relocation mappings in the previous screenshot have been defined: one is for relocating all devices with IP addresses between 192.168.1.1 and 192.168.1.255 to the Management Devices group and another mapping for relocating all the devices for which the custom data item "Location" has a value of "Region A" to the Warehouses group. Since the relocation mapping with the IP address filter is listed above the mapping with the custom data filter, the IP address mapping will take precedence. If a device satisfies both conditions (e.g. has an IP address 192.168.1.10 and a value "Region A" for "Location"), it will be relocated to the Management Devices group.

3. Add or edit device relocation mappings.

   A relocation mapping includes the target or destination group (which can be a virtual group) to which the devices would be relocated. It also includes the conditions or the relocation parameters that must be satisfied for a device to be relocated.



Add/Edit Device Relocation Mapping dialog box

The **target group** is the group, sub-group, or virtual group to which devices will automatically be relocated when connecting to the Deployment Server if the conditions specified in the relocation parameters are met.

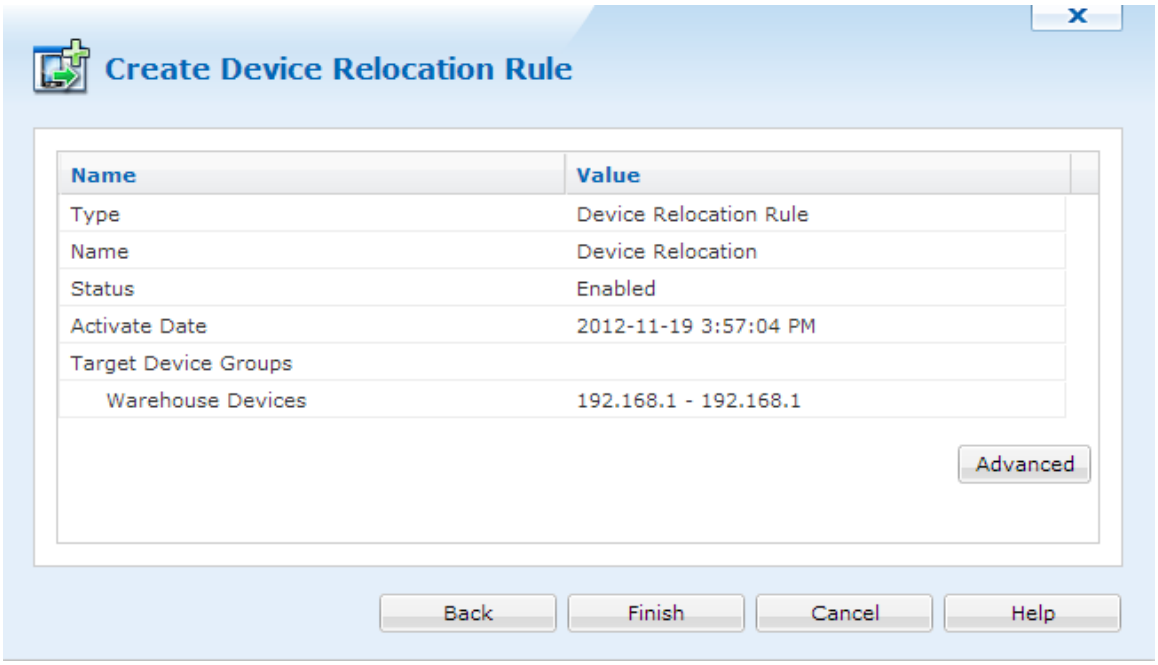
Multiple **relocation parameters** can be specified to manage the dynamic relocation of devices. A single parameter can be specified or both parameters can be used for a relocation mapping, in which case the device will be relocated if it satisfies both parameters.

The following table describes the fields of the **Add/Edit Device Relocation Mapping** dialog box:

Field Name	Description
IP Address Range	Devices can be automatically relocated based on the IP address information of the device at the time it connects to a Deployment Server. A range of IP addresses can be specified and if the device's IP is within that range, the device will be relocated to the target group.
Custom Data Identifier	You can use a custom data value as one of the criteria for relocating devices from one device group to another. MobiControl allows you to retrieve arbitrary data from the device's registry, files on the device and other sources using custom data. Please see the "Windows Mobile Custom Data" topic on page 700 for more information.

4. Review the summarized settings.

   This page gives you an opportunity to review the settings of the device relocation rule before committing them to the database. If you wish to make any corrections, click the **Back** button, otherwise click **Finish** to complete the wizard.



Edit Device Relocation Rule Summary dialog box

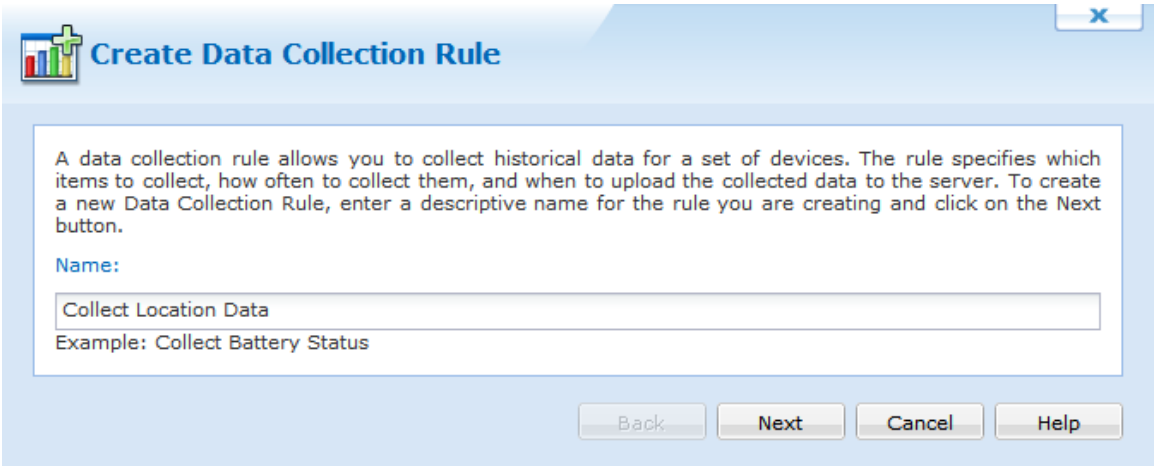
Windows Mobile Data Collection

Data collection rules allow administrators to automatically collect a variety of data from mobile device(s).

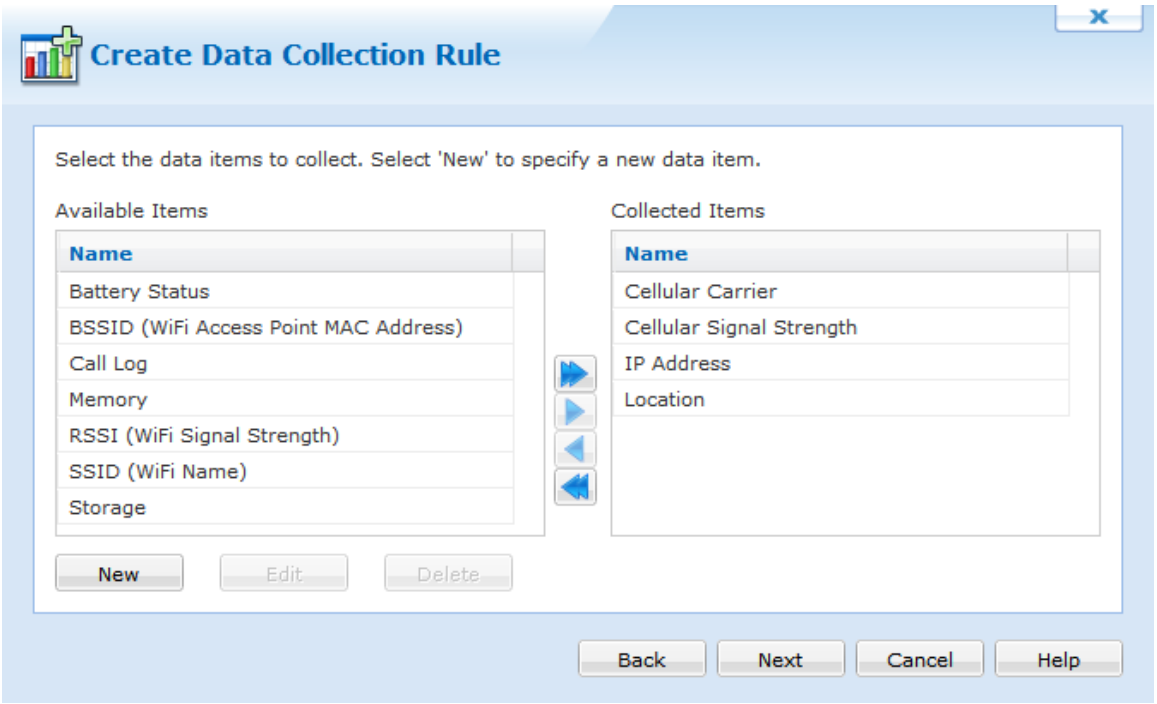
The following series of steps describes how to use the Create Data Collection Rule Wizard to create a data collection rule:

1. Start the wizard.

   From MobiControl Manager, select the Rules view (tab), then click **Rule,** click **Create Rule,** and click **Data Collection Rule**. Enter a meaningful name for your new data collection rule and then click **Next**.



2. Select data items to collect.



   Select individual items or all items from the **Available Items** list by highlighting and then select the corresponding direction arrow(s). These items will move to the **Collected Items** list. If you have added something that you would like to remove from the **Collected Items** list, simply select the

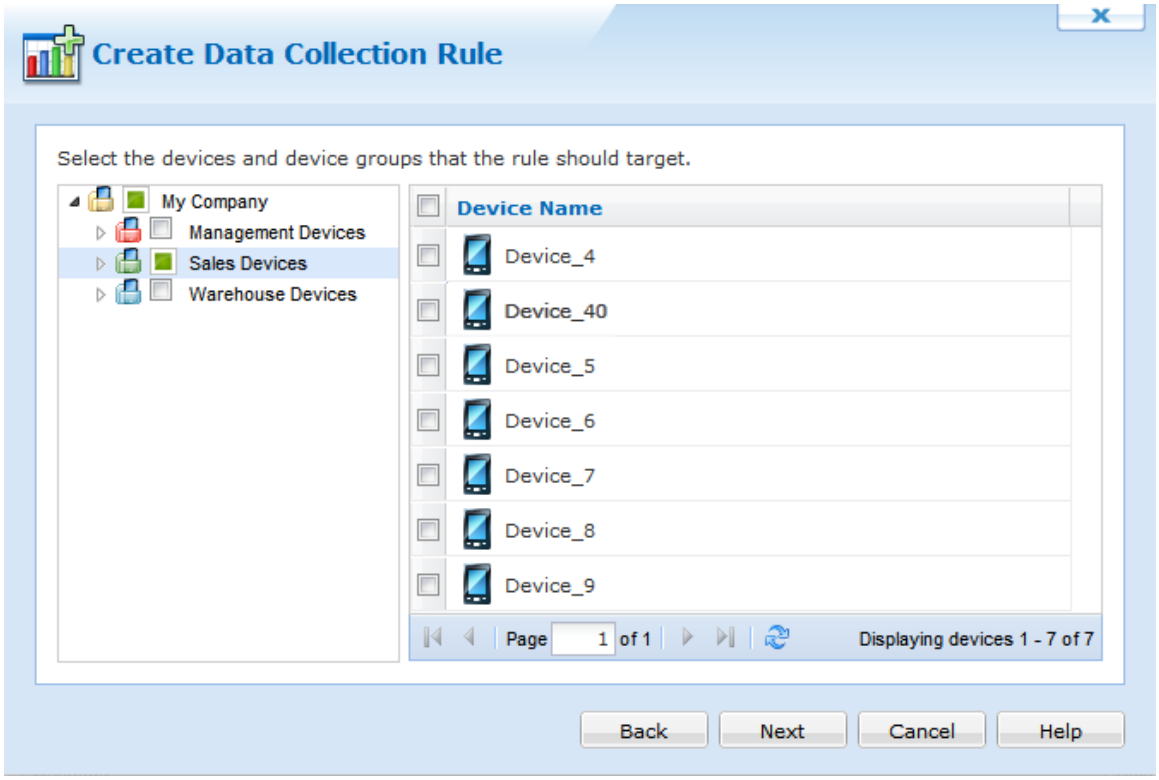
item and then click the direction arrow(s) to place the item(s) back into the **Available Items** list.

Item Name	Description
Available Memory	Shows the collected data is the combination of device memory, storage memory and virtual memory on the device
Available Storage	Shows the amount of room that is left on the main memory of the device
Battery Status	Shows what percent the battery was at the time the data collection rule ran
Call Log	Shows the incoming, outgoing and missed calls with call duration
Cellular Carrier	Shows what carrier the device is connected to at the time the data collection rule ran
Cellular Signal Strength	Shows what the signal strength is of the device at the time the data collection rule ran
IP Address	Shows the IP address of the device at the time the data collection rule ran
Location	Shows the GPS latitude, longitude, speed and heading
SSID	Shows the SSID that your device is currently connected to
Wi-Fi Signal Strength	Shows the signal strength of a wireless connection. A value of 0 is collected when there is no Signal listed in Manager

After selecting the choice(s), click the **Next** button.

3. Select devices.

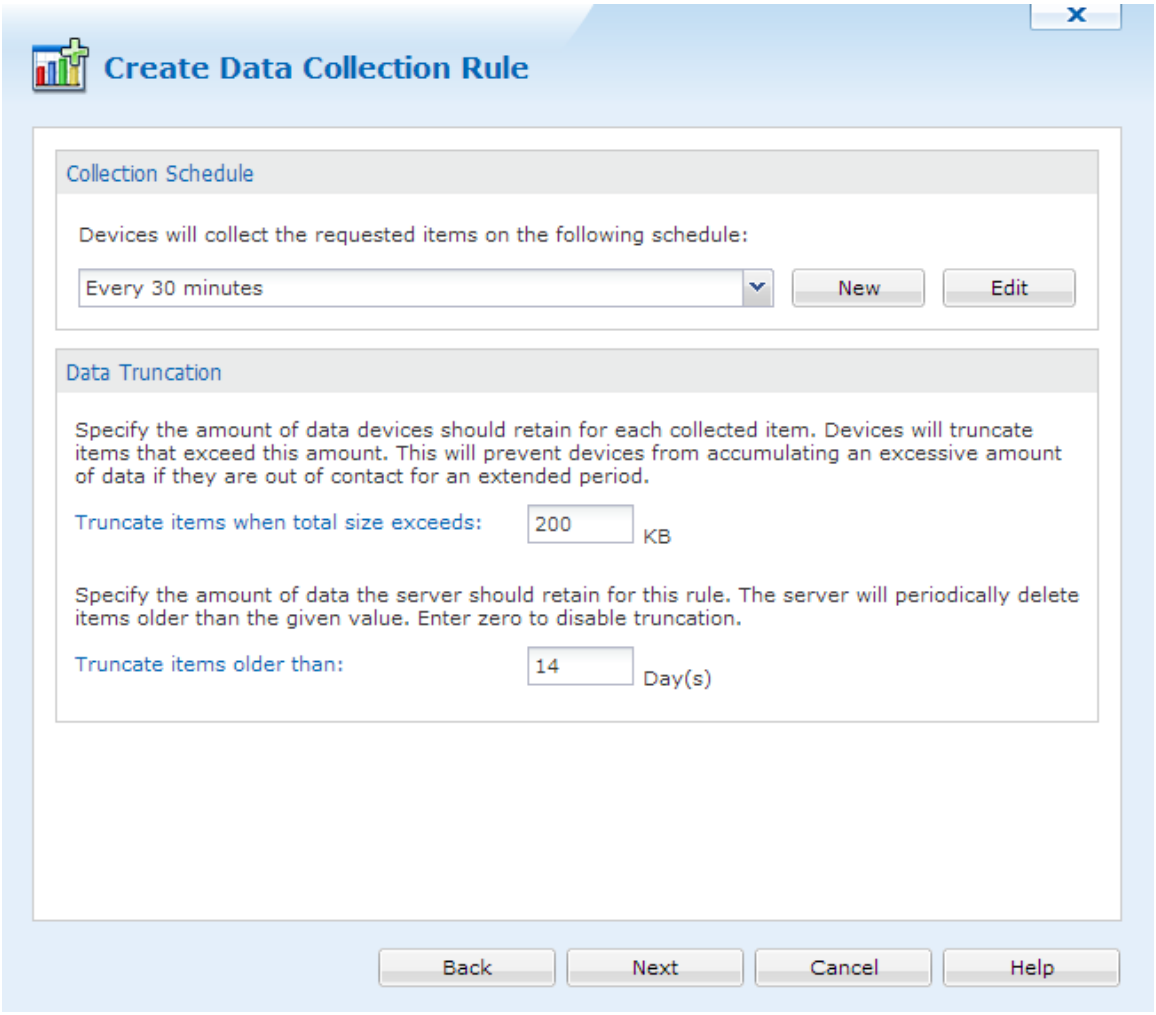
   Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.

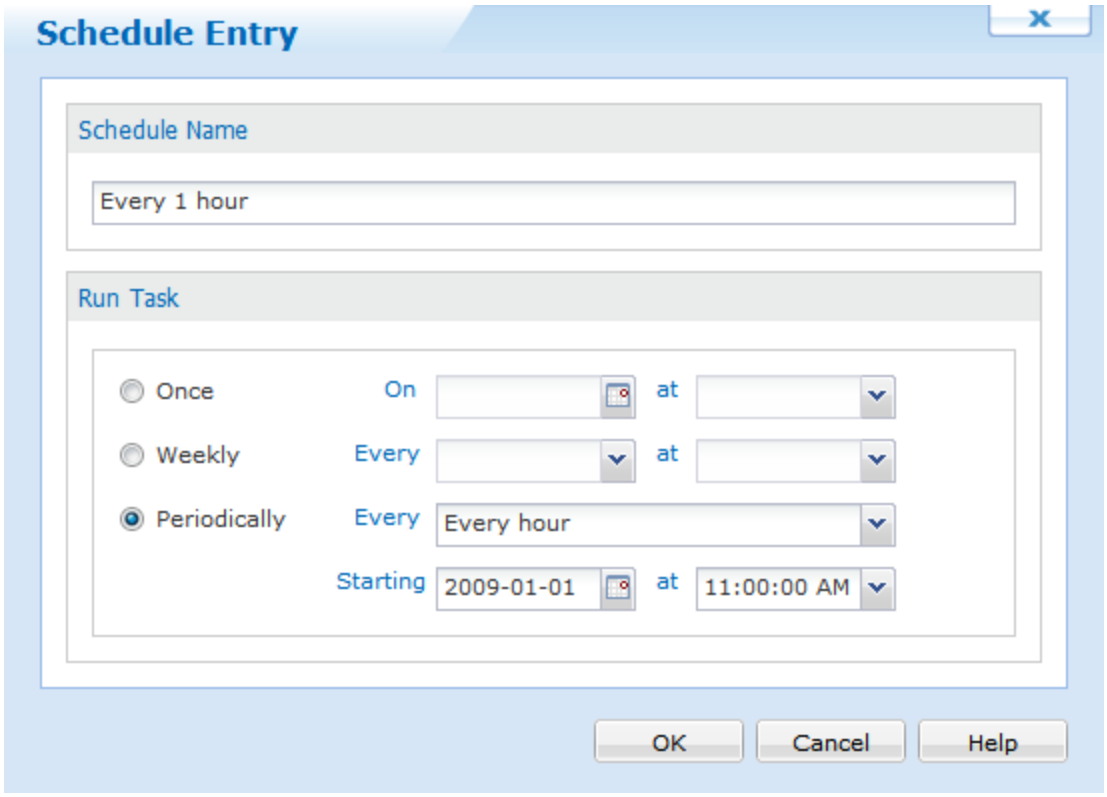


4. Configure data collection rule schedule and optional settings.

   Select the time interval the devices will collect the data and choose the size of the data being collected. This helps control memory used on the device and the number of days you would like to retain the data in the database.

   To set up a new schedule, click New.




Schedule Entry
Schedule Name
Every 1 hour
Run Task
Once
On
at
Weekly
Every
at
Periodically
Every
Every hour
Starting
2009-01-01
at
11:00:00 AM
OK
Cancel
Help

Section Name	Description
Collection Schedule	This option enables you to create a custom data collection schedule with a custom date and time. Select the **New** button to create the new schedule. This will open up the second dialog box above. If you already have a previously created schedule, you can select edit to open the second dialog box above.
Schedule Name	Enter a meaningful schedule name that will be used to identify your custom schedule(s).
Run Task	Select the frequency for which you want to initiate the data collection on your device(s).
Delivery Schedule	This option will deliver the data collected from the device to the Deployment Serverbased upon the set update schedule. Currently, this option uses device schedule as the delivery schedule and is not configurable.

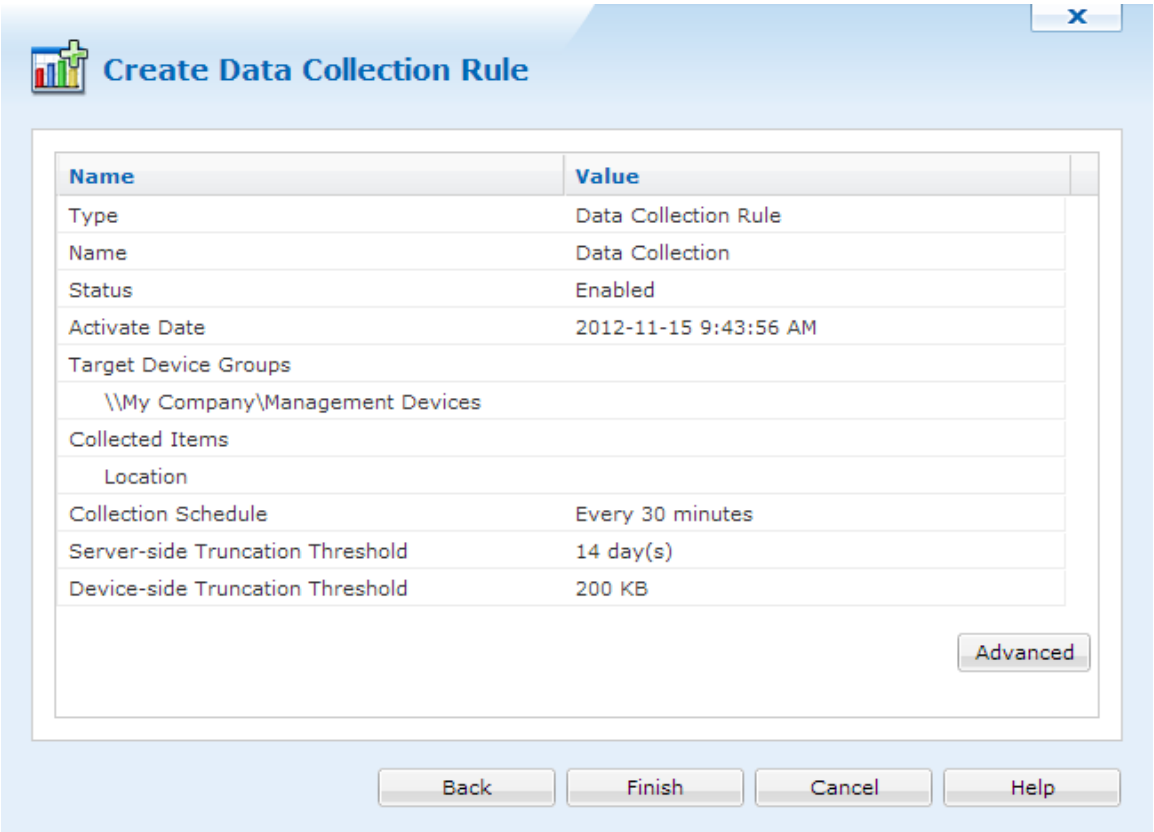
Section Name	Description
Device-Side Data Truncation	Specify the maximum size of data to be stored from the data collection ruleon the device(s).
Database Data Truncation	Specify the number of day(s) that you would like to retain the information in your database. Data collected older than the number of days listed will be deleted from the database

NOTE:

Creating a frequent collection schedule may affect the device's battery life. Also, frequent data collection can be managed with the truncation options available. This will help control how much data is kept on the device and in the database.

After entering your choice(s) in the above dialog box, click the **Next** button.

5. Review the summarized information.



The data collection rule can be deployed real-time or at a pre-set time. The data collection rule, although set to be activated at a scheduled time, can also be set to be deactivated. The deactivation setting is optional.

Click **Finish** to complete the wizard.

Windows Mobile Alert Rules

Alert Rules allow Administrators to be notified when events of interest arise on the system. This notification system allows Administrators to quickly and effortlessly communicate an event message to large groups of people via email, and notifies users via the MobiControl Manager Alert popup window. For every type of scenario, whether it is a Rule Change or a Device Error, the system will rapidly deliver your message to a designated audience.

To create an Alert Rule, select the Rules view (tab) within MobiControl Manager, then click the **Rule** menu, select **Create Rule**, and click **Alert Rule**. The Create Alert Rule Wizard will be displayed.

NOTE:

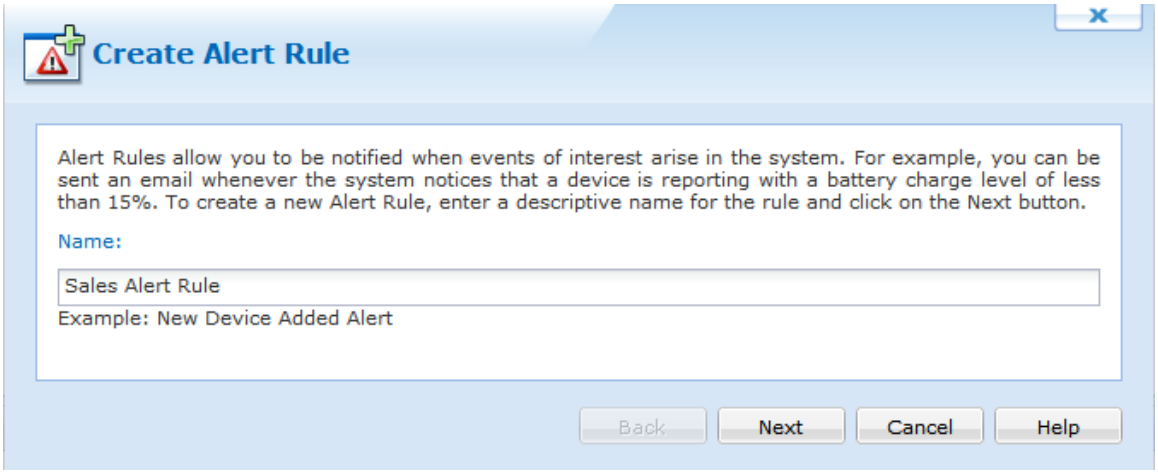
The Deployment Server must be online in order for Alerts to be generated and sent out.

The steps below describe how the Create Alert Rule Wizard can be used to create an add devices rule:

1. Start the wizard

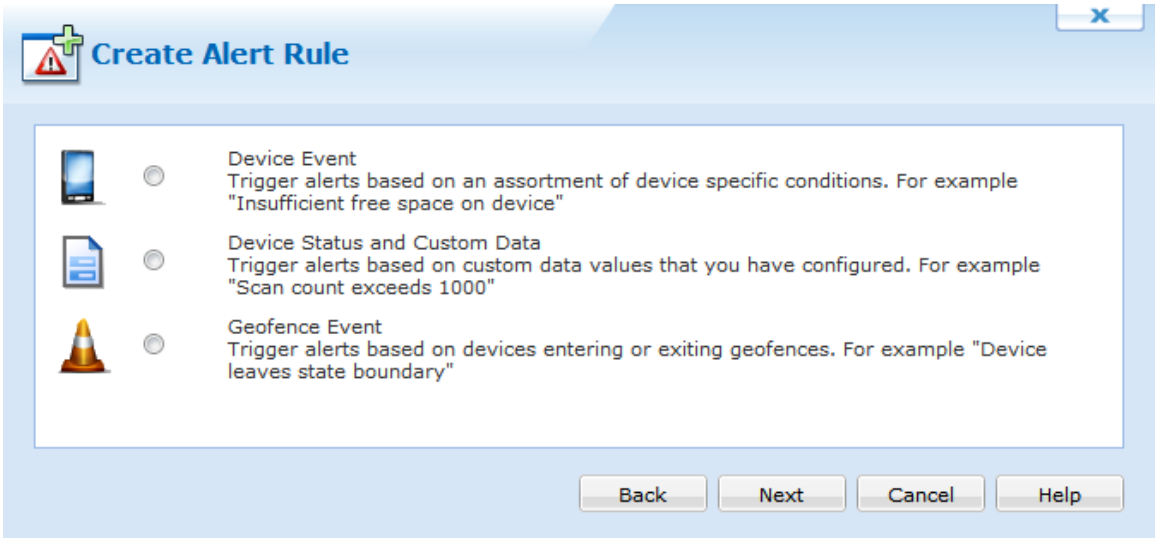
   Select the Rules view (tab), then click the **Rule** menu, select **Create Rule**, and click **Alert Rule**. The first page of the Create Alert Rule Wizard will be displayed.

   Enter a descriptive name for the Alert Rule you are creating and click **Next.**



First page of the Alert Rule Wizard

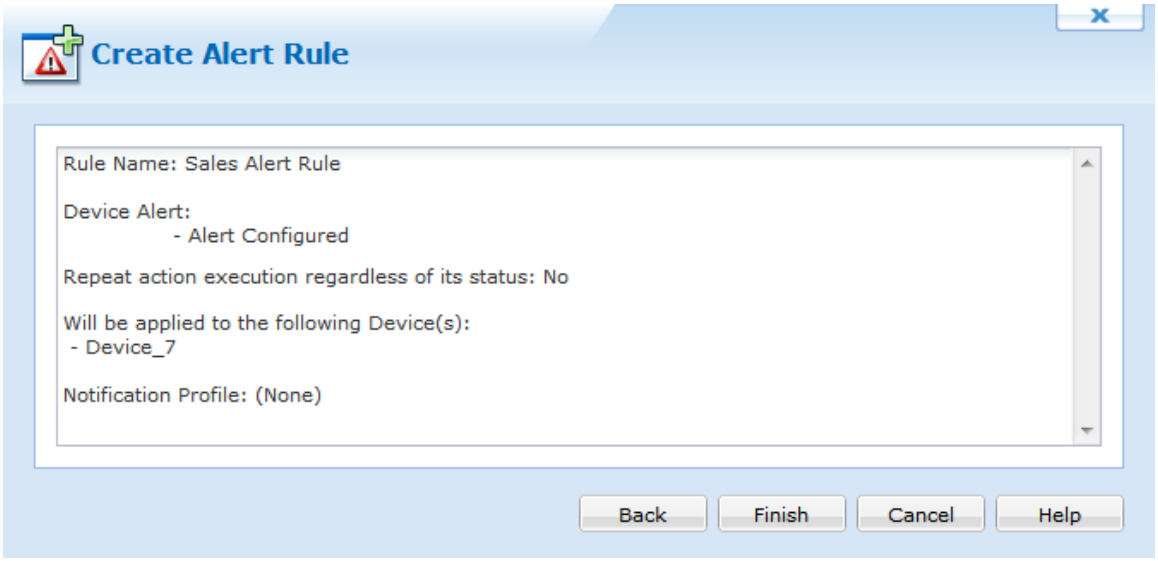
2. Select the Alert Rule Type.



Select the Alert Rule Type and click Next.

Type	Description
Device Event	Trigger alerts based on an assortment of device specific conditions.
Device Status and Custom Data	Trigger alerts based on Custom Data vales that you have configured.
Geofence Event	Trigger alerts based on devices entering or exiting geofenced areas.

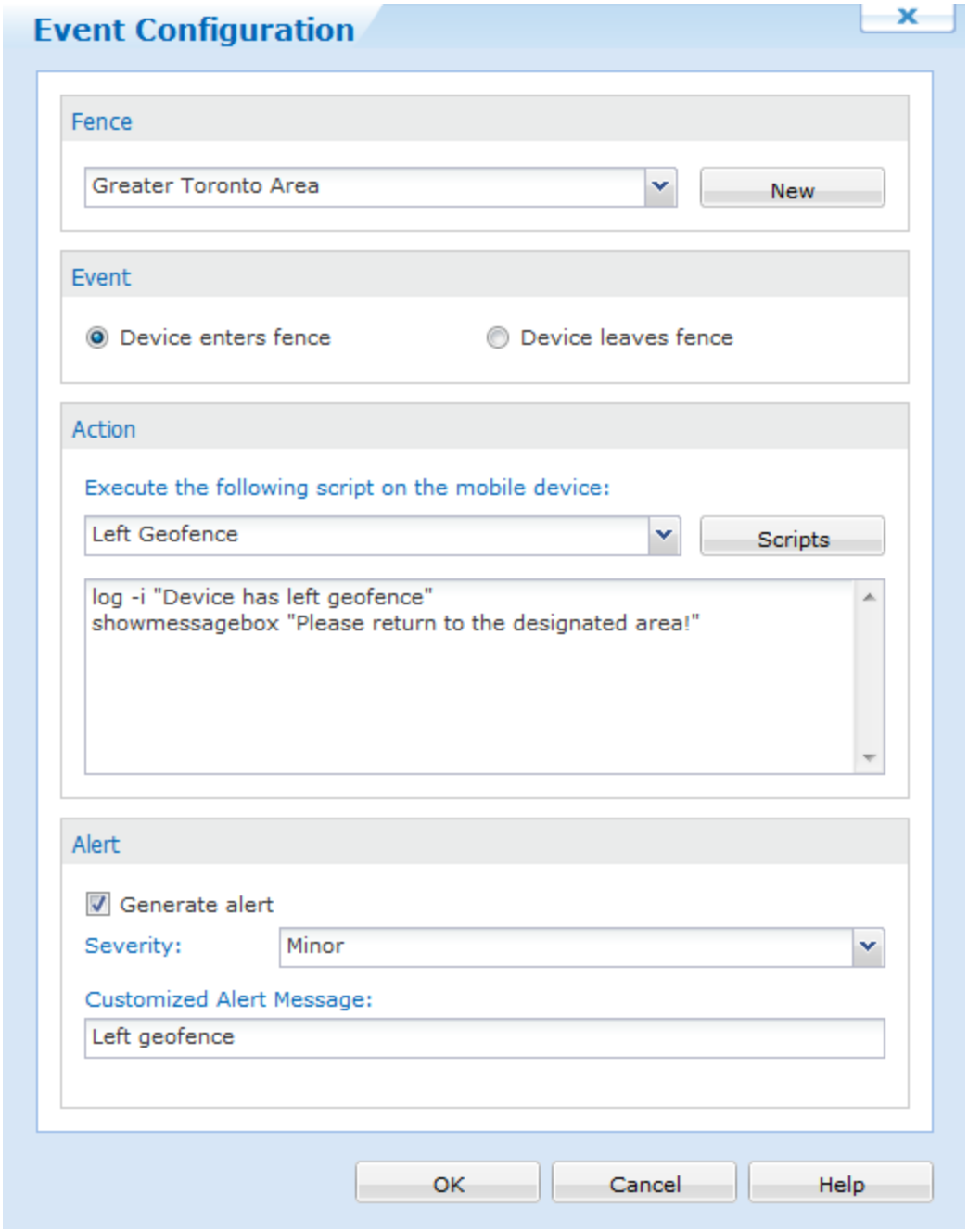
3. Review the summarized information.



Click **Finish** to complete the wizard.

Geofence Event

A Geofence Event is an alert trigger based on a GPS enabled device entering or leaving a Geofenced area defined by you. In order to create a Geofence event, you need to create an Alert Rule with a Type of Geofence Event.



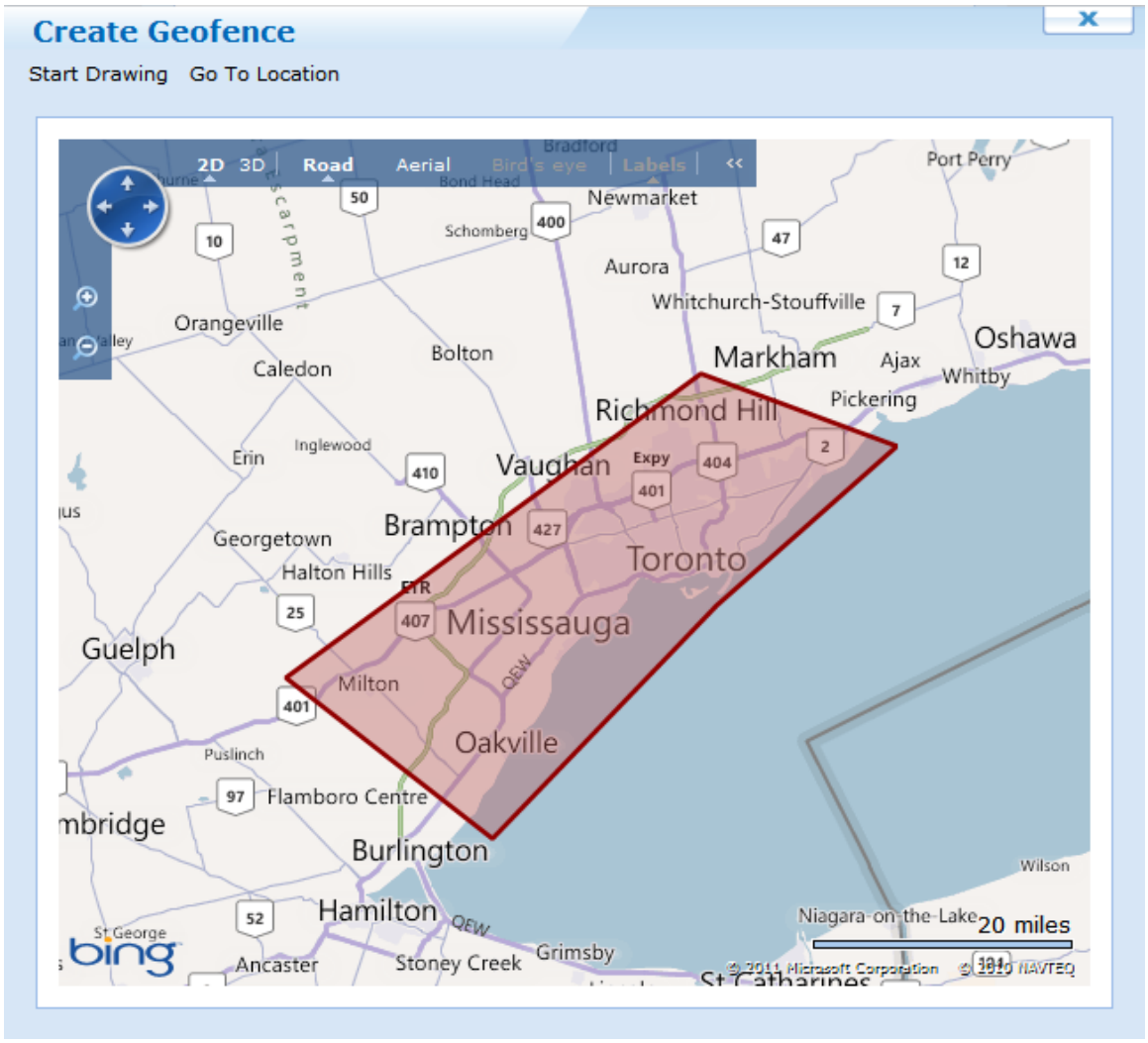
The **Fence** section allows you to create a geofence by clicking on the New button in the dialog box.

The **Event** section allows you to configure whether this event should be triggered on entry or exit of a fence.

The **Action** section allows you to configure what script you want to run on the mobile device when the event is triggered. This is optional, but you have for example the ability to run an Activate Connection, Log Event, Show Message or even wipe the device completely.

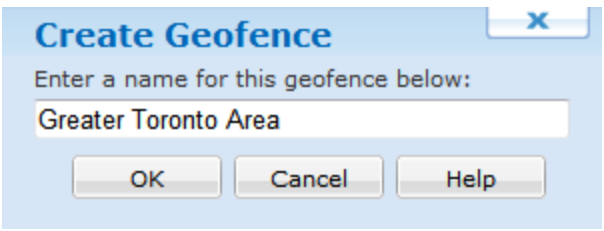
The **Alert** section allows you the option to Generate an alert, configuring its Severity (Minor, Serious and Critical) and add a Customized Alert Message, such as "Entered geofence".

When you click on the **New** button in the **Fence** section, the following Geofence Creation dialog box appears:



The two options available are to Start Drawing and Go to Location.

The **Start Drawing** option allows you to begin drawing on the map below the button. The area drawn on the map will be defined as the Geofence. The defined area must be a complete geometric shape, which means the Start Drawing point will be the same as the End Drawing point. When you have completed a proper geometric shape you be asked to name your geofenced area.



Prior to selecting the Start Drawing button, you have the ability to use the view control buttons in the map in order to move to a desired location, zoom in and out, switch to 3D, Road, Aerial and Bird's eye views among the many options. This allows you ease to create an appropriate view for your geofence.

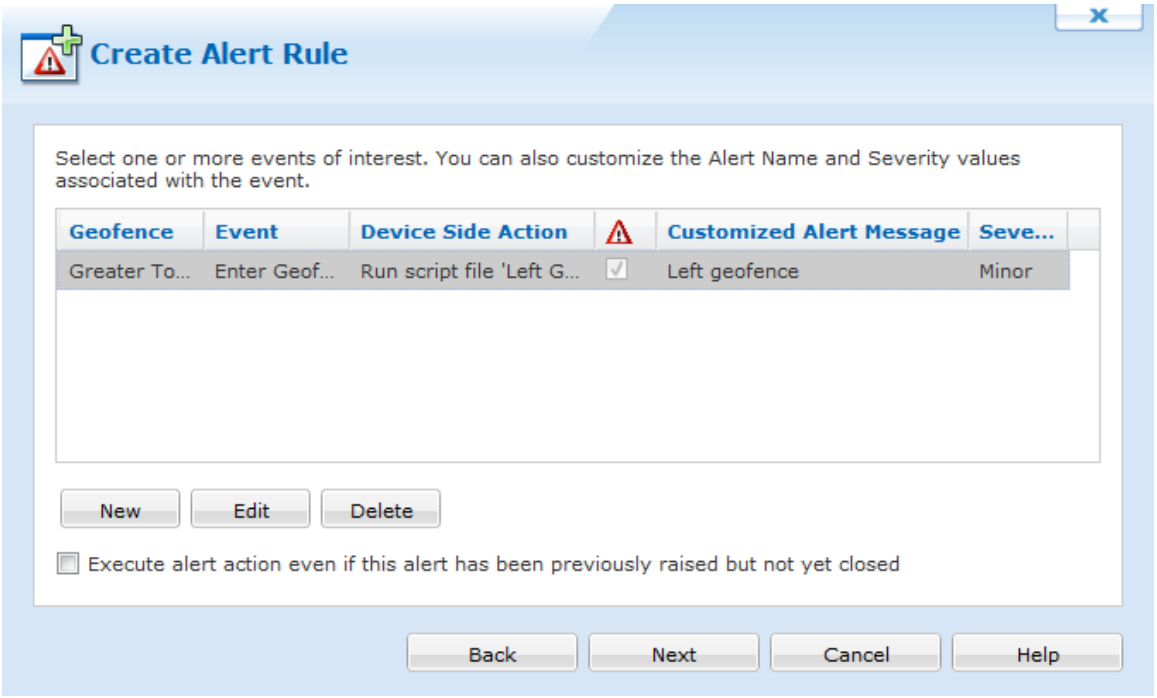
Alternatively to identify the appropriate view of the map, you can click on **Go to Location** which will allow you to specify a street address, location, landmark, or an existing geofence.

EXAMPLE:

- 350 Fifth Avenue, New York City
- Rome
- SFO (San Francisco International Airport)

Once you have the appropriate view displayed, you can click on Start Drawing and you are now able to create a fence. The first click of the mouse is first point of the fence. In order to complete the fence, you must have at least 3 distinct points selected on the map. In order to complete your fence, the last point must end off at the first point so it completes the closure of the fence. Once the last point is selected, a pop-up requesting the name of the geofence is shown. Here you should enter a meaningful name for that specific geofence in case you would like to use it again.

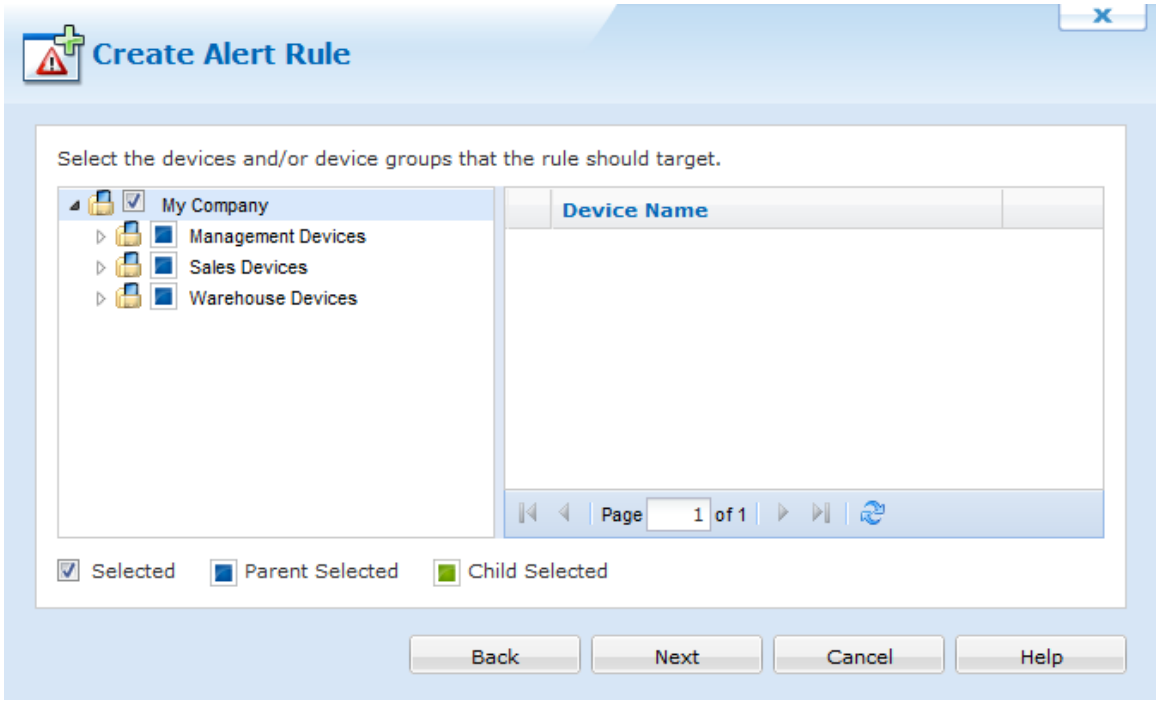
Select Geofence



Once the event is configured it will display as shown in the above diagram. Here you have the ability to create new events, edit existing events or delete events. Also, on this dialog box, there is a checkbox at the bottom allowing you to determine whether or not you want to Execute alert action even if this alert has been previously raised but not yet closed.

Select Devices

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



Select Power Policy

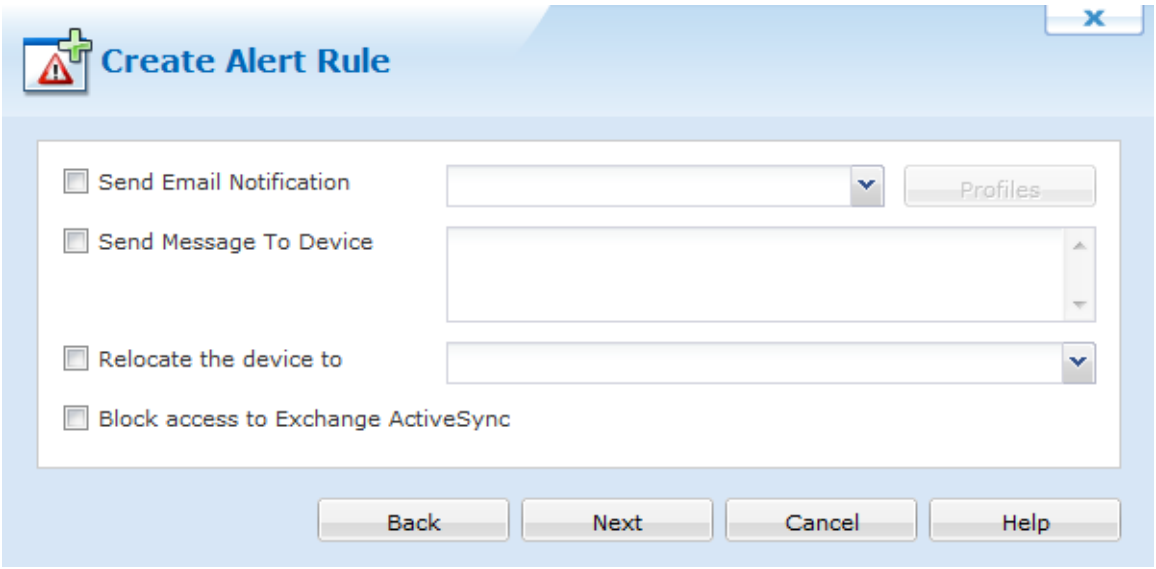
Clicking Next moves you to the Power Policy section as seen below.

The options available for the Power Policy are Continuous and Periodic.

Power Policy	Description
Continuous	This indicates the GPS radio is always on and the location will be monitored in real time. It is best to use this option with devices that have an external power source or are vehicle mounted because this option takes up a lot more power.
Periodic	This will turn on the radio based on a schedule that you define. Based on your business requirements, this can be as responsive as every 2 minutes, or every weekday all the way up to every year. It is best to use this option when you have battery powered devices in order to minimize the amount of power consumed with having this feature on.

Notification Profile Settings

Once the Alert Rule is selected, you must select your Notification Profile.

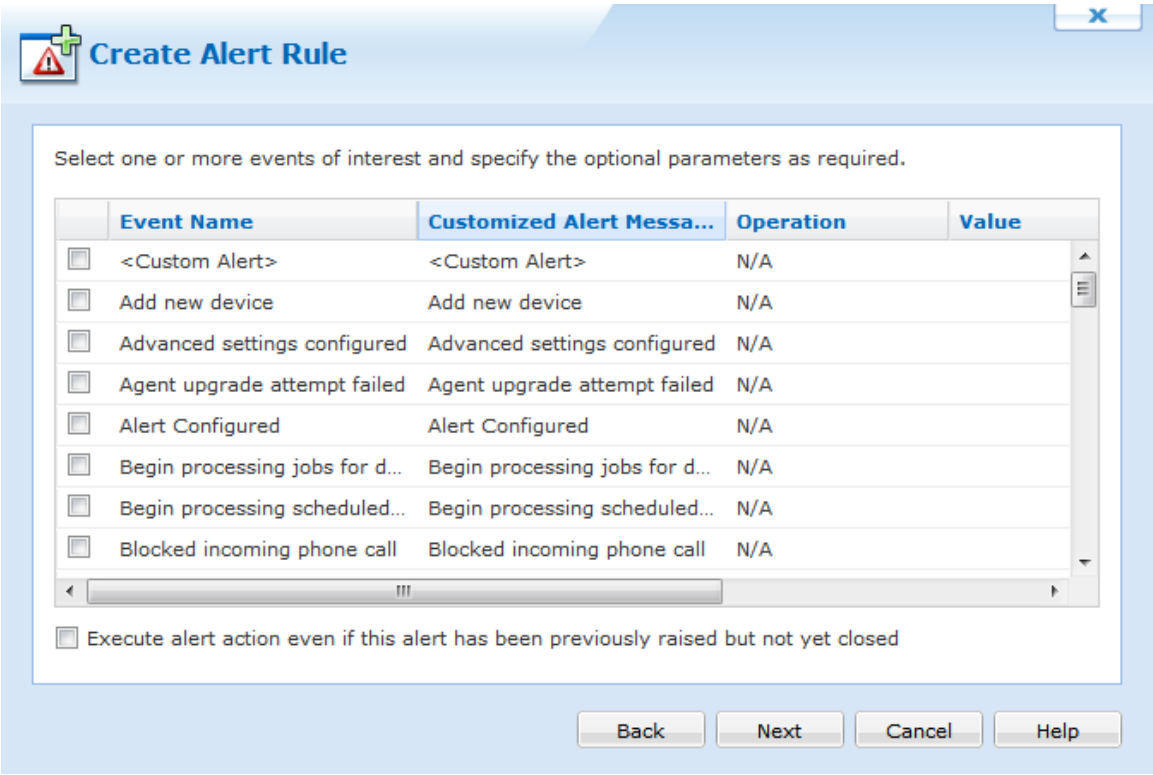


Select an existing notification profile, or click New to create a new Notification Profile. For assistance with notification profiles click here. Once you have selected your notification profile click Next.

Click Next and continue the Alert Rule Wizard here.

Device Event

A Device Event is an alert triggered based on an assortment of device specific conditions. See below for a full list.



Device Event Notification Selection Window

Severity is set to Minor by default and can be altered.

The below table shows all available default Device events:

Log Event	**Alert Message (Customizable)**
<Custom Alert>	<Custom Alert>
Add new device	Add new device
Advanced settings configured	Advanced settings configured
Agent upgrade Attempt failed	Agent upgrade attempt failed
Alert Configured	Alert Configured
Begin processing jobs for device	Begin processing jobs for device
Begin processing scheduled jobs	Begin processing scheduled jobs
Blocked incoming phone call	Blocked outgoing phone call
Change password failure	Change password failure
Change password success	Change password success
Custom Data configured	Custom Data configured
Custom log	Custom log

Log Event	Alert Message (Customizable)
Data Collected	Data Collected
Data Collection configured	Data Collection configured
Dependent packages not installed	Dependent packages not installed
Device connected	Device connected
Device disabled	Device disabled
Device disconnected	Device disconnected
Device Enabled	Device Enabled
Device has not been connected for %VALUE% minutes	Device has not been connected for %VALUE% minutes **NOTE:** *%DAYS% and %HOURS% can be used in place of %VALUE%.*
Device Manually relocated	Device Manually relocated
Device relocated	Device relocated
Device security configured	Device security configured
Error creating file on device	Error creating file on device
Error message received from device	Error message received from device
Error receiving file	Error receiving file
Error sending file	Error sending file
Error sending message	Error sending message
Error writing to file on device	Error writing to file on device
Exchange ActiveSync configured	Exchange ActiveSync configured
File synchronization failed	File synchronization failed
File synchronization was aborted by pre-sync script	File synchronization was aborted by pre-sync script
File(s) synchronized	File(s) synchronized
File synchronization was aborted by pre-sync script	File synchronization was aborted by pre-sync script
File synchronization failed	File synchronization failed
Geofencing Configured	Geofencing Configured
Inaccurate device date-time detected	Inaccurate device date-time detected
Incompatible platform, processor or OS version	Incompatible platform, processor or OS version
Installation aborted by user	Installation aborted by user
Installation was aborted by install script	Installation was aborted by install script

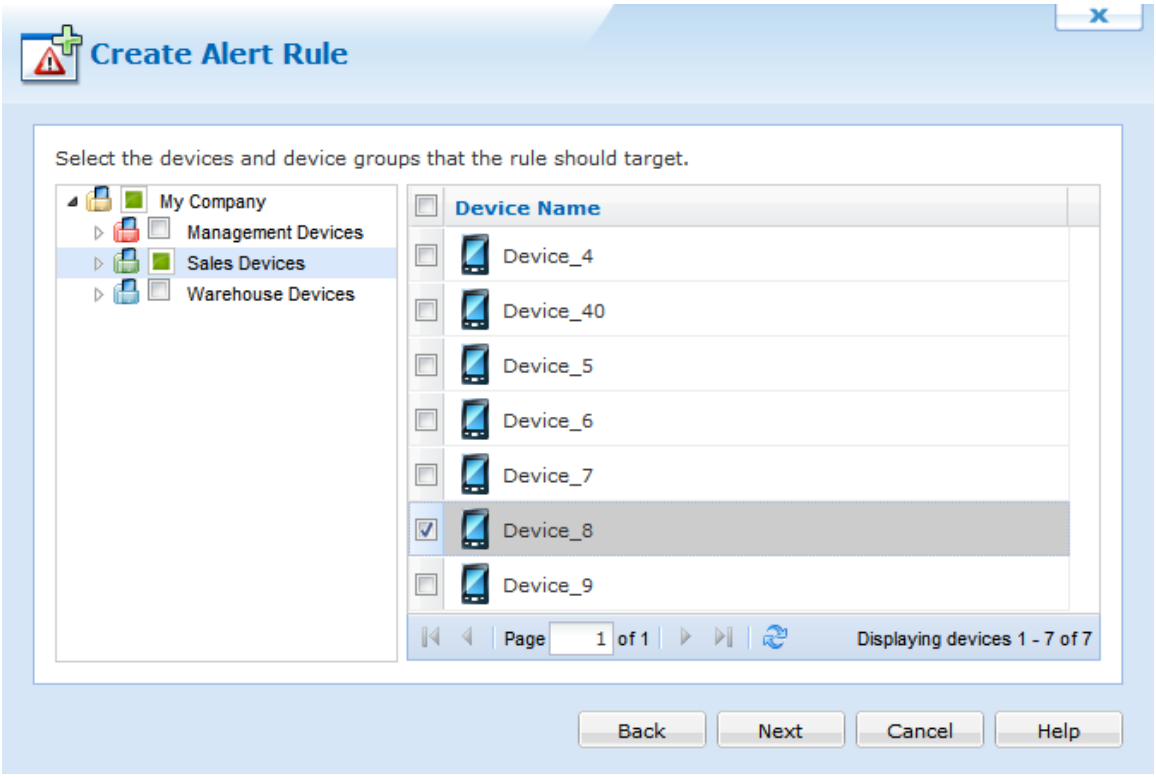
Log Event	Alert Message (Customizable)
Insufficient free space on device	Insufficient free space on device
Invalid device software version	Invalid device software version
Invalid message received from device	Invalid message received from device
Lockdown removed	Lockdown removed
Logon failure	Logon failure
Logon success	Logon success
Multiple packages with the same name in job list	Multiple packages with the same name in job list
No Package ID in installation report	No Package ID in installation report
Package file is corrupted	Package file is corrupted
Package file not found	Package file not found
Package uninstalled	Package uninstalled
Package with higher version number already installed on the device	Package with higher version number already installed on the device
Pending jobs cannot be processed until device user is authenticated	Pending jobs cannot be processed until device user is authenticated
Process Learned	Process Learned
Processed successfully	Processed successfully
Remote Control	Remote Control
Stopped illegal process	Stopped illegal process
Time Sync Configured	Time Sync Configured

The following list of variables are only available within the Customized Alert Message field:

Type	Description
%RULENAME%	The name of the rule
%PACKAGENAME%	The name of the package

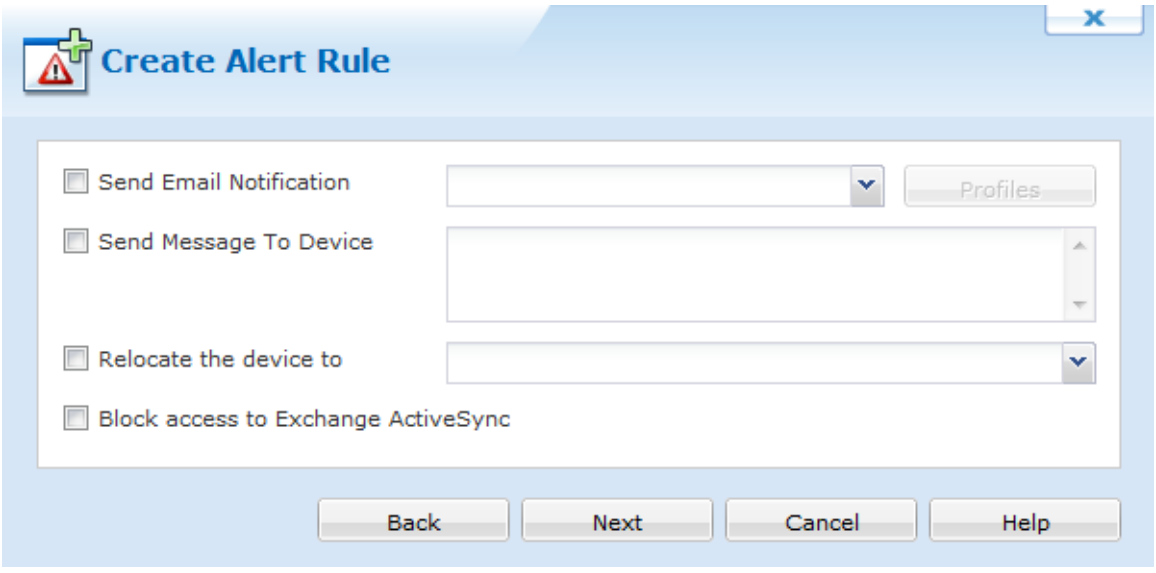
Select devices.

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



Notification Profile Settings

Once the Alert Rule is selected, you must select your Notification Profile.

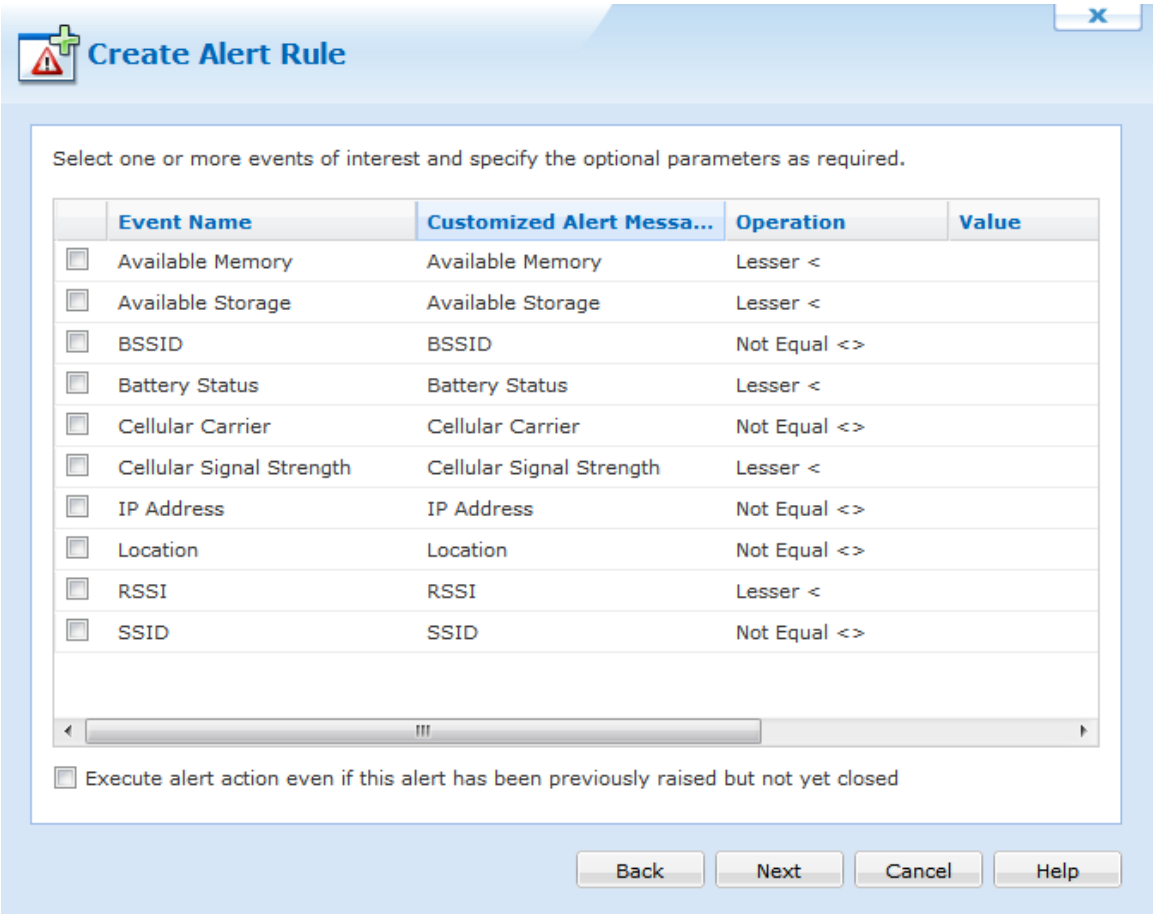


Select an existing notification profile, or click New to create a new Notification Profile. For assistance with notification profiles click here. Once you have selected your notification profile click Next.

Click Next and continue the Alert Rule Wizard here.

Device Status and Custom Data Event

A Device Status and Custom Data Event is an alert triggered based on an assortment of data values that you have set. See below for a full list.



Device Status and Custom Data Event Notification Selection Window

The Operation and Value fields allows to filter out Alerts based on specific values or value ranges. The Operation field specifies at which point an alert will be created for the data value you have specified. Severity is set to Minor by default and can be altered.

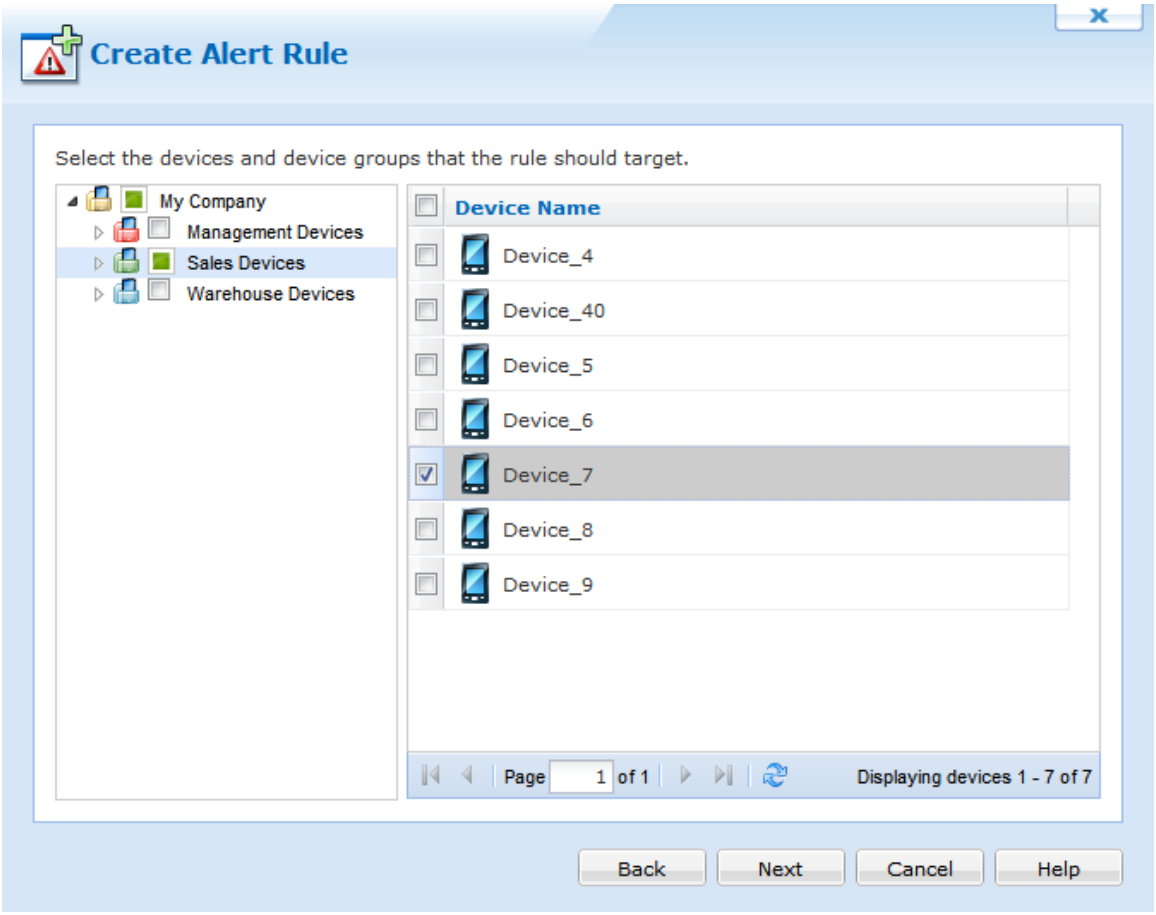
The below table shows all available default Device Status and Custom Data Event events:

Log Event	Alert Message Alert Message (Customisable)
Battery Status	Battery Status
Available Memory	Available Memory
Available Storage	Available Storage
SSID	SSID
Wi-Fi Signal Strength	Wi-Fi Signal Strength

Log Event	Alert Message Alert Message (Customisable)
IP Address	IP Address
Cellular Carrier	Cellular Carrier
Cellular Signal Strength	Cellular Signal Strength

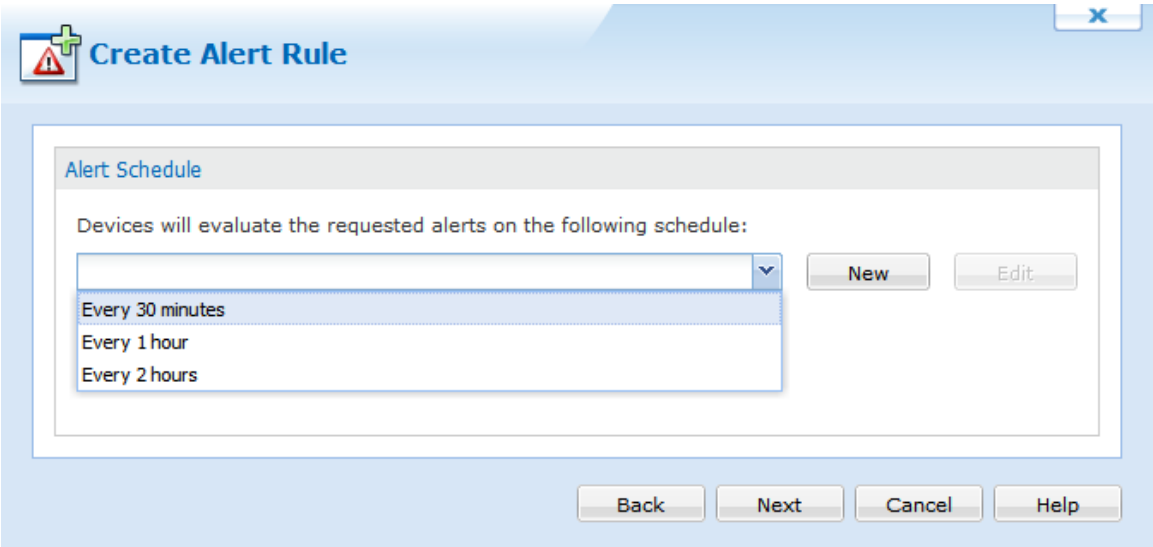
Select devices.

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



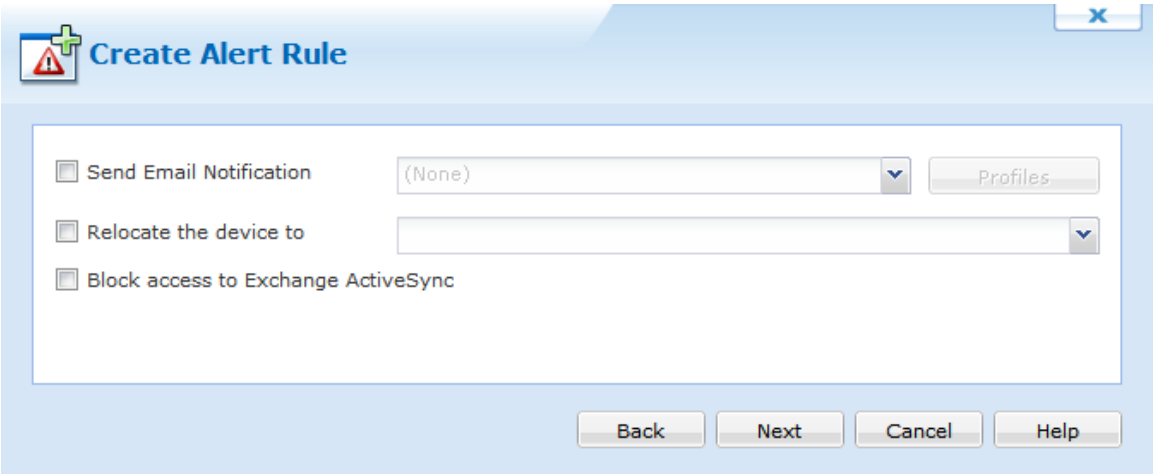
Select Schedule.

Select how frequently the devices should be checked for the requested Alert information. Once you have completed this section, click the **Next** button.



Select Actions.

Select an existing notification profile, or click Profile to create a new Notification Profile. For assistance with notification profiles Click Here. Once you have selected your Notification Profile you can select a Device Side Action. This action is a script that will be launched on the device when certain criteria is met. For assistance with the Script Manager Click Here.



After selecting your Profile and Actions, click Next and continue the Alert Rule Wizard here.

Windows Mobile Telecom Expense Management

The Telecom Expense alert rule allow MobiControl Administrators to monitor how much data and minutes a group of devices/individual devices use, based on a company data plan. This rule allows Administrators to set a soft threshold along with a hard threshold. When data or voice minutes reach either the soft or hard threshold, devices can automatically be relocated to another group and have either data or voice disabled. An email can also be generated and sent to a configured email address when a threshold is reached.

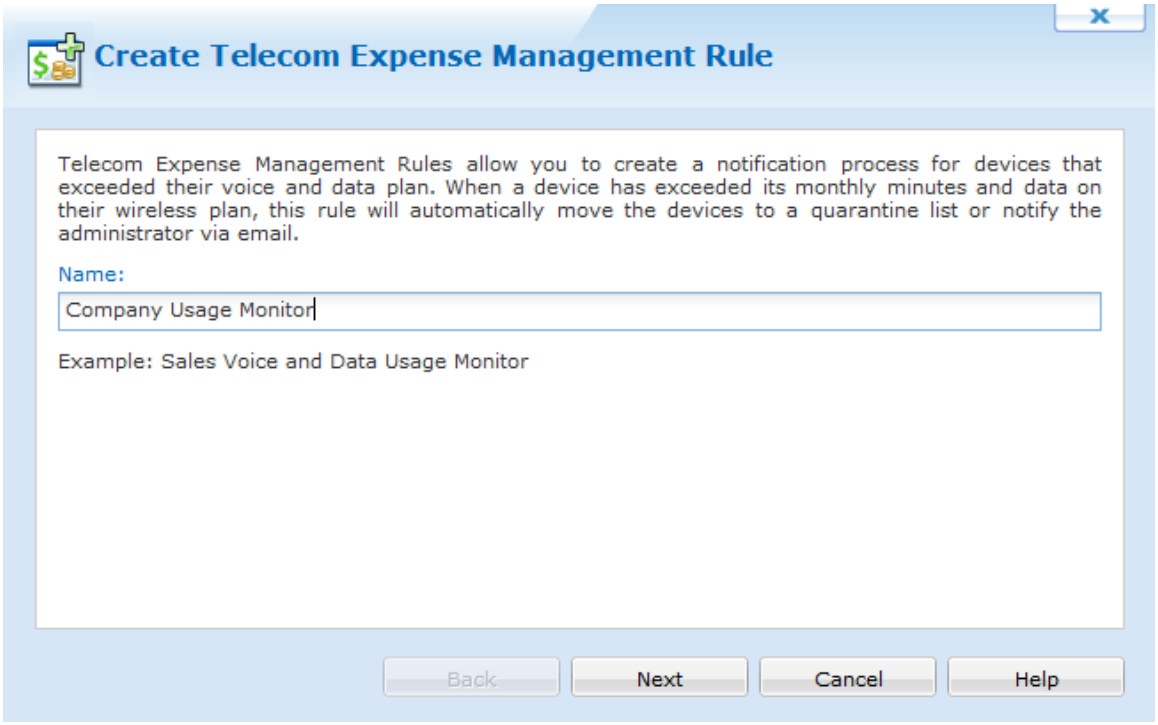
This allows enterprises to better manage company data and voice minutes.

The steps below describe how the Create Telecom Expense Management Wizard can be used to create an Telecom Expense Alert using the MobiControl Web Console:

1. Start the wizard.

   Select the Windows Mobile Tab, then select the Rules tab. After, right click on the **Telecom Expense** folder, and select **Create Telecom Expense Management Rule**. The first page of the Create Telecom Expense Management Wizard will be displayed.

   Enter a descriptive name for the Telecom Expense rule and click **Next.**



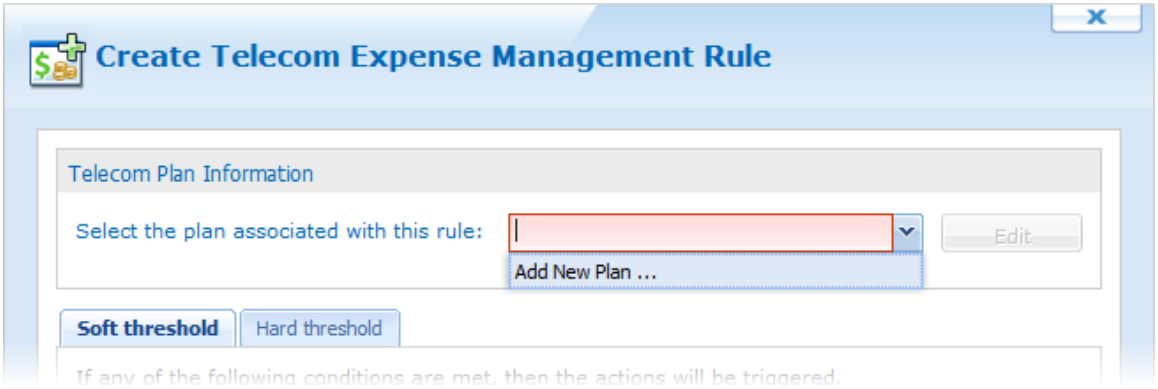
Enter a descriptive name for the Telecom Expense Rule

2. Select the target for the rule.

Here, we can select which group or device will be monitored with the Telecom Expense Management rule. Groups or devices that have ■ means that they are automatically selected because their parent group is selected. Groups that have ■ means that a child of that group is selected. Click **Next** to continue.

3. Telecom Expense Management configuration

On this screen, we are able to create a new data plan that will be associated with this rule, or choose an existing one. To create a new plan, choose the **Add New Plan** from the very top drop down menu.

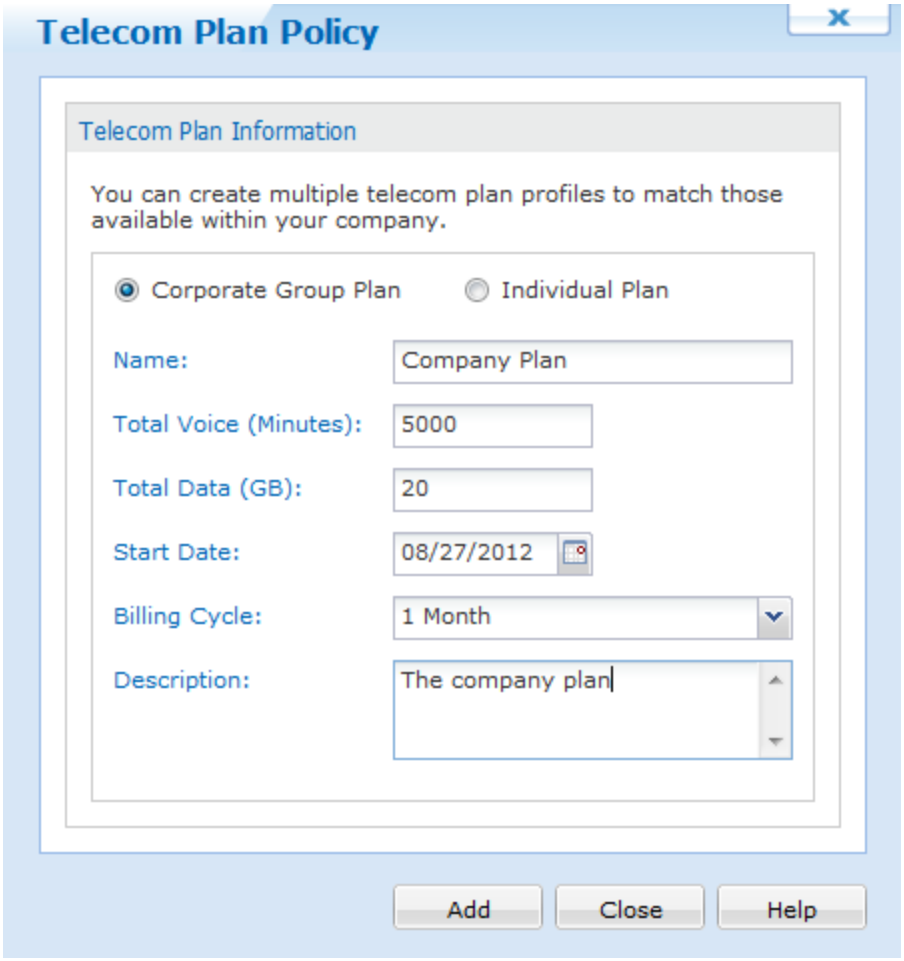


Adding a new Telecom plan

When **Add New Plan** is selected, the Telecom Plan Policy window is shown. Here we can choose whether this plan should be for a Corporate Group plan or an Individual Plan.

It is recommended that Corporate Group Plan is selected if the Telecom Expense Management rule is targeting a group of devices.

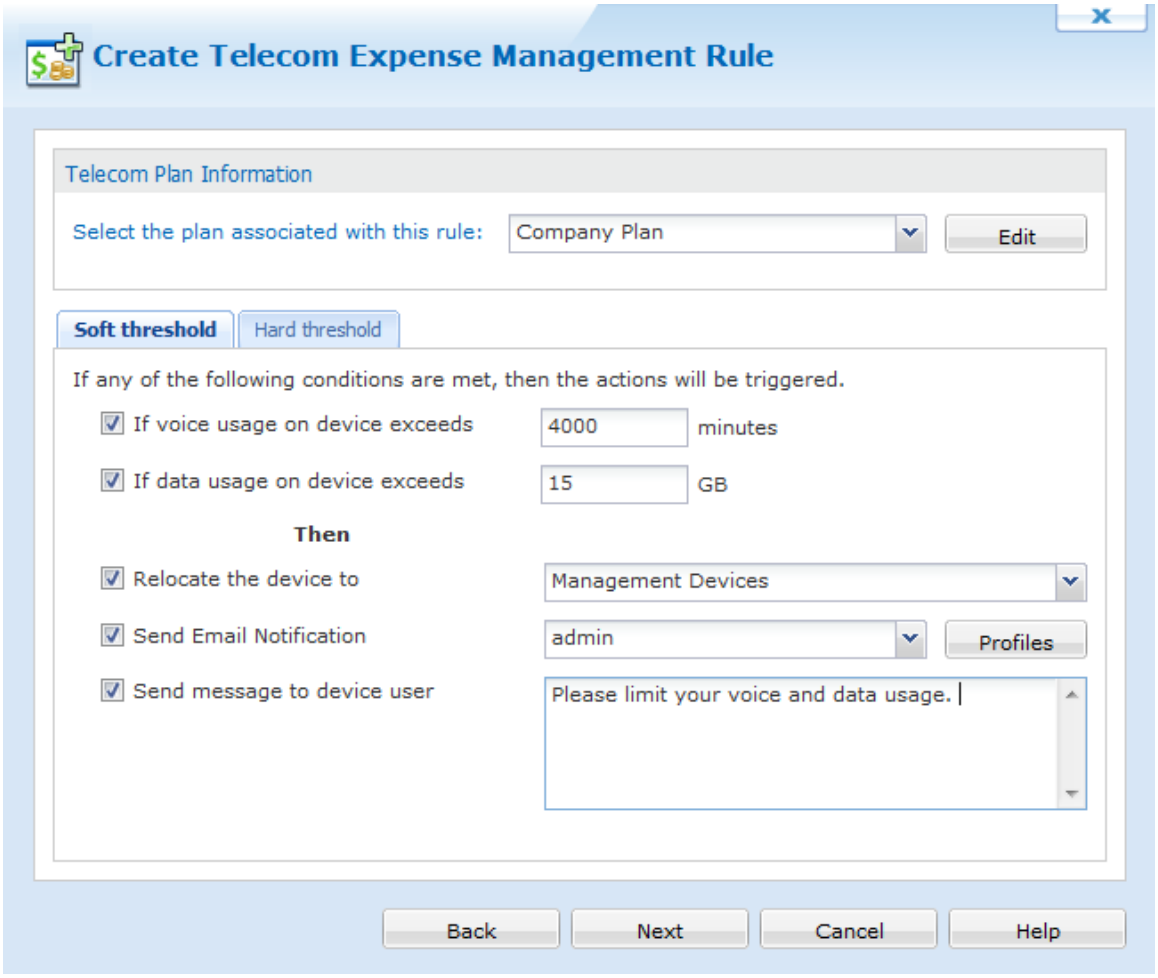
- A name and a billing cycle must be entered to add a plan.
- Voice is calculated in minutes, while data is calculated by gigabytes. If either of these are left blank, then unlimited is automatically listed.



Telecom Plan Policy

When a plan policy is created we can then configure the soft and hard threshold for the rule. Think of the soft threshold as a warning, and the hard threshold as critical. If the "voice usage on device exceeds" check box is selected, MobiControlwill check if a device or devices reach the number specified. The same rule applies for monitoring data usage. If any of the numbers are reached, MobiControl can then move the device to a new group, send an email notification, or send a message to the user.

After setting up the configurations here, click **Next**.



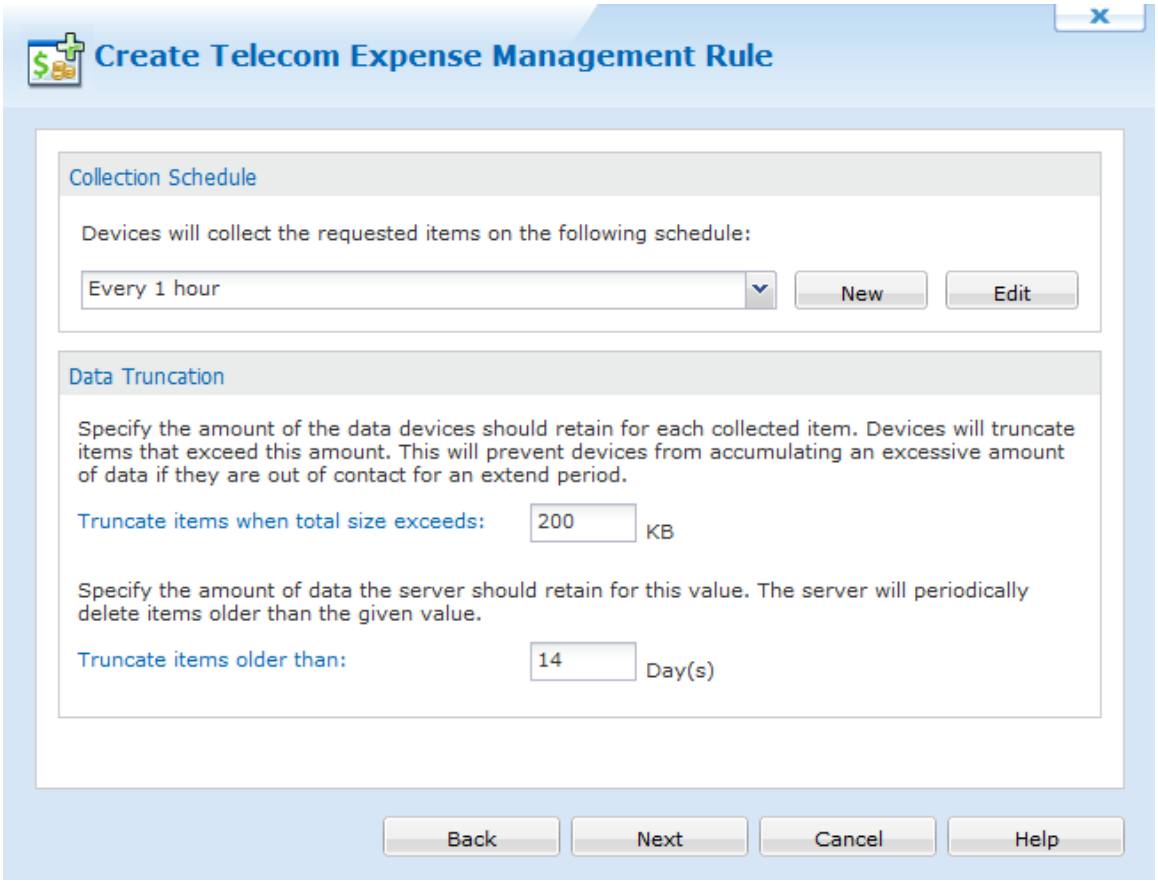
Telecom Expense configuration

4. Configure Data Collection and Optional Settings

Here, we can set how often the data is to be collected. Options include every 30 minutes, every hour, every two hours or daily. We also have the ability to create a custom collect schedule.

Data truncation specifies the amount of data that each device should retain. Any amount of collected data that goes above this number, will be truncated. This can be left as the default value.

After specifying the collection schedule and data truncation settings, click **Next**.

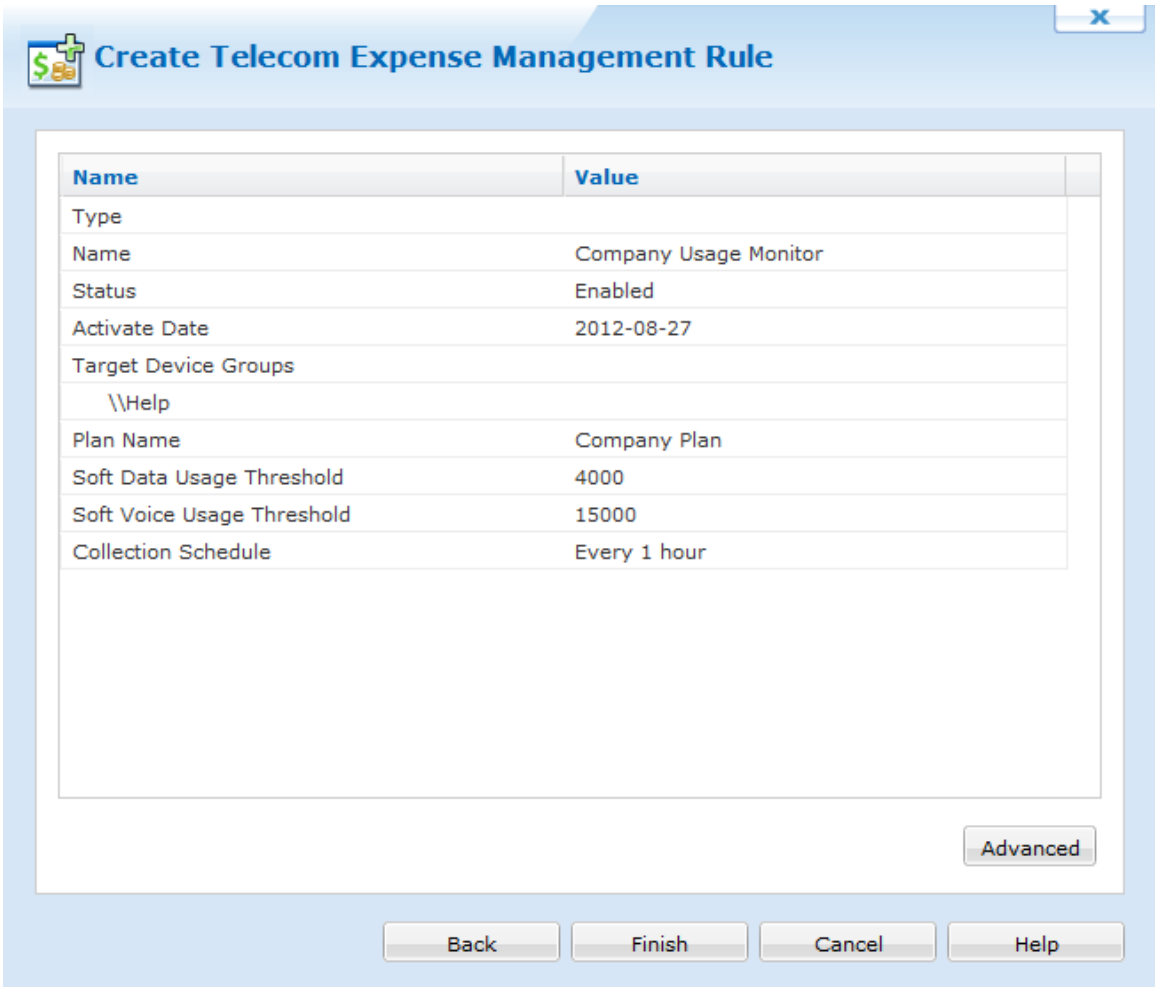


Data collection and optional settings

After specifying the collection schedule and data truncation settings, click **Next**.

5. Review the summarized information.

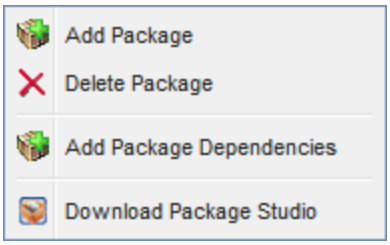
   The summary page will show all options and configurations that was specified in the previous steps. If something is needed to be changed, just click back and change the setting.



   Once everything is confirmed, click **Finish** to complete the wizard.

Packages Tab

The Packages view (tab) provides a list of the packages that have been imported into the MobiControl system, and the status of their distribution to the devices in the deployment. From this tab you can:



- Upload a Package
- Delete a Package
- Download Package Studio
- Create a Package Dependency

The left panel lists all of the packages that have been imported into the MobiControl system. Package are created using MobiControl Package Studio. Please see the "MobiControl Package Studio" topic on page 413 for more information.

If multiple versions of a package have been imported, each is listed with its own unique version number. The version number is set when creating or editing a package using MobiControl Package Studio.

Adding or Deleting a Package

To add a package to MobiControl, click **Package,** and then click **Add Package.**

To delete a package from MobiControl, select the version number node for the package, click **Package,** and then click **Delete.**

Download Package Studio

Package Studio must be downloaded in order to create packages. The Package Studio is typically installed with the thick client, but if you are using Web only then you can download Package Studio to work with on your desktop.

Package Dependencies

Package dependencies are a way to ensure the correct sequence of installation of packages on a device. To establish a package dependency, click **Package,** and then click **Add Package Dependencies.**

Panels in the Packages Tab

Info Panel

The Info panel provides detailed information about the package that is currently selected in the listing panel. Information includes the meta-data associated with the package that was specified when it was created, for example, processor, platform or OS version, and vendor information. Please see the "Create Package Project" topic on page 415 for a detailed explanation of these fields.

The content displayed in this panel is stored in the MobiControl database. You can select **Refresh** or press F5 on this tab to retrieve updated information from the database.

Devices Panel

The Devices panel lists the devices that have the selected package installed, or marked as pending for installation/uninstallation.

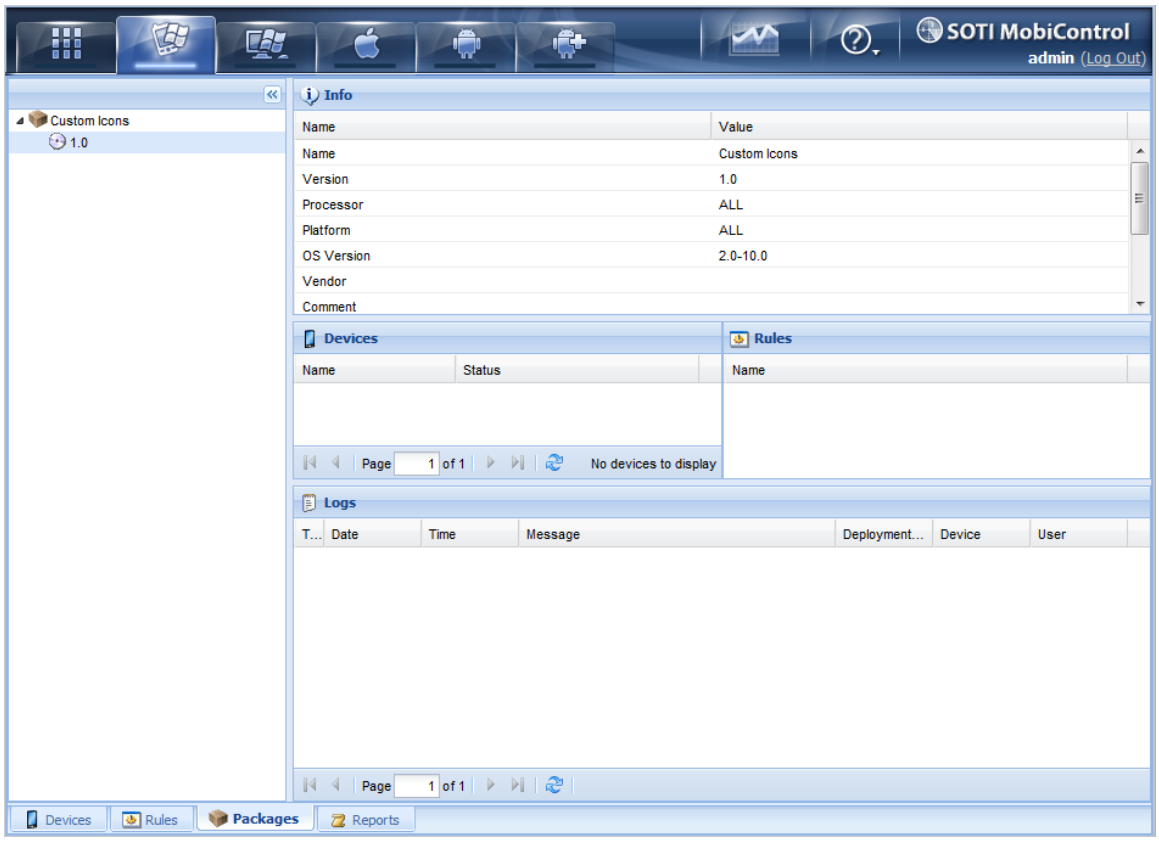
Rules Panel

The Rules panel lists the deployment rules that are configured to deploy the selected package.

Logs Panel

The Logs panel lists events occurring in the MobiControl system. This listing is filtered based on the package that is selected in the package listing.

You have the option to enable or disable logging, as well as adjust the maximum number of logs displayed and frequency with which the Manager should refresh the log panel.



MobiControl Packages Tab Packages view (tab)

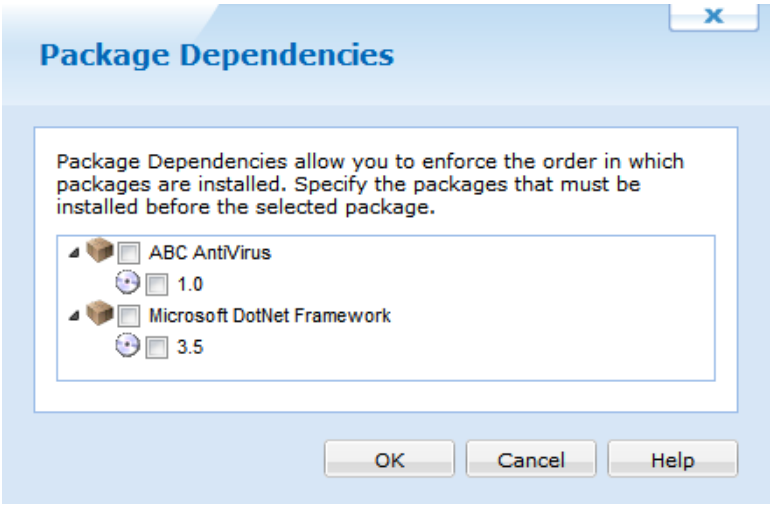
Package Dependencies

Package dependencies provide a mechanism to enforce the order in which packages are installed on a device.

To display the **Package Dependencies** dialog box, right-click on the package and select **Add Package Dependencies** from the pop-up menu. The **Package Dependencies** dialog box lists the configured dependencies.

Adding Package Dependencies

To add a package dependency, select the package(s) and version(s) upon which the target package is dependent.



Package Dependencies dialog box

EXAMPLE:

Packages A and B need to be installed, but it is mandatory that A is installed before B. Configure a dependency for package B: when editing the package dependencies for package B, select package A.

NOTE:

If a package depends on another package that is scheduled to install at a later time, then the Deployment Server will not push the package unless it is also scheduled to install at the same time or later. Please see the "Windows Mobile Package Deployment" topic on page 764 for more information about installation schedules.

Reports Tab

MobiControl includes an advanced reporting engine—Crystal Reports—that gives detailed information about all aspects of system operation. The product includes a set of canned reports that provide information about key areas of system operation. Reports can also be customized as well as new reports can be created and added to the system as needed.

MobiControl Web Console Reports view (tab)

Report Types

The following reports are included with MobiControl:

- A **deployment server activity report** is a detailed report for deployment server activity over a specified time period.
- A **deployment rule report** is a detailed report of deployment rules and all devices.
- A **Battery and Storage Report** is a detailed report of the battery and storage of the selected devices.
- A **Cellular Signal Strength Data Report** is a detailed report of the cellular signal strength of the selected devices.
- A **deployment rule summary report** is about deployment rule exceptions, showing how many devices have executed the rule successfully, are pending, or have encountered an error.
- A **Deployment Server activity report** is a detailed report of Deployment Server activity over a specified time period.
- A **device activity report** provides information about the device activity during a specific time period.
- A **device custom data report** provides information about devices with the custom data values of selected custom data fields.
- A **device note report** provides information about the notes for your devices.
- A **device package report** provides information about packages installed on your device.
- A **device program report** provides information about all the programs installed on your devices.
- A **device relocation rule report** provides information about all the relocation rules for your devices.
- An **out of contact devices report** provides information about devices that have not connected to the system since the specified date.
- A **package deployment report** provides information about package deployment.
- A **Location Collected Data Report** is a detailed report of the location data collected for the devices.
- A **Connectivity Information Report** is a detailed report regarding device's connectivity.
- A **Device Tree Report** provides information about the device tree structure.
- A **Device Tree with Virtual Groups Report** provides information about the device tree structure along with the virtual groups.
- A **Log Information Report** provides information about the device logs.
- A **Phone Number Report** provides information about the phone number of devices.
- A **Alert Summary Report** provides summary of the alerts.
- A **deployment rule report** is a detailed report of deployment rules and all devices.
- A **Geofence Report** provides detailed report based on the Geofence.
- A **Uninstalled Mandatory Applications Report** provides information about the mandatory application not installed on the devices.

Generating a Report

1. In MobiControl Manager, select the Reports view (tab).
2. Select a report in the left pane of the Reports view (tab).
3. Click the **Generate Report** button.
4. For some reports, a window will appear requesting additional parameters (e.g. time period) that may be required.

MobiControl Web Report toolbar view

Saving a Report

1. Generate a report.
2. On the report screen, click the **Export Report** button. (It is the first icon in the toolbar, beside the **Print Report** button.)
3. Select the desired file type. Available file types are:
    - Adobe PDF (`.pdf`)
    - Crystal Reports (`.rpt`)
    - HTML 3.2/4.0 (`.html`)
    - MS Excel 97-2000 (`.xls`) or Data only (`.xls`)
    - MS Word editable RTF (`.rtf`)
    - ODBC
    - Record-style (columns of values with or without spaces) (`.rec`)
    - Report definition (`.txt`)
    - Rich text format (`.rtf`)
    - Comma-separated values (`.csv`)
    - Tab-separated text (`.ttx`)
    - Text (`.txt`)
    - XML (`.xml`).
4. Select the location to which you want to export the report. The options available are:
    - Application
    - Disk file
    - Exchange folder
    - Lotus Domino
    - Lotus Domino Mail
    - MAPI (Messaging Application Programming Interface)

Printing a Report

1. Generate a report.
2. On the report screen, click the **Print Report** button. (It is the second icon in the toolbar, beside the **Export Report** button.)
3. The print menu will pop up. Select the desired printer and the report will be printed there.

Generating Custom Reports

It is possible to create custom report files on any available statistic you desire. The Deployment Server database is a standard SQL database and can be queried by writing a custom query. Also, it is possible to create additional reports that are built into MobiControl. For more details, please contact us.

Other Tools

These other tools are available through the toolbar:

- The **Stop Loading** button stops the report generation process.
- **Refresh** regenerates the report. If parameters were required to generate the original report (e.g. time period), a window will appear requesting the additional parameters.
- The **Search Text** button searches the body of the report for a specified text string.
- The **View Zoom** field allows the user to select view magnification, page width, and whole page views.

MobiControl Tutorial

This is the last step of the MobiControl Tutorial. We hope you feel comfortable with MobiControl!

Windows Desktop Devices

The **Windows Desktop Device** tab enables you to access the devices connected to the deployment running a Windows desktop OS. All functions that affect this operating system are performed such as:

- Location Services
- Device Security
- Device Configuration
- Adding a Device
- Distributing software to a device
- Data collection functions
- Alerts

There are five views within the MobiControl web console. The views can be selected using the tabs at the bottom of the MobiControl Manager user interface.

- The **Devices view (tab)** allows users to view information about configured devices, for instance packages installed, device ID, and IP address. The Devices view (tab) also allows users to control and configure devices, for example, to remote control a device or to change a device's name.
- The **Rules view (tab)** allows users to view information about the configured rules. The Rules view (tab) also allows users to configure rules, for instance, create an add devices rule, a deployment rule, a file sync rule, an enable rule, or a disable rule.
- The **Packages view (tab)** allows users to view information about packages, for instance the packages currently configured or a list of devices onto which a certain package has been installed. The Packages view (tab) also allows users to configure package-related information, for example to add or delete packages.
- The **Deployment Servers view (tab)** allows users to view information about the configured Deployment Servers or to manage Deployment Servers, for example, enabling or disabling, shutting down, or viewing a list of devices connected to a Deployment Servers.
- The **Reports view (tab)** provides users with a set of reports containing detailed information about the operation of the system. Provided reports include: deployment rule execution summary report, device configuration rule execution summary report, and device activity report.

Windows Desktop Devices Tab

The Devices view (tab) is the main view into the status of the devices in the MobiControl system.

Device Tree

The device tree provides a structured view of the devices in the system.

Commonly-reported device information can be easily referenced in the device tree window by right-clicking in any open space in the device tree window and selecting the information that you would like to see displayed.

Devices are added to the system by defining an add device rule and creating a MobiControl Device Agent that is installed on the device. Please see the "Add Windows Desktop Devices" topic on page 880 for a detailed explanation of how to add devices to MobiControl.

Info Panel

The Info panel provides detailed status information about the group or device that is selected in the device tree. When a group is selected, the displayed information includes the number of subgroups and how many unique, online, offline, or disabled devices are in the group. For devices, the displayed information includes device ID, IP address, battery and memory status. In addition, custom data retrieved from your devices may also be displayed. Please see the "Windows Desktop Custom Data" topic on page 839 for detailed information about configuring custom data retrieval.

The content displayed in this panel is stored in the MobiControl database. This information is refreshed when a device establishes a new connection to the MobiControl Deployment Server, and when you click **Refresh** or press F5 on this tab.

Logs Panel

The Logs panel provides a listing of the events occurring in the MobiControl system. This listing is filtered based on the group or device that is selected in the device tree. If only one device is selected, only the events related to that device are displayed. If a group is selected, events for the group and all the devices that belong to that group are displayed.

You have the option to show or hide logging, adjust the maximum number of logs displayed, and the frequency with which the Manager should refresh the log view.

Update Schedule Panel

The Update Schedule panel lists the dates and times when the device is programmed to query the MobiControl system to check for updates. By default, a device will also check for updates whenever it connects to the MobiControl system. Please see the "Windows Desktop Device Update Schedule" topic on page 861 for more information.

Installed Applications Panel

The Programs panel lists the applications that are installed on the device that is selected in the device tree. This is the same listing that is displayed by the **Remove Programs** applet provided by the Microsoft operating system.

Rules Assigned Panel

The Rules Assigned panel lists the deployment and file sync rules assigned to the group or device that is selected in the device tree. Rules are inherited from parent groups; a rule will apply to a device if it belongs to group to which the rule has been assigned.

The assignment of rules to groups provides a flexible and convenient means for easily configuring devices. For example, once you have set up your rules for software or data distribution, you can automatically provision your devices by simply adding them to the appropriate group within the device tree. Please see the "Windows Desktop Rules" topic on page 877 for information on creating deployment rules and file sync rules.

Notes Panel

The Notes panel lists the notes that are associated with the selected device. If a group is selected in the device tree, all the notes for the devices that belong to the group are listed. Notes are a convenient way to maintain information about the device such as trouble tickets. Please see the "Device Notes" topic on page 1384 for information on creating device notes.

Packages Panel

The Packages panel lists the packages that are configured on the device that is selected in the device tree. The assignment of packages is directly based on the assigned rules. This panel provides a status column which indicates the state of the package for that device. For example, the status "Pending" indicates that the package has been queued and its installation on the device is pending.

You can force the re-installation of a package on a given device by right-clicking on the package in the Package Panel and selecting **Force Package Reinstall on Next Schedule** or **Force Package Reinstall Now.**

Collected Data Panel

The Data Collection Panel allows you to view the collected historical data for a set of devices. By creating a Data Collection Rule you will be able to specify which items to collect data from, how often to collect them, and when to upload the collected data to the server. Please see the Creating Data Collection Rules page for information on creating Data Collection.

Location Panel

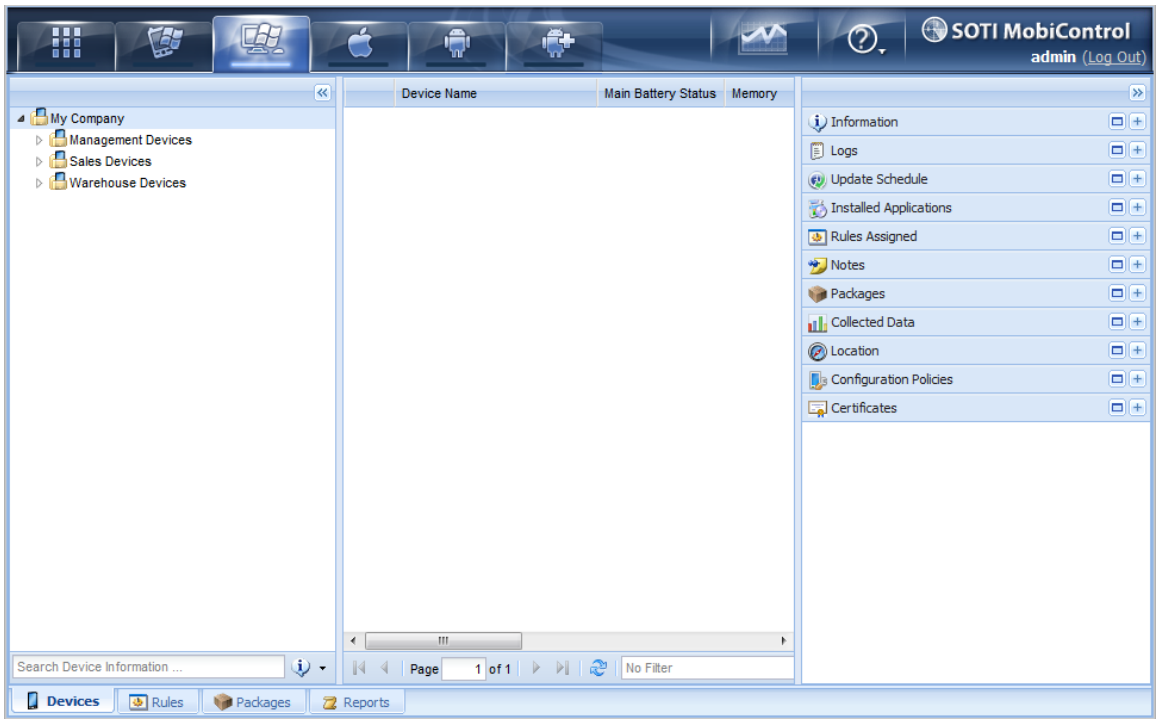
The Location Panel gives the ability to locate, track and gather information on the movement of your GPS enabled devices, no matter where they are in the world which is powered by Microsoft's Bing maps technology. Whether you need to confirm the current location of a particular field-worker, track the progress of an important shipment or collect historical information on the movement of a group of devices or vehicles in order to analyze performance, MobiControl's Location Services can help. Please see the Location Services page for more information.

Configuration Policies Panel

The Configuration Policies panel lists all policies that are currently configured on the device. It also lists where these policies are inherited from. This allows us to have a quick look to see what configurations are currently on devices.

Certificates Panel

The Certificates Panel lists all certificates that MobiControl sent to devices. Certificates can range from email to WiFi authentication.



MobiControl Devices Tab Devices view (tab)

Windows Desktop Device Configuration

MobiControl offers Windows desktop device users to engage interface lockdown, also known as "kiosk mode", and send the configuration to the device automatically.

MobiControl's security provides powerful features for securing devices and mobile data, while maximizing usability and making security implementation easy, efficient and cost-effective. Salient features of MobiControl's security include:

- Over-the-Air (OTA) security policy distribution
- Policies can be assigned at the individual device, group or global level

To access MobiControl's Security Center, select the device or group of devices for which you want to configure security and then click **Device,** click **Device Configuration**.

Lockdown Policy

MobiControl allows administrators to operate mobile devices in a lockdown or kiosk mode by providing them with a specialized interface that strictly provides the device user with access to approved applications and websites only. Integrated locked-down or industrial web browser allows restricting browsing to specific Internet or Intranet sites only. Please see the "Windows Desktop Device Lockdown" topic on the next page for more information on configuring lockdown.

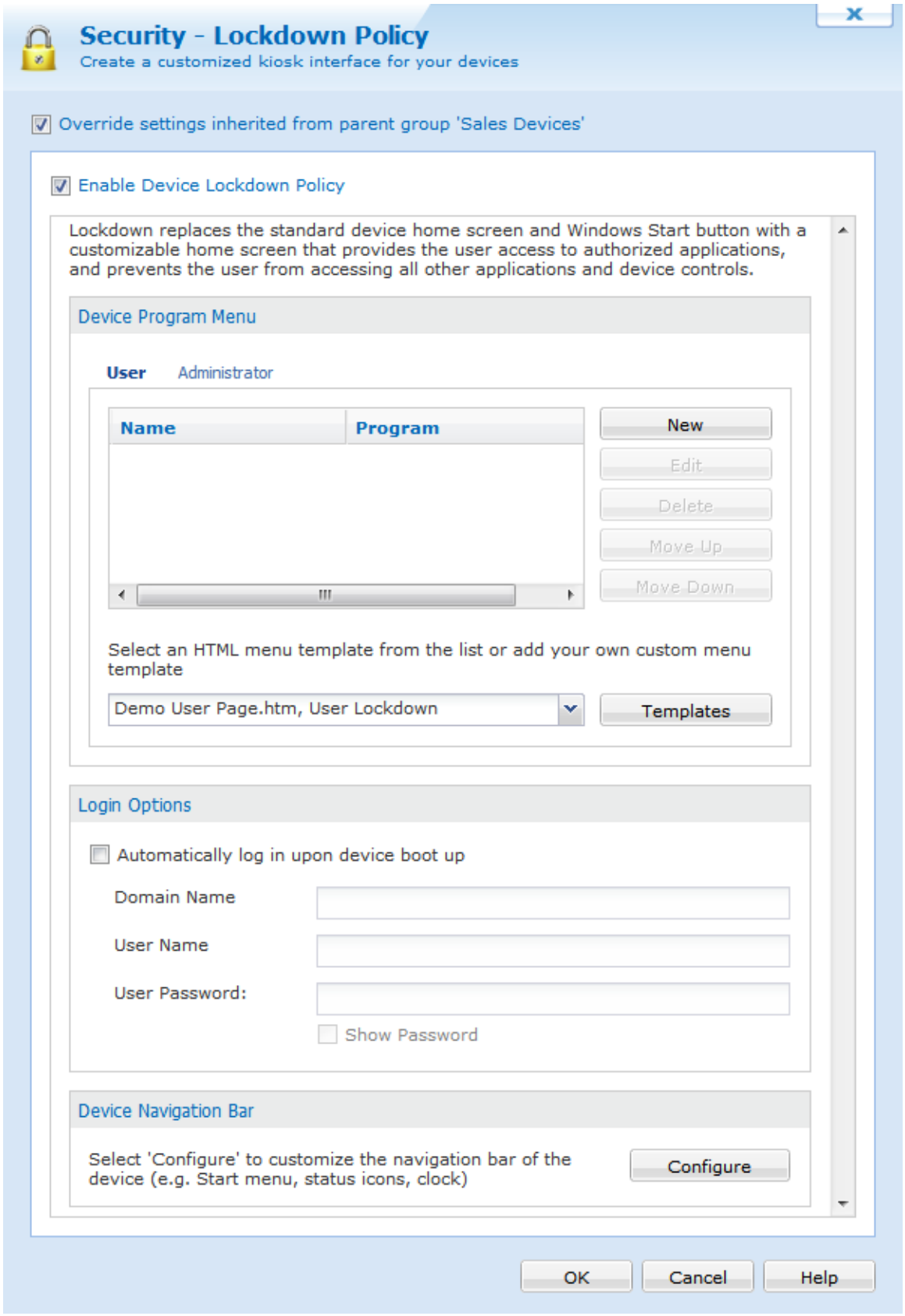
Connection Security Policy

To protect the integrity of the corporate firewall and to secure communication and data flowing from the mobile devices to the server across public unsecured networks, MobiControl allows the use of SSL Mode for encrypting communication using SSL certificate-based communication security. Please see the "Windows Desktop Connection Security" topic on page 831 for more information on configuring connection security.

Windows Desktop Device Lockdown

Device lockdown replaces the standard device home screen and Windows **Start** button with a customizable home screen. Users have access only to authorized applications and websites, and are prevented from accessing all other applications and device controls.

Please see the Windows Desktop Device Speed Lockdown page for more information about the Speed lockdown.



Lockdown Policy dialog box

For assistance with Override Settings Click Here.

By locking down devices, organizations can minimize the risk of unauthorized persons accessing information on their mobile devices. Administrators can control exactly which programs users are allowed to run, and which websites they are allowed to visit. This decreases the amount of down-time caused by users changing settings that may adversely affect the operation of the device or application software, and also decreases support costs. MobiControl allows running the mobile devices in a kiosk mode with a read-only access to provide critical information to the end users, without giving them access to change the settings.

The lockdown menu can only be dismissed by an administrator. Specification of a user password is optional. If not configured the device user can access the lockdown menu directly after turning on the device. If a user password is defined, then the password must be entered in order to access the lockdown menu.

To configure lockdown settings for a device or group of devices, select the target device or group in the device tree view in the main console window and select **Security** from the **Configure Device(s)** submenu.

Field Name	Description
Enable lockdown menu	Use this checkbox to enable or disable the device lockdown menu.
Device Program Menu	The device program menu is a list of programs and websites to which the user has access. There are pre-configured HTML menu templates that can be edited or applied to the menu, and an option to enable or disable the launching of a menu item with keyboard shortcuts. Please see the Device Program Menu section below for details.
HTML menu template	Select a menu template from the drop-down list. Please see the Templates section below or the Customizing Lockdown Program Menu Templates page for more information.
Enable program launch via keyboard shortcuts	Keyboard shortcuts such as numeric keys can be used to launch lockdown menu items. See the Shortcuts section below.
Device Navigation Bar	The device navigation bar, commonly referred to as the task bar, contains the **Start** button and small icons for quick access to device status and settings such as the time, date, wireless status, or volume control. By default, when lockdown is enabled, the standard operating system navigation bar is replaced with a customizable navigation bar. Select the **Configure** button to specify which icons in the custom navigation bar are to be made available to the device user. Please see the Navigation Bar Configuration section below for details.

Add New Menu Item dialog box

TIP:

- To provide the device users with access to specific websites and prevent access to other websites, provide the URL in the **Program Path** of the **Add New Menu Item** line.
- If you link to a search engine the end user will gain full access to the Internet.

Device Program Menu

Use the **New** button to add menu items. Each entry consists of a user-friendly name and a complete file path to the executable, `.lnk` shortcut file, `.cmd` script file, or website address (URL). To adjust the position of the menu items, use the **Move Up** and **Move Down** buttons.

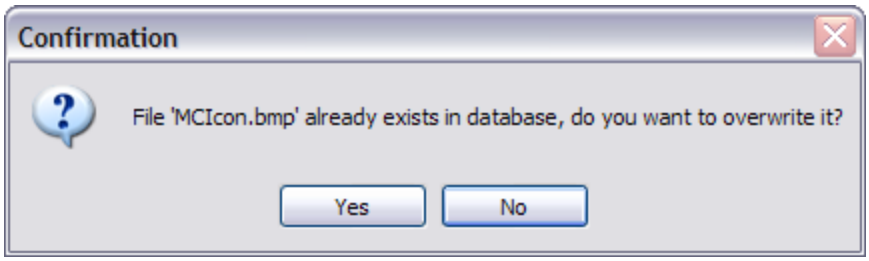
Field Name	Description
Display Name	This is the displayed name of the menu item which will appear on the device.
Program Path	This is the path for the web address, or executable file on the device. For instance, the program path for Pocket Word is `C:\MyFolder\MyApp.exe`. The path will not be

<table>
<tr><th>Field Name</th><th>Description</th></tr>
<tr><td></td><td>displayed on the Menu page.

NOTES:

• For command line parameters, a comma must be used to separate the program path from the parameter. For example, write <code>\windows\poutlook.exe,contacts</code> without spaces.
• Incase a " character is required for paths including spaces in them, in place of double quotes, %22 MUST be used.</td></tr>
<tr><td>Image (optional)</td><td>This is the name of the image file that you want to display in the lockdown menu with this menu entry. By selecting the image in this dialog box, it will be automatically delivered to the device along with the lockdown configuration. Select an image from the drop-down list, or click the browse button to select an image from your desktop computer.
In order to display this image in the lockdown menu, it is necessary for the HTML template to have a special <code><MCDispImgN></code> tag. Please see the Customizing Lockdown Program Menu Templates page for instructions on how to make this image appear in the Lockdown menu.

NOTE:
If you wish to replace an image that had been previously imported, upload the new graphic file, maintaining the same file name as the old one. You will be asked to confirm the overwrite of the old file. Click Yes, and the new image will be in effect.

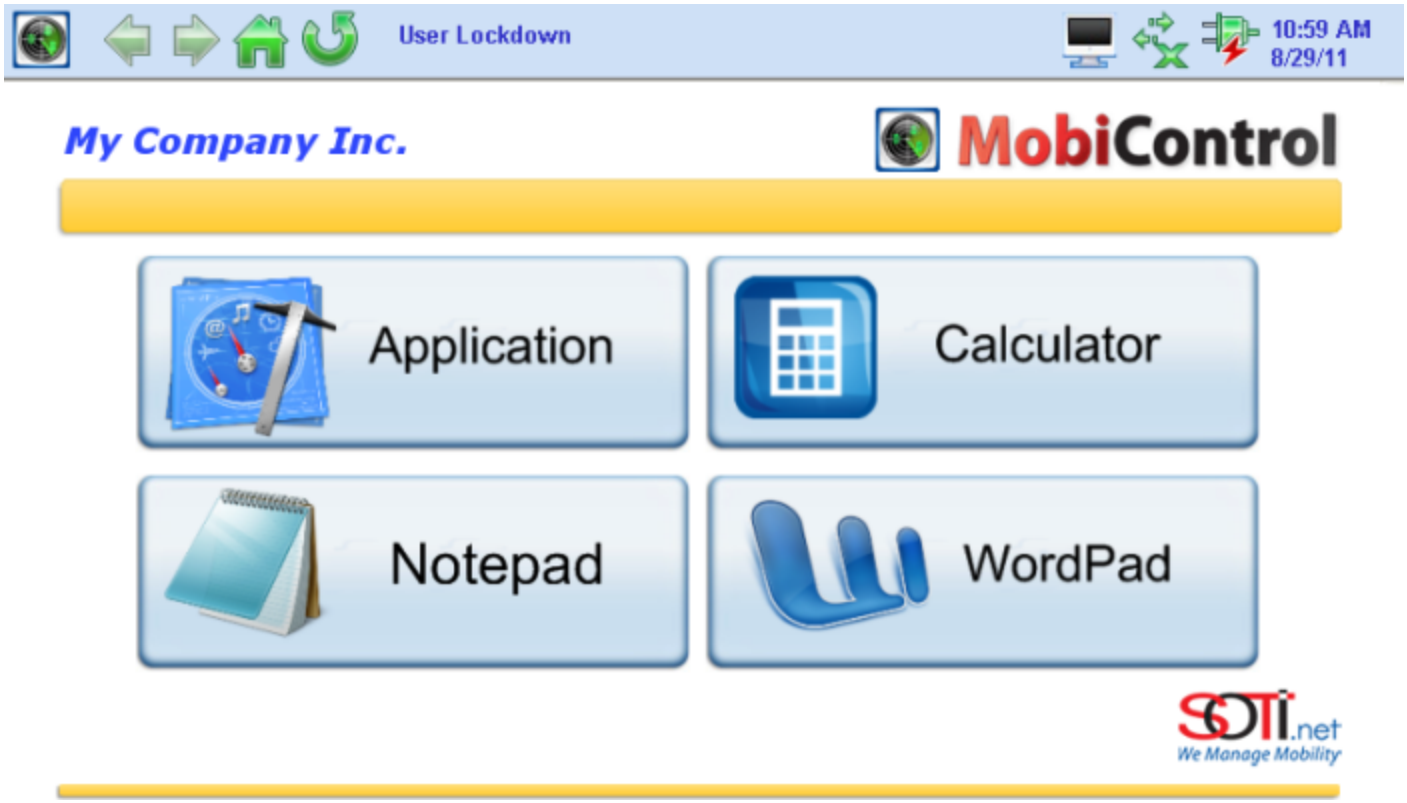
Lockdown Menu Image Overwrite Confirmation dialog box</td></tr>
</table>

TIP:

On devices that feature a numeric keypad, an alternative to tapping the screen to launch the menu entries is entering the number that corresponds to the menu item. For example, press 2 to launch the second menu item.

Templates

The lockdown program menu is displayed as an HTML web page to the user. The Template drop-down box allows you to select an HTML template from a list of built in templates and your own customized templates.



Device lockdown page

You can easily create a customized lockdown template by copying an existing template and directly modifying HTML code in the built-in Lockdown Menu Template Editor available in MobiControl. (Please see the Customizing Lockdown Program Menu Templates page.) You can also use your favorite HTML editor. When editing the HTML file, be sure to preserve the special MobiControl Menu tags. These special tags are automatically replaced with the appropriate Program Menu entries by MobiControl.

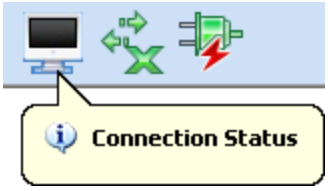
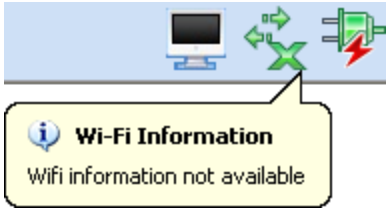
Once you have selected the desired template and clicked the **OK** button, MobiControl will merge the menu items that you have configured with the selected template and generate a custom HTML menu page.

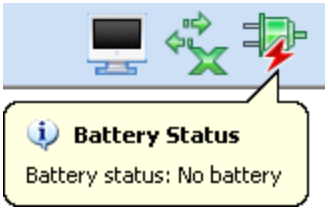
Keyboard Shortcuts

If the checkbox next to **Enable program launch via keyboard shortcuts** is selected, program menu items may launch in a few additional ways: pressing a numeric key on the device or using a scanner will launch the program menu item corresponding to the value of the numeric key or barcode. To prevent this, clear the checkbox next to **Enable program launch via keyboard shortcuts**.

Navigation Bar Configuration

Navigation Bar Configuration dialog box

Field Name	Description
Show Navigation Bar	This checkbox determines if the following buttons are displayed on the **Menu Bar**: • Back • Forward • Home • Refresh The **MobiControl** "start" icon will still be present. 
Show Agent Connection Status	This checkbox determines if the **Connection Status** will be displayed on the **Menu Bar**. 
Show Wireless Network Status	This checkbox determines if the **Wireless Network Status** will be displayed on the **Menu Bar**. 

Field Name	Description
Show Battery Status	This checkbox determines if the **Wireless Network Status** will be displayed on the **Menu Bar**. 

Connection Security

To ensure the integrity of the corporate firewall and to provide an additional layer of security for data flowing between the mobile device and the MobiControl Manager(s) and Deployment Server(s) over public networks, SSL Communication Mode is available to provide encrypted communication. When SSL is not enabled MobiControl encrypts all communications using proprietary algorithms. SSL provides the additional benefit of standards-based authentication and encryption security.

To enable SSL communication for a device or group of devices, select **Connection Security Policy** from the MobiControl Security Center. Please see the "Windows Desktop Configuration" topic on page 823.)

This dialog box allows you to enable SSL communication for specific devices. For example, one group of devices which are in your warehouse do not need to use SSL, whereas you do want another group of devices that are in the field and communicating over public networks to use SSL.

Configure SSL device settings dialog box

For assistance with Override Settings Click Here.

The dialog box above allows you to specify the means by which you wish to have the MobiControl system deliver the Device Agent's certificate and private key to the device.

NOTE:

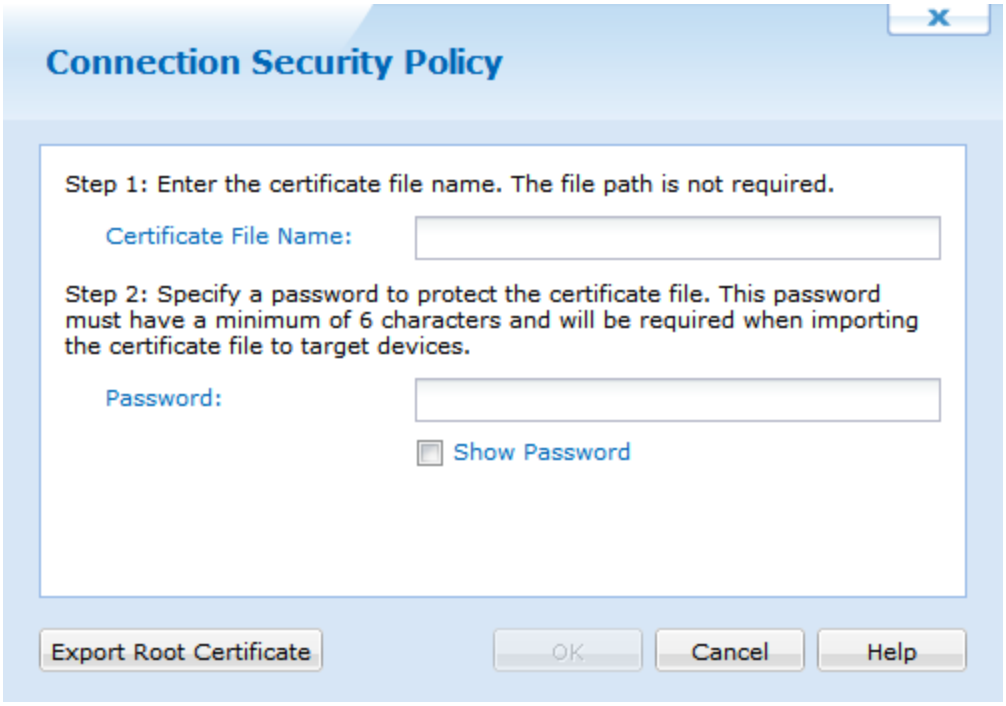
When SSL is enabled, MobiControl acts as its own certificate authority. It generates certificates for the MobiControl entities (Manager, Deployment Server, and Device Agents).

The table below summarizes the three available options for delivering and installing the device's MobiControl certificate:

Option	Description
Automatic delivery and silent installation of certificates	When this option is selected the Deployment Server will automatically deliver the certificate and private key for the device when the device connects. No user interaction is required.
Automatic delivery and prompt for password before installation on device	This option provides additional assurance that only authorized devices receive an SSL certificate and private key. When this option is selected, the Deployment Server will prompt the device user to enter the password specified in this dialog box before it delivers the certificate and private key. The device will be able to connect and stay online even if a password is not entered, however in this state the device will not receive any packages, or execute file synchronization. The administrative user can remote control the device to assist the device user with entering the password to retrieve the device certificate. The user will be given several chances to enter the correct password. If the user enters an incorrect password five times, and the **Keep Device Connected** check box is not selected, the device will be disconnected and disabled. To re-enable the device right-click on it in the device tree and select **Enable.** If the **Keep Device Connected** check box is selected, the device will remain online, and as described above, will not be eligible for package delivery or file synchronization but can be remote controlled.
Manual Installation (No automatic delivery or installation)	When this option is selected certificates and private keys will not be automatically delivered to the devices. The certificate and private key must be exported (`*.pfx` file), and delivered to the device by some means. This could be via email, file transfer, etc. **NOTE:** Importing certificates is only supported on Windows Mobile 5 devices and Windows desktop clients (Windows 2000/XP).

In all the cases above, the Device Agent stores the certificate and private key into the Windows operating system's personal certificate store. The MobiControl Root CA certificate, on the other hand, is stored in the operating system's trusted root certificate store.

Manual Installation



Export Device Certificate dialog box

When this option is selected, the certificate and private key must be exported (`*.pfx` file), and delivered to the device via email, file transfer, storage card, etc.

Once the `*.pfx` file has been delivered to the target device, the user must use the MobiControl applet running on the device to import it. For further information, refer to the SSL Cert tab in the mobile device configuration applet on importing the certificate. (Please see the "Mobile Device Configuration Applet" topic on page 397.

Configure Windows Desktop OS Devices

There are seven main aspects to device configuration. Each of these settings can be configured for a single device or applied at the device group level thereby configuring a set of devices. When the devices are moved from one device group to another in the device tree, the settings for the new device group are applied automatically to the devices. Please see the "Device Relocation Rule" topic on page 335 for more information on automatically re-configuring devices based on their location (using IP address or other custom criteria).

Custom Attributes

Custom Attributes allows us to create custom information that appears on the information panel on the right hand side of the web console. Please see the "Custom Attributes" topic on page 1343 for more information.

 Custom Data

This option allows you to create your own monitoring fields to be shown in the Device Info window. This can be useful for monitoring various aspects of third-party applications. Please see the "Windows Desktop Custom Data" topic on page 839.

 Connection Settings

This option allows you to configure advanced settings for your mobile device(s), via. configure connection security by enabling or disabling SSL, select connection mode between persistent, scheduled and manual, change connection retry interval and set log file management, among other options. Please see the "Windows Desktop Connection Settings" topic on page 849.

 Deployment Server Priority

This option allows you to specify the Deployment Server preferences for the devices. When a device is configured with more than one Deployment Server, it will try to connect to highest priority one first and if this server is not accessible, then it will try to connect to the next server available. Please see the "Windows Desktop Device Update Schedule" topic on page 861.

 Remote Control Settings

Select a device skin to display in the MobiControl Remote, and choose the connection profile to use when remote controlling the device. This allows for customized remote control settings, optimised for different types of connections, for instance, high-speed Wi-Fi or low-speed cellular connections). Please see the "Windows Desktop Remote Control Settings" topic on page 857.

 Support Contacts Info

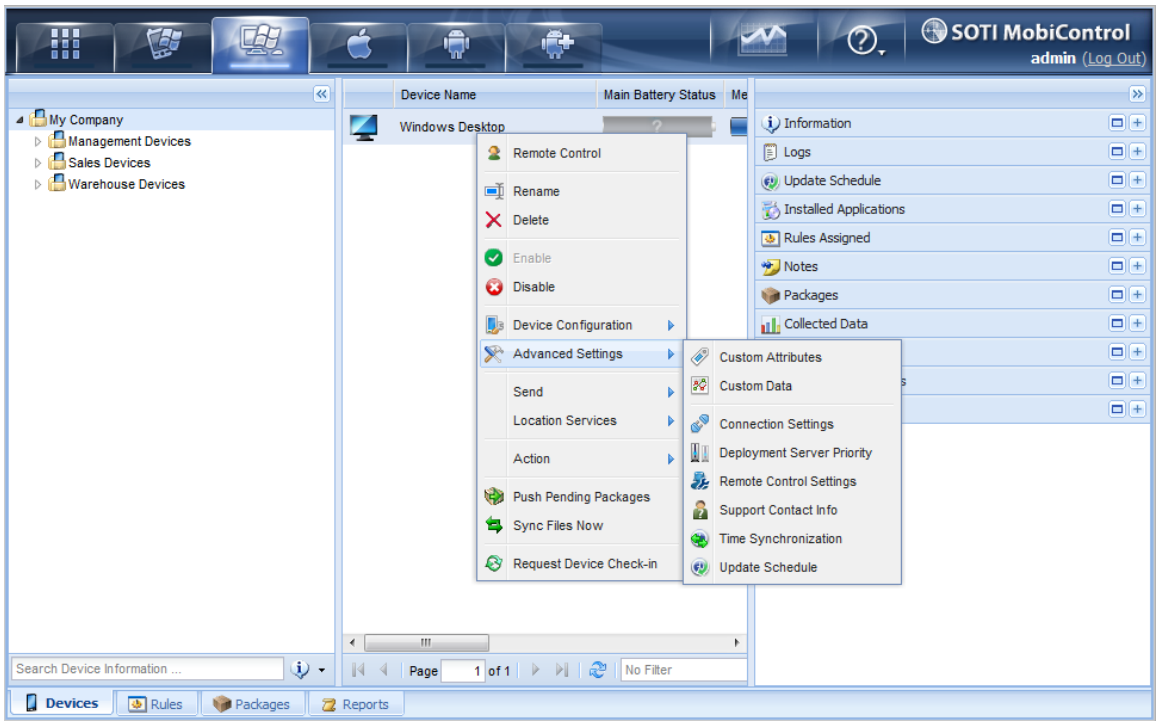
If users call support for their mobile device needs, configuring this option allows them to find the contact information reliably. Since this information is set centrally all information is updated once it's changed. Please see the "Windows Desktop Support Contacts Info" topic on page 858 for more information.

 Device Time Synchronization

This option allows you to enable time synchronization for a mobile device, allowing the device to update its date and time settings by periodically synchronizing them with an SNTP/NTP time server or the MobiControl Deployment Server. Please see the "Windows Desktop Device Time Synchronization" topic on page 859.

 Device Update Schedule

Adjust the interval at which the mobile devices contact the Deployment Server for new updates, configuration changes and packages. Please see the "Windows Desktop Device Update Schedule" topic on page 861.

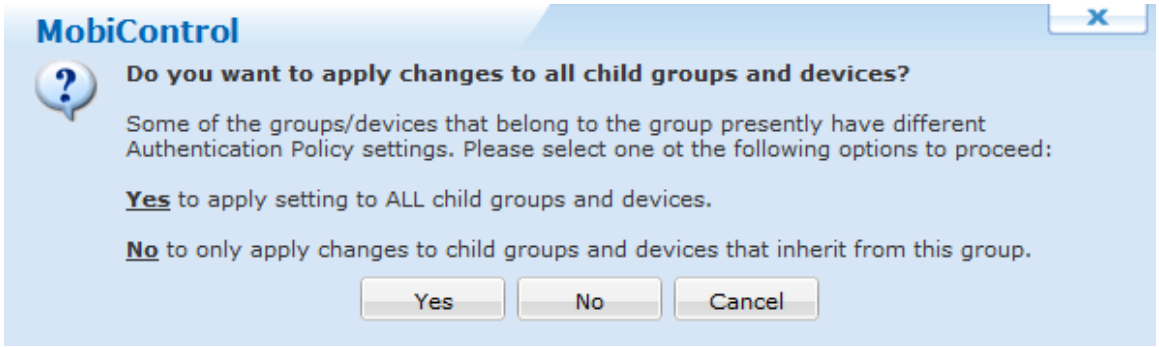


Device Configuration Menu options

Configuration Override Settings

Override settings allows you to create unique configuration settings at the current level which you have selected. This will override the settings that the device or group was previously inheriting from the parent group.

If the configuration settings are different at any sublevel (be it device or subgroup) then a confirmation prompt will allow you to choose whether the current setting(s) should be applied to all sub devices and groups or only the level that inherit configurations from this group.



Custom Attributes

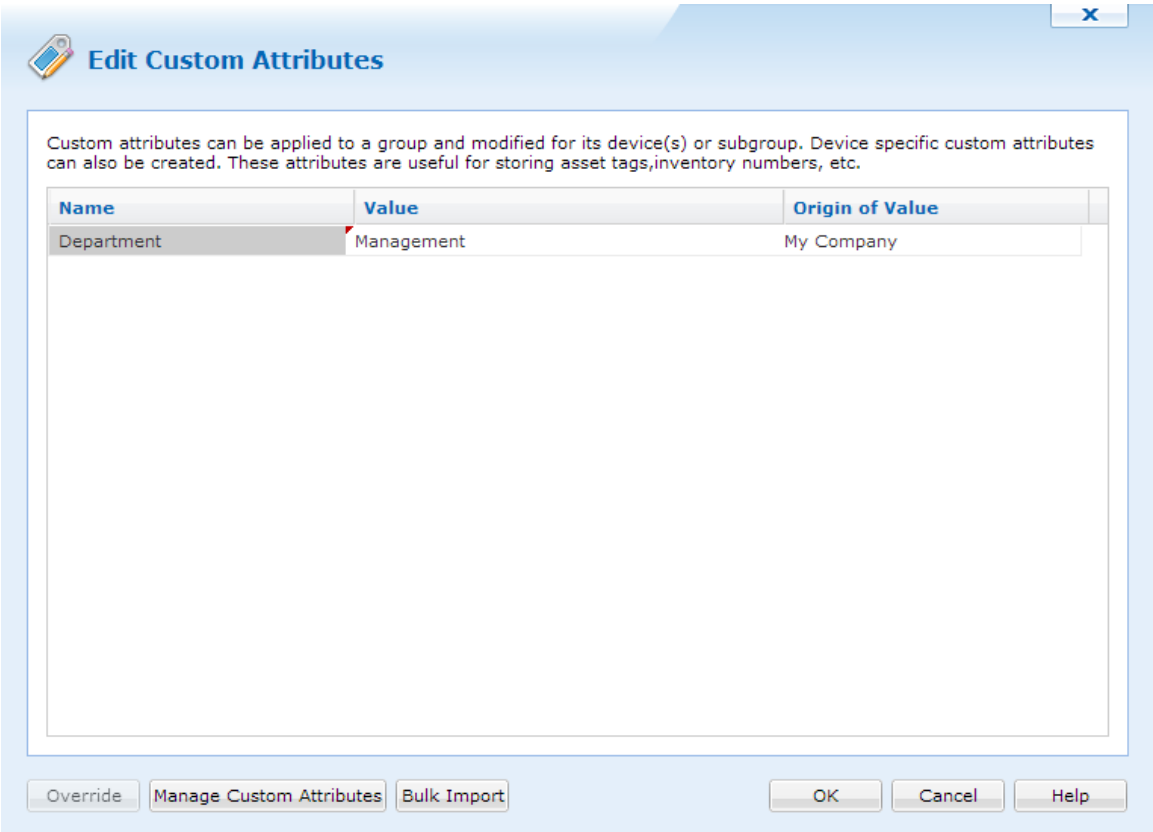
Custom Attributes allows us to create attributes to show in the information panel with our own data. This offers custom organization and labelling. For example, we can create a department attribute and put a different department for each device or device group.

Custom Attributes can also be propagated to devices so that they can be used in other applications and information.

NOTE:

Custom Attributes are available for all device types.

To set up Custom Attributes, right click a device or device group, go to Advance and click **Custom Attributes**.



Custom Attributes panel

The Custom Attributes panel has 3 columns: name, value and origin of value.

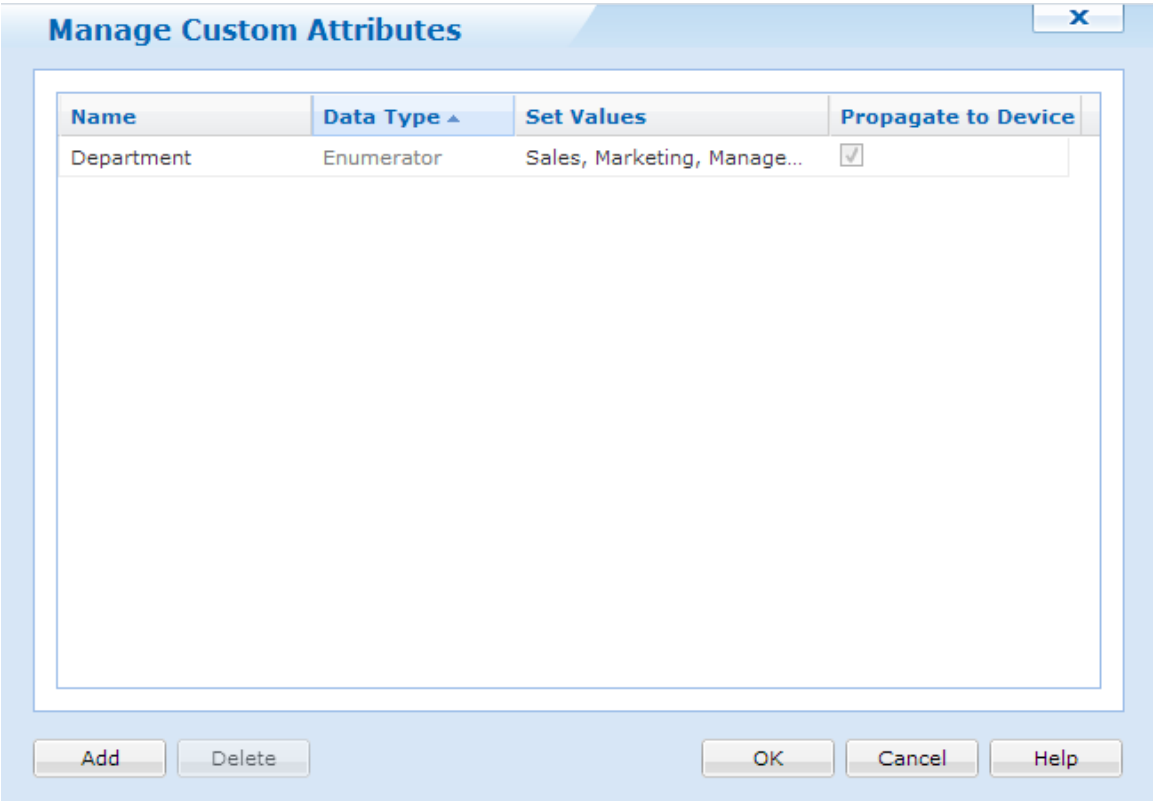
The name column shows the name of the Custom Attribute that will be shown in the info panel. Value contains the actual attribute for this field. Origin of value shows us where this field came from. For example, if Custom Attributes were set at the root level of the device tree, the origin of value will show the root level device group.

Clicking **Override** will change the origin of value to that where the device resides. This is useful if attributes change for each device. The Override button will change to **Remote Override** if we want to inherit the value from a parent group.

To create new attributes, click **Manage Custom Attributes**.

Manage Custom Attributes

When Manage Custom Attributes is clicked we a new dialog box appears. Here we will be able to create the Custom Attributes.



Manage Custom Attributes

Click  to add a new attribute.

When Add is clicked, a new row will appear. Clicking the field under name will allow us to name this attribute.

Data Types

There are 5 available data types to have for Custom Attributes:

- Text
- Numeric
- Date
- Boolean
- Enumerator

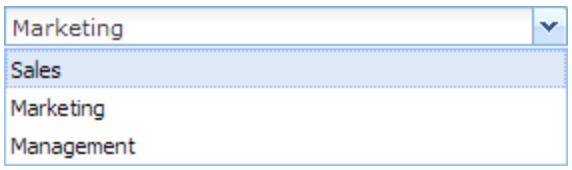
Text will allow us to create values with **letters and numbers**.

Numeric will allow us to create values with **only numbers**.

Date will allow us to set dates.

Boolean will create a checkbox for **yes or no / true or false**.

If we select enumerator, this allows us to create a drop down list when we set the attribute. To create the list, click the field in **Set Values** column. Here we can type the items we want in the drop down list. **Each value must be separated with a comma (,)**. For example, if we want to create a department attribute, we can have Sales, Marketing, Management. When we set this attribute, we will be presented with the drop down.



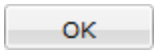
Enumerator Example

Propagate to Device

Checking this off will have MobiControl create the Custom Attributes in the pdb.ini file on the device. Applications can then read this file and pull the Custom Attribute value.

Bulk Import

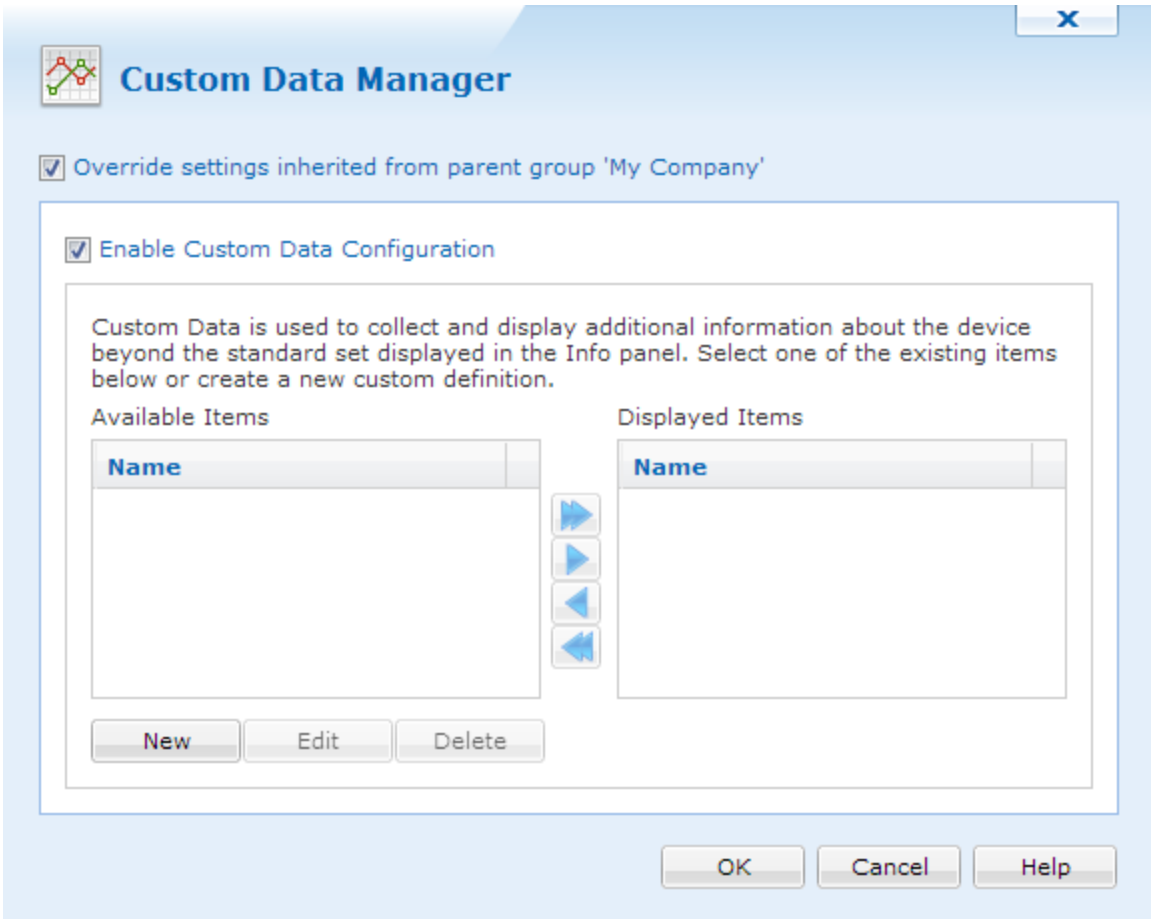
If there is a large amount of Custom Attributes to be inserted, we can do a bulk import so that everything is added at once.

Once everything is set, click 

to save and close the Custom Attributes.

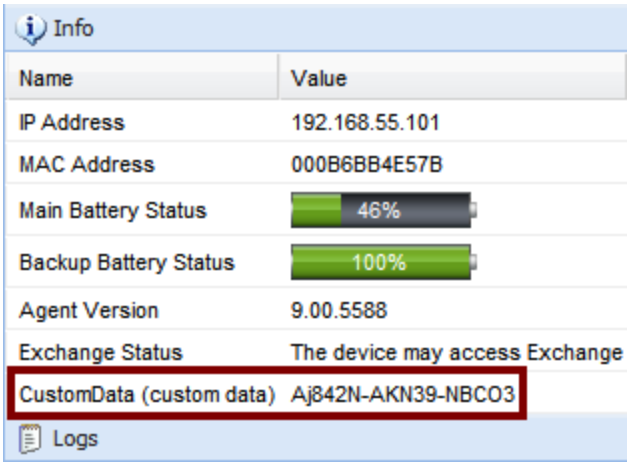
Windows Desktop Custom Data

The custom data feature in MobiControl allows users to create their own monitoring fields to be shown in the **Device Info** window. This can be useful for monitoring various aspects of third-party applications. Custom data values are refreshed from the device when the device reconnects to the MobiControl Deployment Server and periodically, while the device status is Online, based on the device update schedule.



Custom Data Manager

The Custom Data Manager is accessible by right-clicking on a device or group, then selecting **Configure Device(s)** and clicking **Custom Data**.



The Device Info panel in MobiControl Manager

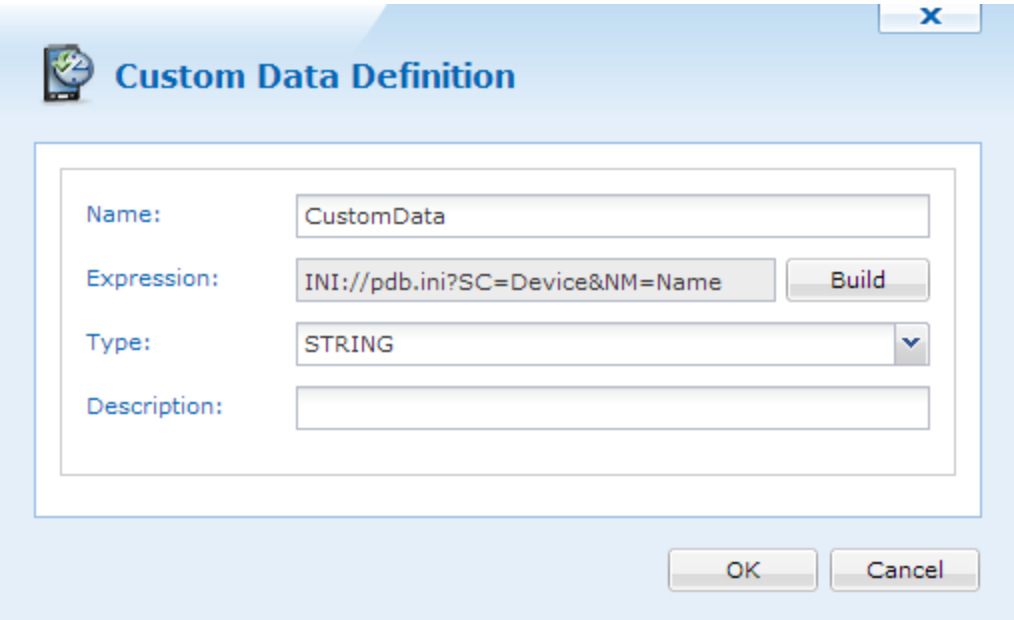
The following custom data types are available:

Type	Format and Description	Example
Text File	<Key>=TXT://\<FileName>?LN=<Value Number> Get the content of specified line of the text file (if LN is not specified, it assumes the first line)	TXT://\Device.log?LN=1
Registry	<Key>=REG://<GlobalKeyName>\<RegistryKey>?VN=<ValueName> Get a value from the registry. <GlobalKeyName> can be one of: • HKEY_CLASSES_ROOT • HKEY_CURRENT_USER • HKEY_LOCAL_MACHINE • HKEY_USERS	REG://HKEY_LOCAL_MACHINE\Software\Apps\SOTI\MobiControl?VN=Version
.INI File	<Key>=INI://\<FileName>?SC=<SectionName>&NM=<ValueName> Get a value from a Section in an .ini file.	INI://\SOTI\pdb.ini?SC=Device&NM=DeviceName
Exit Code	<Key>=EXE://\<Executable> [<ArgumentList>] Get the exit code of the executable	EXE://\windows\system32\calc.exe
STDOUT	<Key>=STDOUT://<Executable> [<ArgumentList>] Get the first line of STDOUT output of the executable.	STDOUT://cmd.exe /c dir
Static	<Key>=Text Enter the static value to display in the device info pane. This information is not based on any value on the device but based on user input.	OwnerName="X & Y Corporation, SalesDepartment"

Editing Custom Data

Configuration of custom data entries is performed through the Custom Data Manager which can be accessed by highlighting the device or the device group and selecting **Custom Data** from the **Configure Device(s)** option in the **Device** menu.

You can use the buttons in the **Custom Data Setting Manager** dialog box to add new entries, edit existing entries and change the order position of the custom data entries as displayed in the **Info** window.

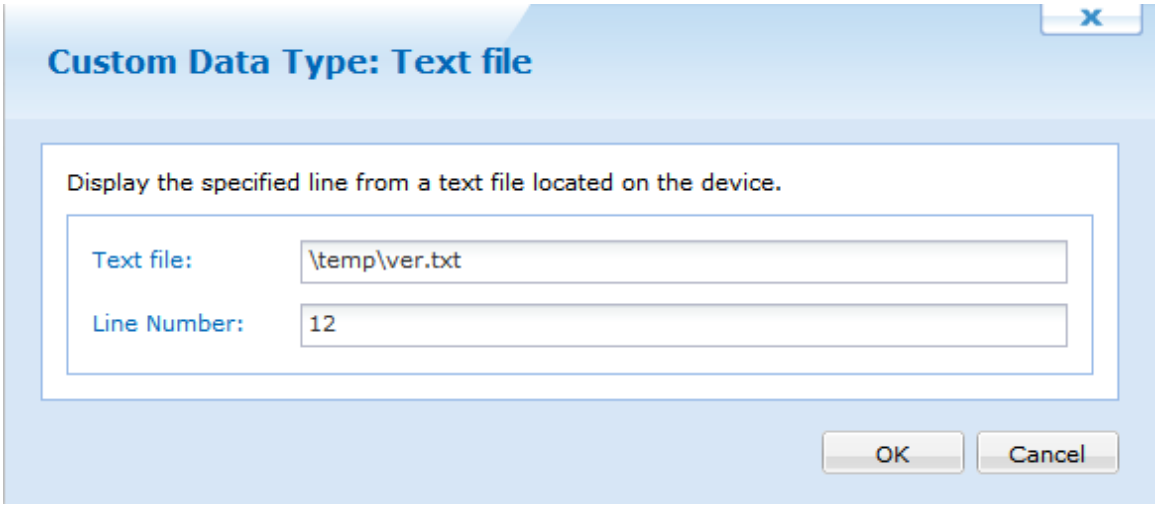


Custom Data Definitions window

The following table describes the fields in the **Custom Data Definition** dialog box.

Field Name	Description
Name	Name of the custom data field that you want to show in the device info pane
Expression	The build button can be used to create a definition which will be used to collect the custom data values.
Type	Default is set to "String." This setting is only recommended when doing custom data collection. Other options are "Float" and "Integer."
Description	A brief note describing the nature of the custom data query and its purpose. This description is shown in the device info pane when the custom data field is selected.

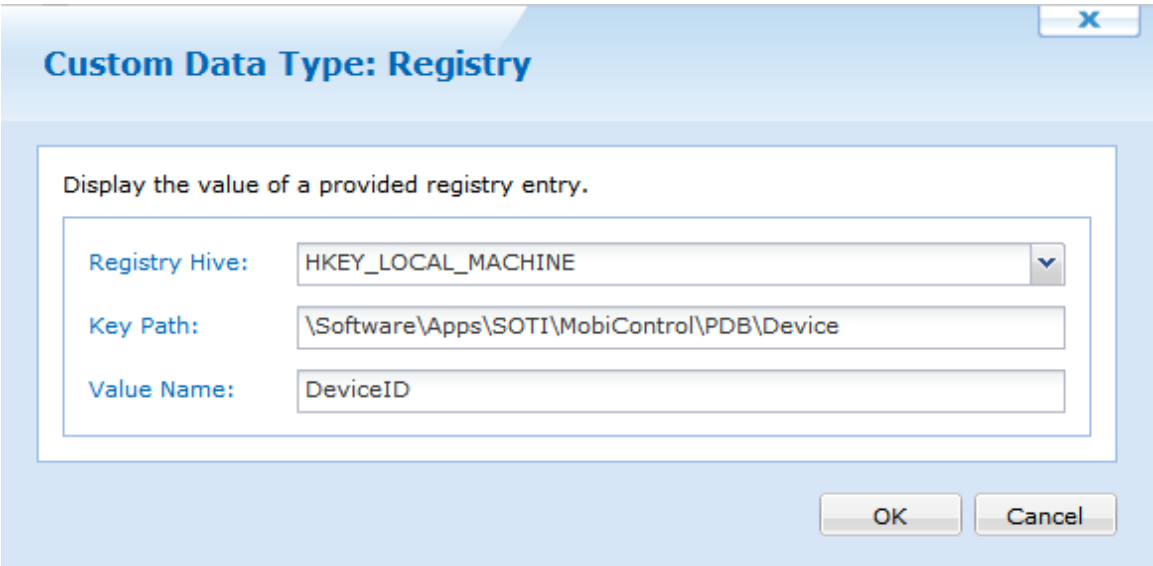
Custom Data: Text Files



The following table describes the fields in the **Custom Data Type: Text File** dialog box.

Field Name	Description
Text File Name	Specify the location of the text file on the mobile device.
Line Number	Specify the line number that should be read from the text file and displayed in the device info pane.

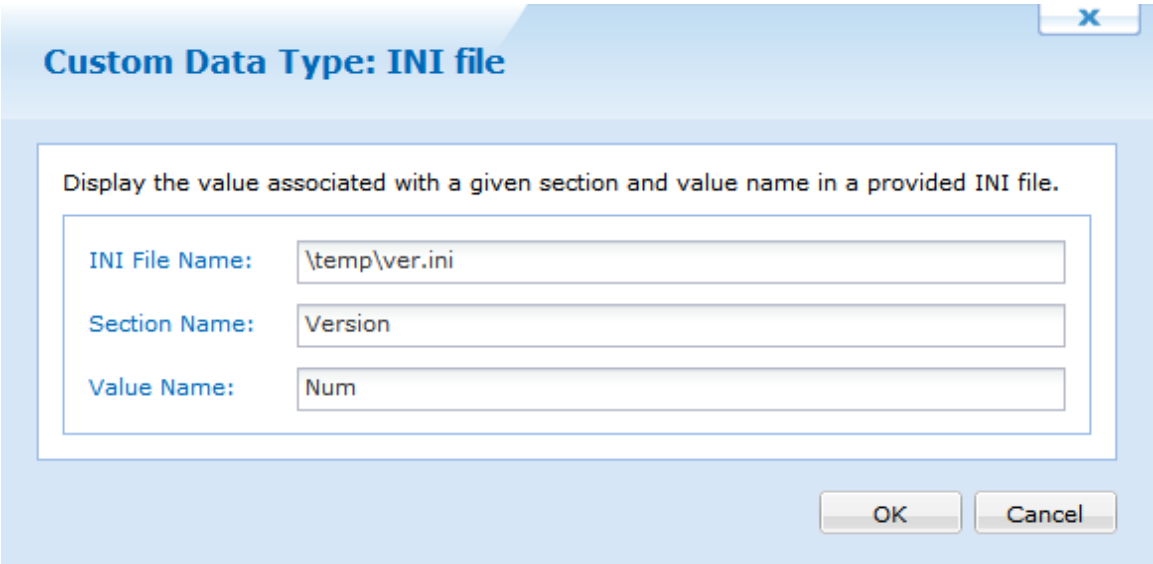
Custom Data: Registry



The following table describes the fields in the **Custom Data Type: Registry** dialog box.

Field Name	Description
Registry Hive	Specify the registry hive where the information is located.
Key Path	Specify the exact path of the value that needs to be read.
Value Name	Specify the name of the value that should be ready and displayed in the device info pane. **NOTE:** Only `REG_SZ` and `REG_DWORD` value types are supported.

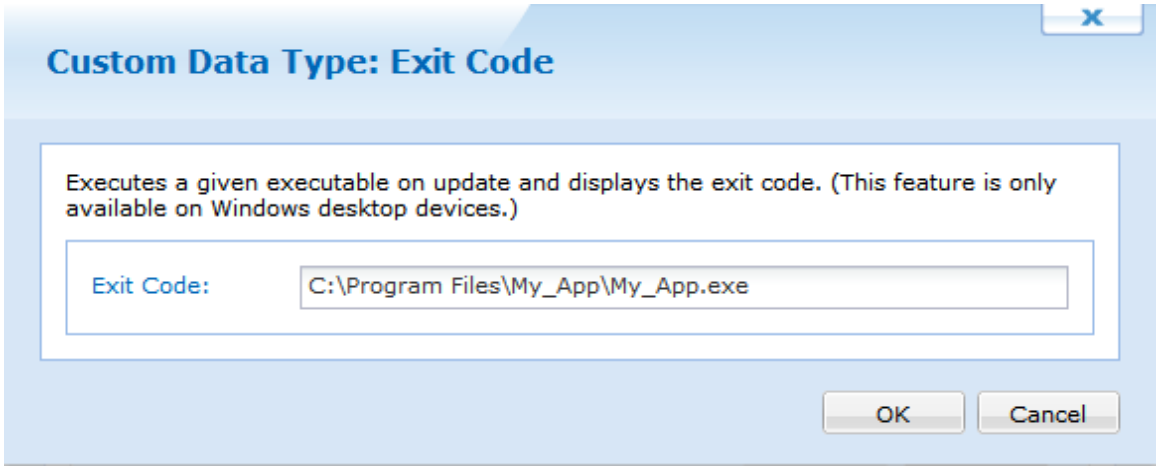
Custom Data: .Ini File



The following table describes the fields in the **Custom Data Type: INI File** dialog box.

Field Name	Description
INI File Name	Location of the `.ini` file on the mobile device
Section Name	Section from which the value should be read
Value Name	Value that should be read from the `.ini` file and displayed in the custom data field in the Device Info panel

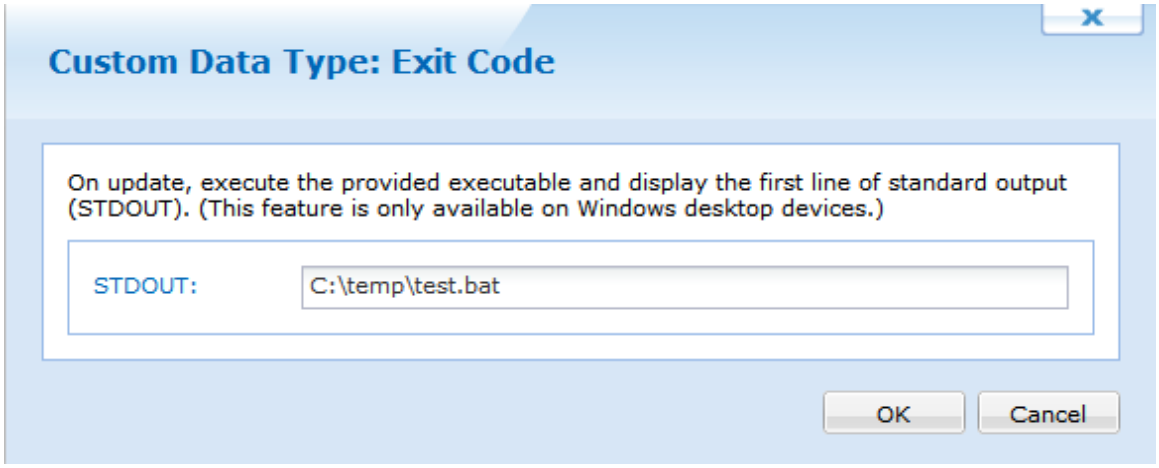
Custom Data: Exit Code



The following table describes the field in the **Custom Data Type: Exit Code** dialog box.

Field Name	Description
Command Line	Display the exit code of the application or command line instructions once they are executed.

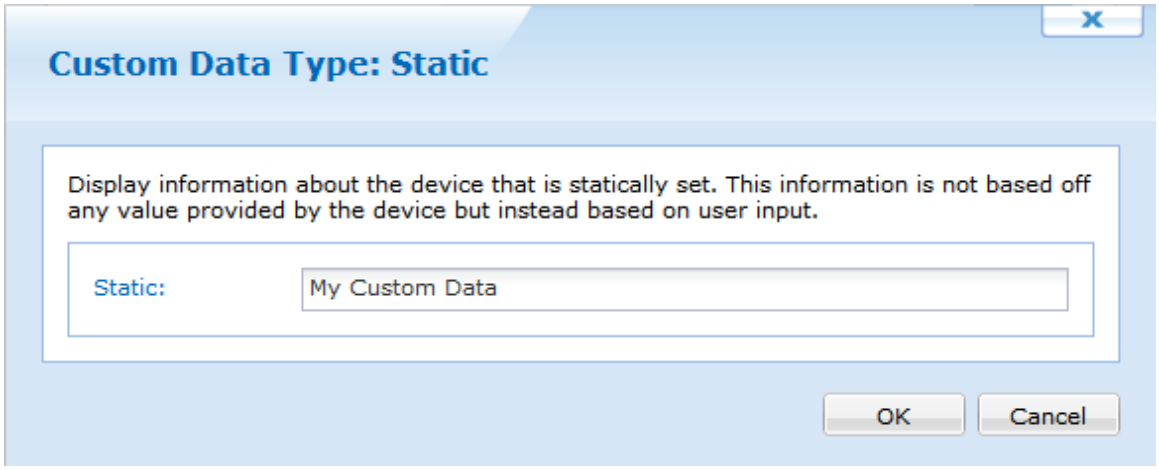
Custom Data: STDOUT



The following table describes the field in the **Custom Data Type: STDOUT** dialog box.

Field Name	Description
Command Line	Enter the command line instructions that should be executed and the first line of the return is displayed in the device info pane.

Custom Data: Static Data



The following table describes the fields in the **Custom Data: Static Data** dialog box.

Field Name	Description
Static Value	Enter the static value here to display in the device info pane. This information is not based on any value on the device but based on user input.

Embedded Query

A query string can be in another query string by using the format `%<KeyName>%`. The embedded query must be defined before the query. It works only in static type query and there has to be one static custom data type for every embedded query.

EXAMPLE:

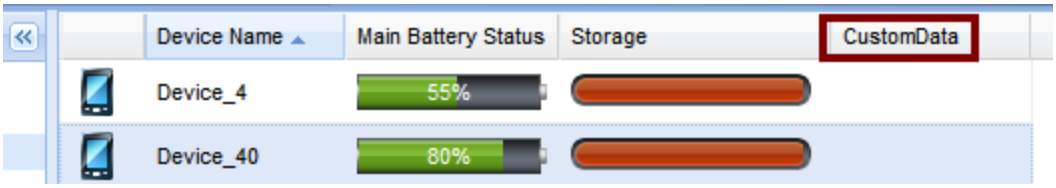
```
Key1=TXT://\RegLocationSSID.txt?LN=1
Key2=REG://%Key1%
```

Limitations

- All result values are limited to 250 characters. They will be truncated if this limit is exceeded.
- All Query Key Names are limited to 80 characters.
- All query strings (URLs) are limited to 250 characters.
- Typing "`STDOUT`" works on DOS and Desktop Agent. It doesn't work on CE and Pocket PC Agent.

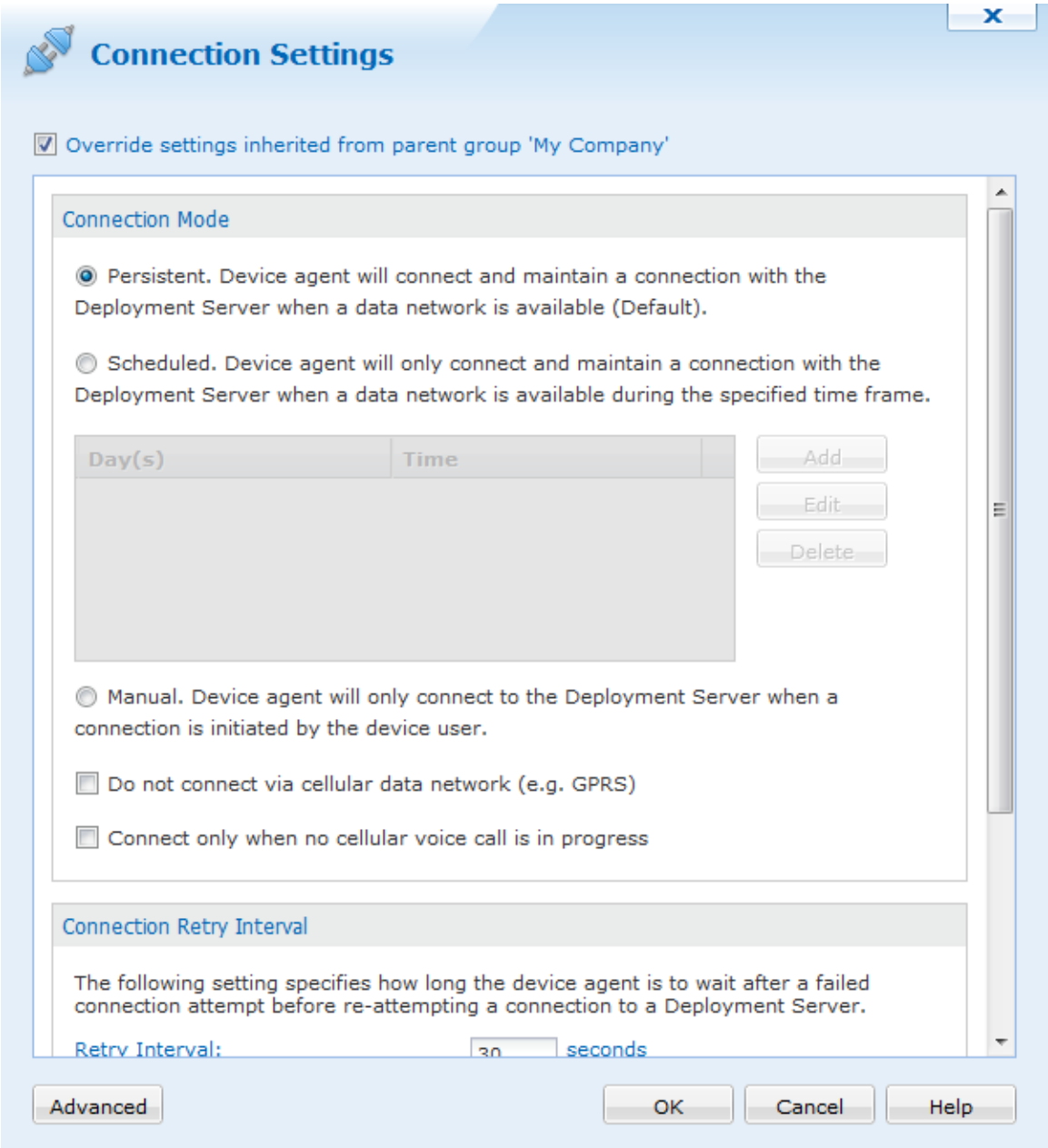
Custom Data Device Column

Once custom data has been configured, you can display or hide these custom data. Right-click on the device tree header or white space in the device tree and select **Custom Data**. You can also choose to display or hide the predefined data values displayed in the list.



Windows Desktop Connection Settings

To access the **Advanced Settings** dialog box, right-click on a device or device group, point to **Configure Device(s),** and select **Advanced Settings.**



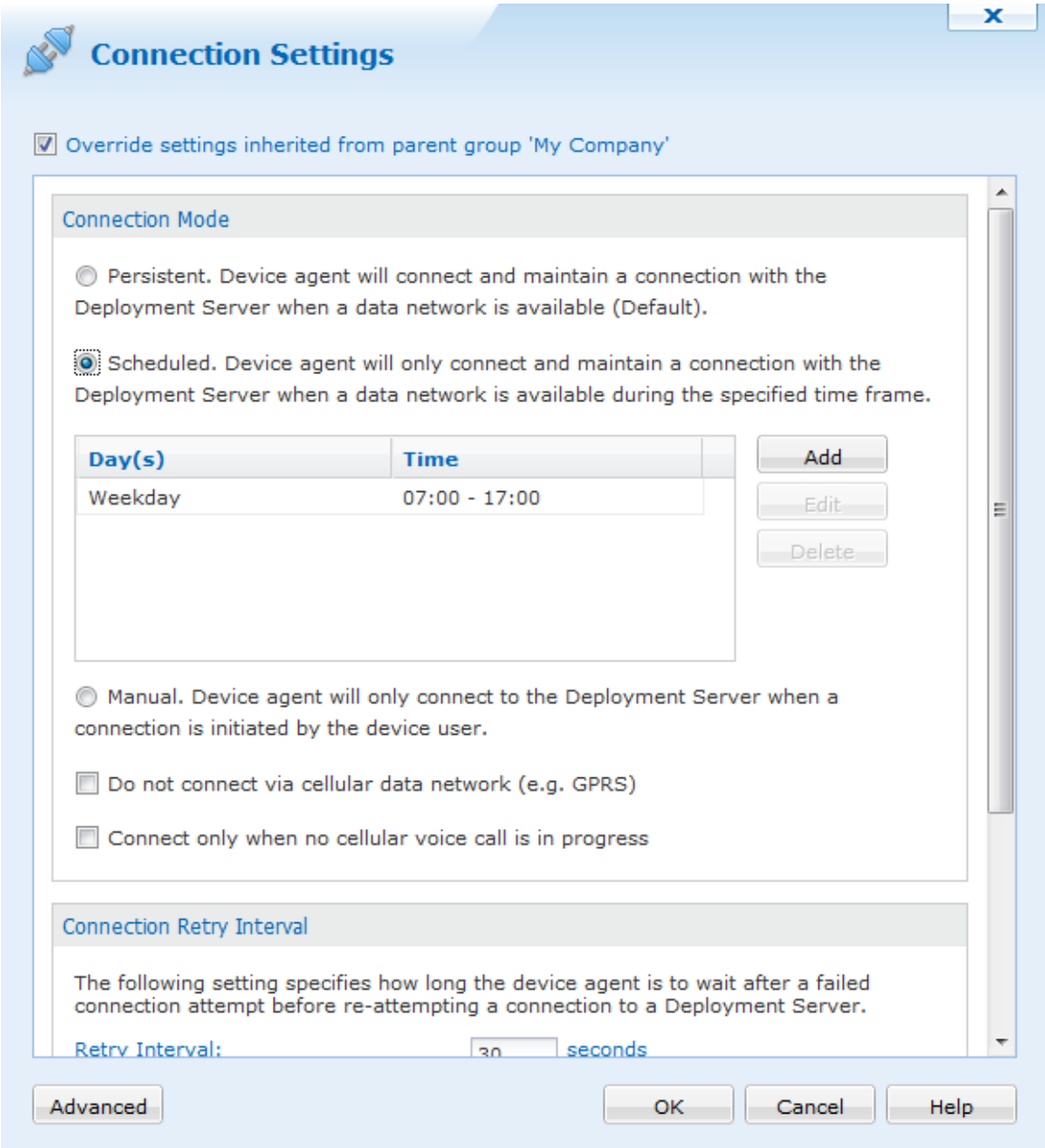
Connection Settings tab

Connection Mode

In any connection mode, the Device Agent does not force the mobile device to establish a network connection; it only takes advantage of an existing network connection.

Option	Description
Persistent	In this mode of operation the Device Agent will persistently try to establish and maintain a TCP/IP connection with the Deployment Server. This maximizes the amount

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>of time the device is connected to MobiControl, ensuring that it is able to quickly receive updates and available for remote control.
This is the recommended mode of operation for most installations.</td></tr>
<tr><td>Scheduled</td><td>In this mode of operation the Device Agent will only attempt to establish and maintain a TCP/IP connection with the Deployment Server during the defined time periods. Within the set time periods, the Device Agent operates in a "persistent" mode. Outside of the set time periods, the Device Agent will remain disconnected from the Deployment Server unless a connection is manually initiated by the device user.
This is the recommended mode of operation for installations where it is not necessary for the device to always be connected to the Deployment Server.
It is important that the time frame configured takes into consideration the device update schedule, and file synchronization schedules. These schedules can only be executed when the device is connected to the Deployment Server.
  TIP:
If you are experiencing aggressive battery consumption with the persistent connection mode, switch to the Scheduled mode, and specify a narrow time frame (e.g. 1–2 hours)</td></tr>
<tr><td>Manual</td><td>In this mode of operation the Device Agent will never automatically attempt to establish a connection to the Deployment Server. Connections must be initiated by the device user via the device configuration applet.
This is the recommended mode of operation for installations where only the remote help desk facilities of MobiControl are being used (not using deployment rules or file sync rules), and it is acceptable and/or required that the device user initiate the connection to the Deployment Server.
  NOTE:
The device must be connected to the Deployment Server in order for a remote help desk session to be established via the "TCP/IP(SERVER)" profile.</td></tr>
<tr><td>Do not connect via cellular data network</td><td>This option prevents the MobiControl Agent from connecting to the server via a data network on the device, e.g. GPRS. It can still connect using any other connection, e.g. Wi-Fi.
Don't use the Connect button on the Device Agent to test the device connection, since the MobiControl Manager (when the setting is implemented) will always allow a connection through GPRS. Instead you can use Disable device then Enable device on the MobiControl Manager to see if the device can connect through GPRS.</td></tr>
<tr><td>Only connect when no voice call in progress</td><td>When a voice call is in progress on a cellular phone device, the data service may or may not be available. To prevent the Device Agent from attempting to establish a connection while a voice call is in progress select this checkbox.</td></tr>
</table>

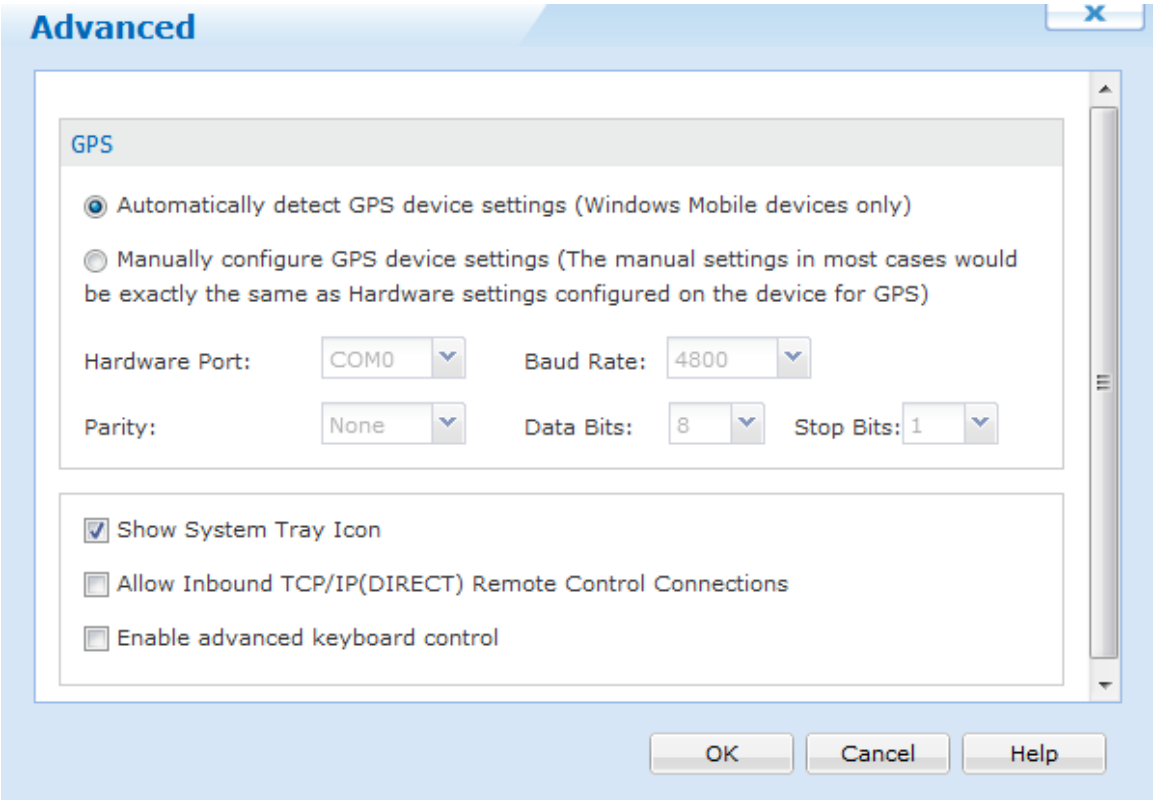


Add Schedule Entry settings dialog box

Connection Retry Interval

This setting determines how long the Device Agent should wait before trying to contact the Deployment Server again after a failed attempt. If your device will experience long periods disconnected from the Deployment Server, you should set this value high in order to prevent battery drain.

Option	Description
Allow Inbound TCP/IP(DIRECT) Remote Control Connections	This box needs to be checked if you intend to connect to your mobile device using the **TCP/IP (DIRECT)** connection mode. This option will enable the **Allow Inbound TCP/IP Connections** option in the Device Agent on the mobile device.



Advanced Settings Advanced tab

Advanced Device Agent Configuration

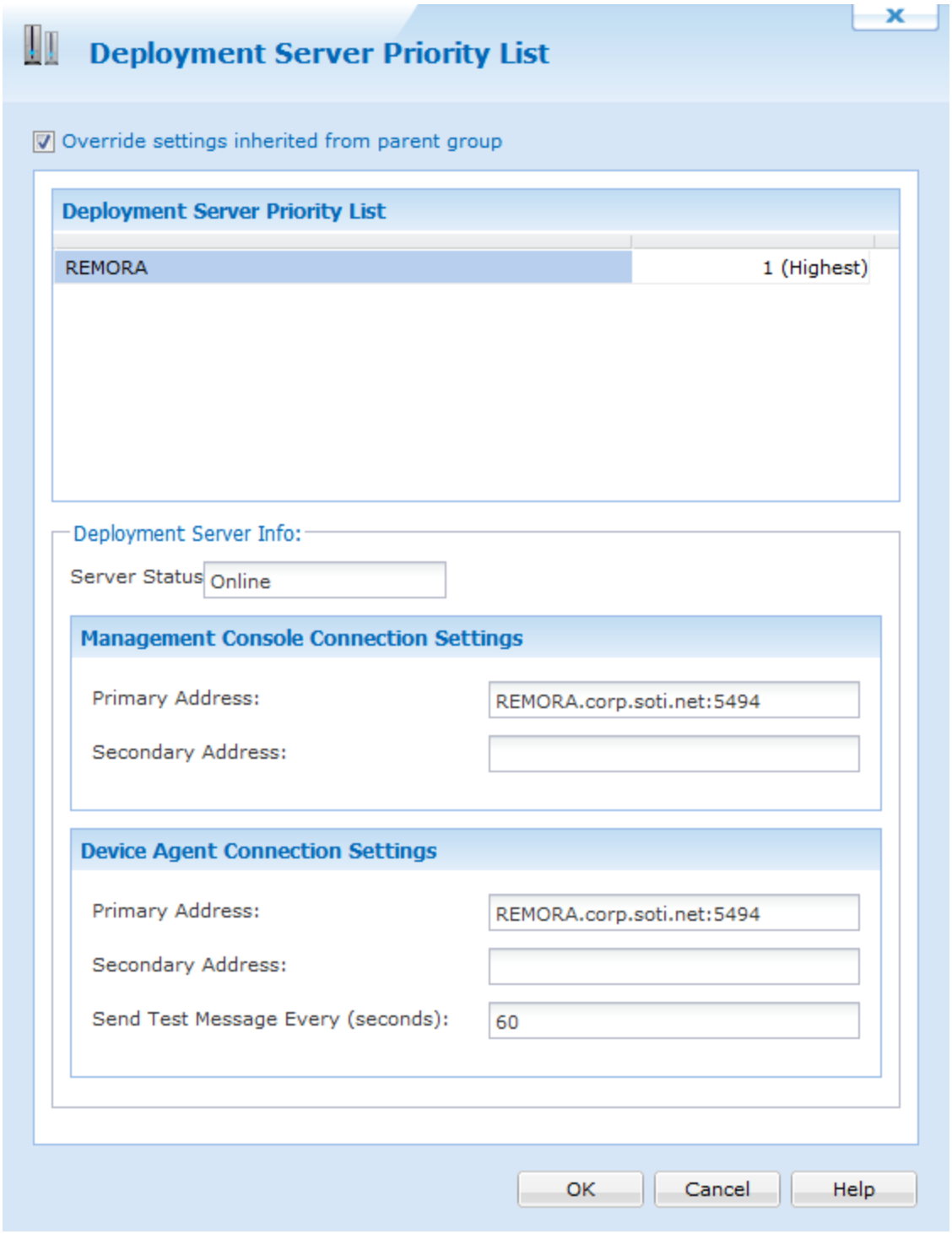
This set of options allows you to tune how the debug log files are managed on the device. Log management works by waiting for the log file to grow to a maximum threshold. Once the given threshold is met, the log file size is reduced down to the given minimum threshold by purging all the older entries.

Option	Description
Minimum Log File Size	Threshold size up to which the log file will be purged.
Maximum Log File Size	Threshold size, reaching which will trigger the log file to be purged to the minimum log file size
Enable Debug Logging (Normally Off)	Enables event logging on the mobile device. All MobiControl-related activity and events will be logged to a log file.The log file can provide vital information to IT support staff in diagnostics and resolving any issues that might have been reported for the mobile device with respect to MobiControl. The mobile device may operate more slowly with this option checked. **IMPORTANT:**

Option	Description
	Debug logs generate a large amount of file system traffic and as such, should only be enabled when you are debugging a problem. In particular, on Windows Mobile 5 devices, this intense logging activity can reduce the life of your flash memory if left on indefinitely.
Automatically Detect GPS Device	Automatically Detects the devices GPS settings, and uses those to locate the Device.
Manually Configure GPS Device	Enter the GPS Configuration settings for your specific devices. These settings can be obtained from the device manufacturer if you are un aware of them.
Show System Tray Icon	Enables the MobiControl Agent icon to be displayed on the device's system tray
Allow Inbound TCP/IP Connections	Enable the agent to listen and accept inbound TCP/IP remote control connections. When unchecked, you can remote control this device through "Remote Control Device via TCP/IP (SERVER)," but you cannot remote control this device by through "Remote Control Device via TCP/IP (DIRECT)."
Enable Advanced Keyboard Control	Enables the hardware keys on the device to be used by third party applications when the lockdown is engaged.

Deployment Server Priority

The **Deployment Server Priority List** dialog box allows you to specify the Deployment Server preferences for the devices. Priority one is the highest and five is the lowest. When a device is configured with more than one Deployment Server, it will try to connect to highest priority one first. If this server is not accessible, then it will try to connect to the next server available.



Deployment Server Priority List dialog box

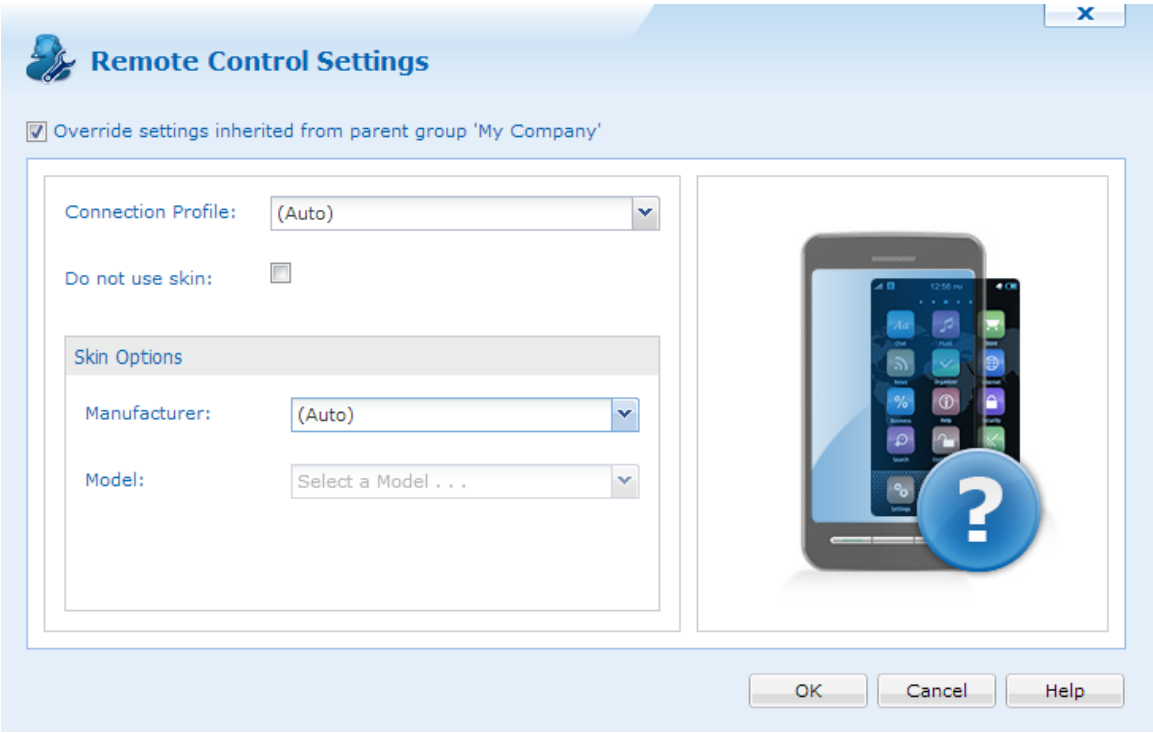
Multiple servers may be assigned the same priority level to establish a pool of Deployment Servers to balance the load of a large number of devices.

If you select "Not used," the selected devices will not connect to that Deployment Server.

Deployment Server priority is only applicable when you have installed multiple Deployment Servers using the same site name. Please see the "Configuring MobiControl Manager" topic on page 399 for more information.

Windows Desktop Remote Control Settings

In the **Remote Control Settings** dialog box, it's possible to select a device skins and connection profiles. Skins for these devices should appear automatically depending on the device agent created.



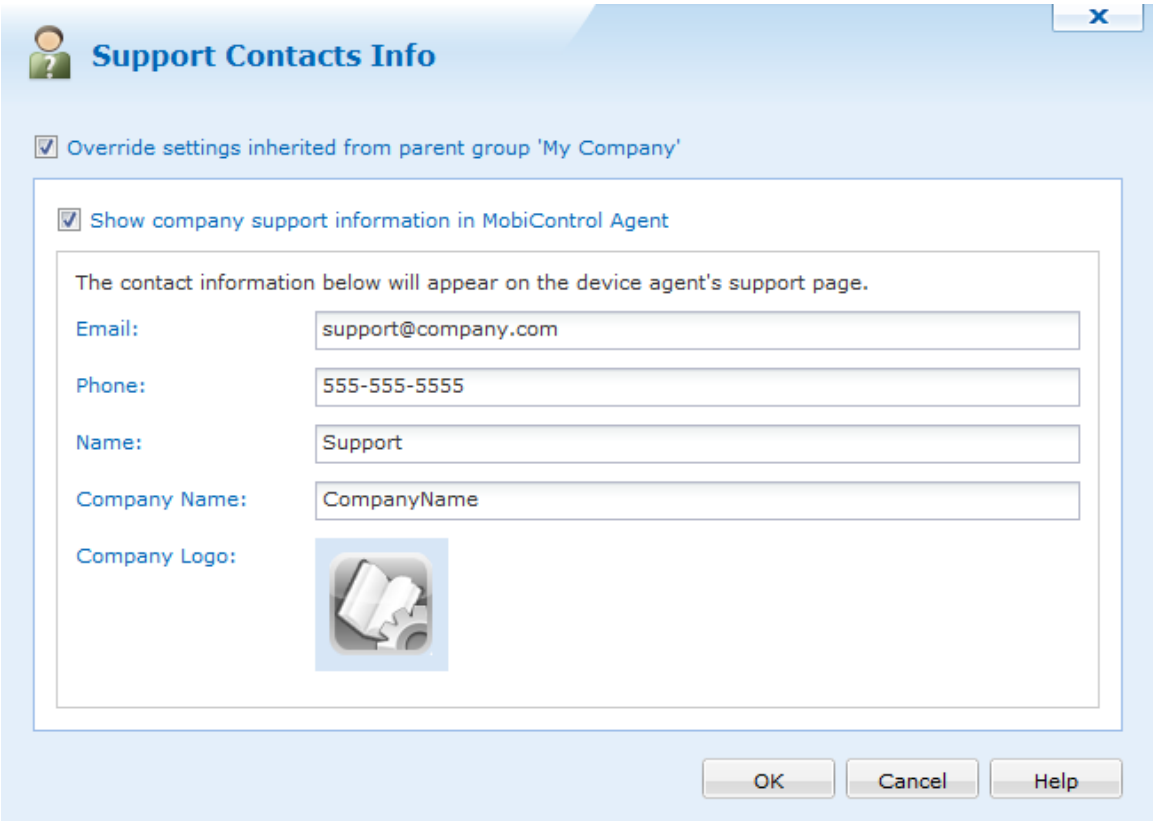
Remote Control Settings dialog box

The following table describes fields in the **Remote Control Settings** dialog box.

Field Name	Description
Connection Profile	This field allows the user to configure the type of connection that will be used for remote control sessions. The available connection types are TCP/IP(SERVER) **(recommended)**, TCP/IP(DIRECT), and <Prompt on Connect>. • The **TCP/IP(SERVER)** setting offers the broadest support for remote control connections. For example, situations where the mobile device does not have a public IP address. When a TCP/IP(SERVER) remote control session is established, the session is bridged through the MobiControl Deployment Server (i.e. The device connects to the MobiControl Deployment Server on TCP port 5494 and the desktop MobiControl Remote client connects to the Deployment Server on TCP port 5494). Since this connection goes through the Deployment Server the performance is generally not as fast as a direct TCP/IP connection, however, it offers improved security as it does not require the mobile Device Agent to accept unauthenticated remote control connections. An example of where this type of connection is required because of network topology is when the mobile devices are behind a firewall and do not have unique public IP addresses. • With the **TCP/IP(DIRECT)** setting, the MobiControl desktop software will open a direct Wireless/Wired TCP/IP connection to the mobile device (i.e. on TCP port 5494). A LAN-based wired/wireless TCP/IP connection generally provides the best performance, however it requires that the mobile Device Agent accept unauthenticated remote control connections unless SSL Security is enabled. Please see the "Windows Mobile Connection Security" topic on page 649.
Do not Use Skin	Checking this off will remove the skin from the device when remote controlling it.
Manufacturer, Model, and Skin Preview	A skin is an image of the body of your mobile device, which mimics the physical device on your desktop screen. Displaying your device in a skin gives you access to most of the physical buttons of the device. It can be useful in training or presentations. Skins should automatically be applied to devices depending on the device agent created. If another skin is wanted to be used, select the manufacturer and model of your device to have its skin be displayed in a remote control session. Skins for most Windows Mobile, Pocket PC and CE .NET based mobile devices are available. We are always adding new skins to our online collection, but if your device is not listed, please contact us to let us know which device you are using.

Windows Desktop Support Contacts Info

The Support Contacts Info panel allows us to set contact information when a user opens up the MobiControl agent on their device. Information that we are able to configure are Email, Phone, Name, Company name and a company logo.



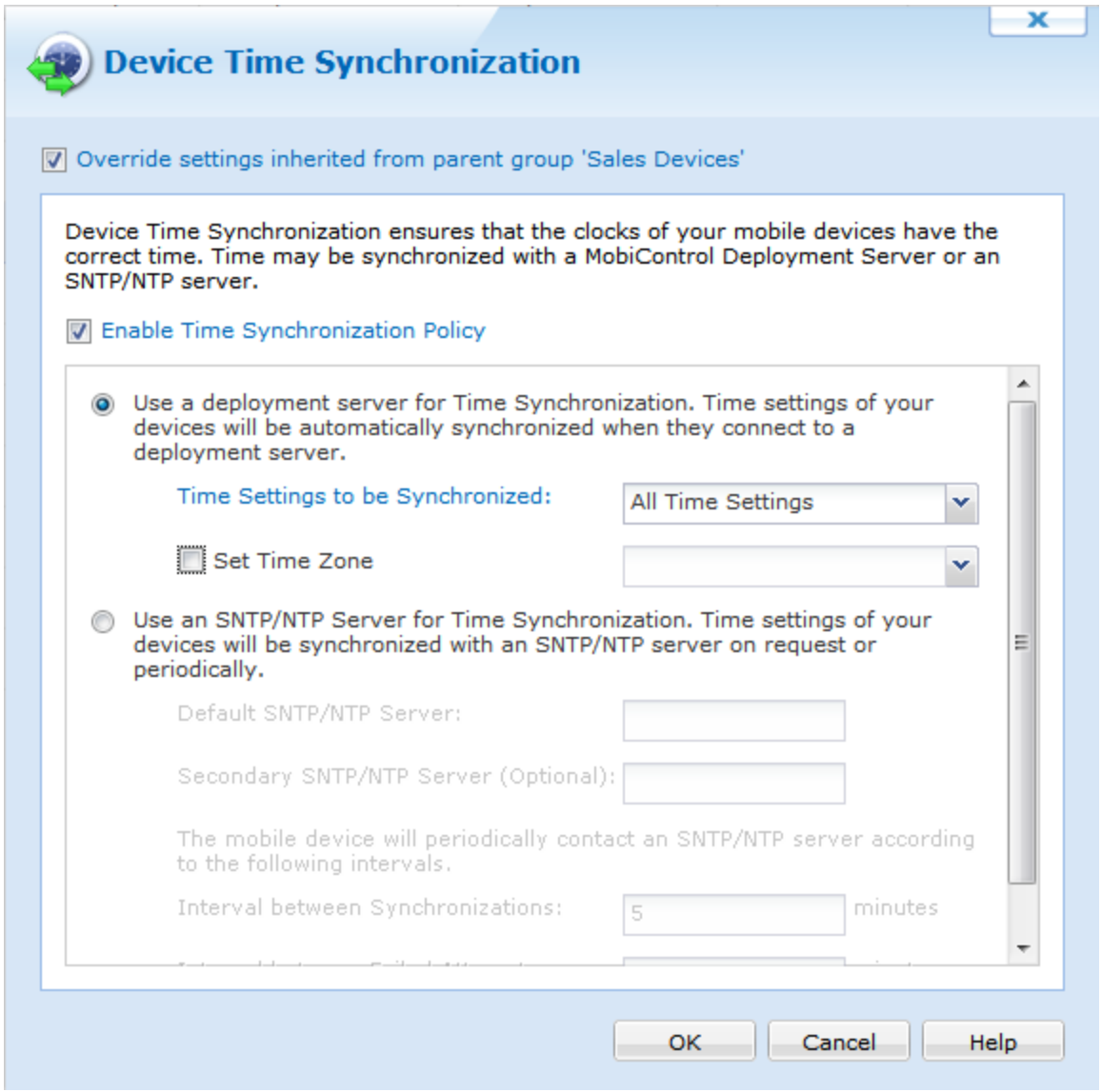
Support Contacts Info dialog box

When each of the fields are set and OK is pressed, this information will then be sent down to the devices where this was configured on. When a user opens up their MobiControl agent and goes to the support info tab, they will be able to see the appropriate information.

Device Time Synchronization

This feature allows you to enable time synchronization for a mobile device, allowing the device to update its date and time settings by periodically synchronizing them with an SNTP/NTP time server or the MobiControl Deployment Server.

To configure the time synchronization settings for a device or device group, select the device or group in the device tree and click **Device,** click **Configure Device(s),** and click **Time Synchronization.**



Device Time Synchronization dialog box

Time Synchronization Settings

There are three different modes available for time synchronization:

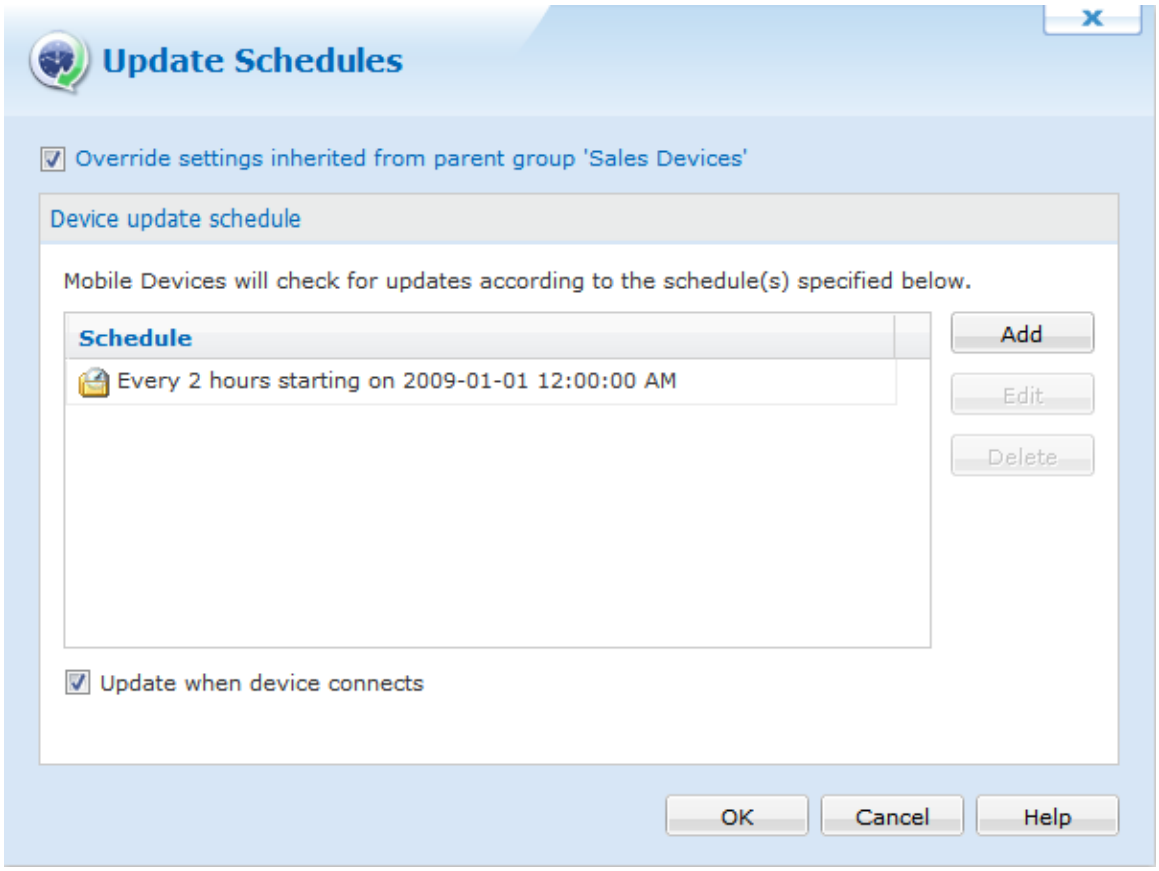
Option	Description
No Time Synchronization	The device time is not synchronized with any server.
Use a Deployment Server for Time Synchronization	The device will synchronize its time with a MobiControl Deployment Server when it connects to it. The time settings available for synchronization include Time Only, and All Time settings: • The **Time Only** option will result in the date and time being synchronized (but not the time zone) • The **All Time Settings** option will sync all of the time settings including DST, time zone, date, and time. • The **Set Time Zone** option to set the time zone for mobile devices which are in a different time zone than the Deployment Server. You can use this on device level or group level.
Use an SNTP/NTP server for Time Synchronization	The device will synchronize its time with the SNTP/NTP server(s) specified in the **Default SNTP/NTP Server** and **Secondary SNTP/NTP Server** fields. When this mode is selected, the option to synchronize automatically becomes available. With automatic synchronization enabled, the device will synchronize its time according to the interval specified in the **Interval between Synchronizations** field. If an automatic synchronization fails, the device will retry after the time interval specified in **Interval between Failed Attempts** has elapsed. **NOTE:** SNTP/NTP Server does not synchronize DST settings. It's similar to time only.

Windows Desktop Device Update Schedule

The device update schedule specifies when the device(s) should query the Deployment Server(s) for updates. Updates may include the addition, update, or removal of packages and modifications to device settings.

If the Deployment Server determines there are pending updates for the device, it immediately sends them to the device. The device also sends the Deployment Server a summary of its installed packages and settings. If the Deployment Server identifies an inconsistency, such as a previously-installed package that is missing on the device, the Deployment Server will re-install the package.

The initial device update schedule is specified by the add devices rule used to add the device(s) to the system. You may edit the schedule for an individual device or a group of devices that have been added to the system by selecting the target device or group in the device tree view in the main console window and selecting **Update Schedules** from the **Configure Device(s)** sub-menu.



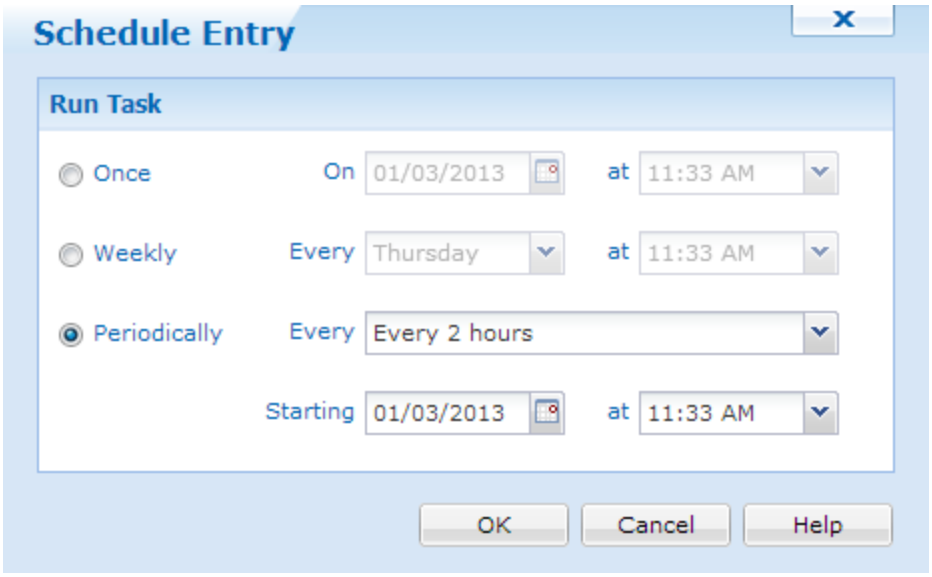
Device Update Schedules dialog box

The following table describes the **Device Update Schedules** dialog box:

Field Name	Description
Add	Select **Add** to specify additional update intervals. The **Schedule Entry** dialog box will be displayed. **EXAMPLE:** To sync a device twice a week, Monday at 06:00 and Friday at 19:00, create two weekly schedule entries.
Edit	Select **Edit** to modify an existing schedule entry. The **Schedule Entry** dialog box will be displayed.
Delete	Select **Delete** to permanently remove an update schedule entry from the dialog box.
Update when device connects	Select this check box to have the device(s) check for updates whenever they connect to a Deployment Server, that is, at every transition from offline to online. If this check box is not selected, the device(s) will only check for updates according to the schedule defined above.

Schedule Entry

The **Schedule Entry** dialog box allows you to specify schedule entries as one-time or periodic events.



Schedule Entry dialog box

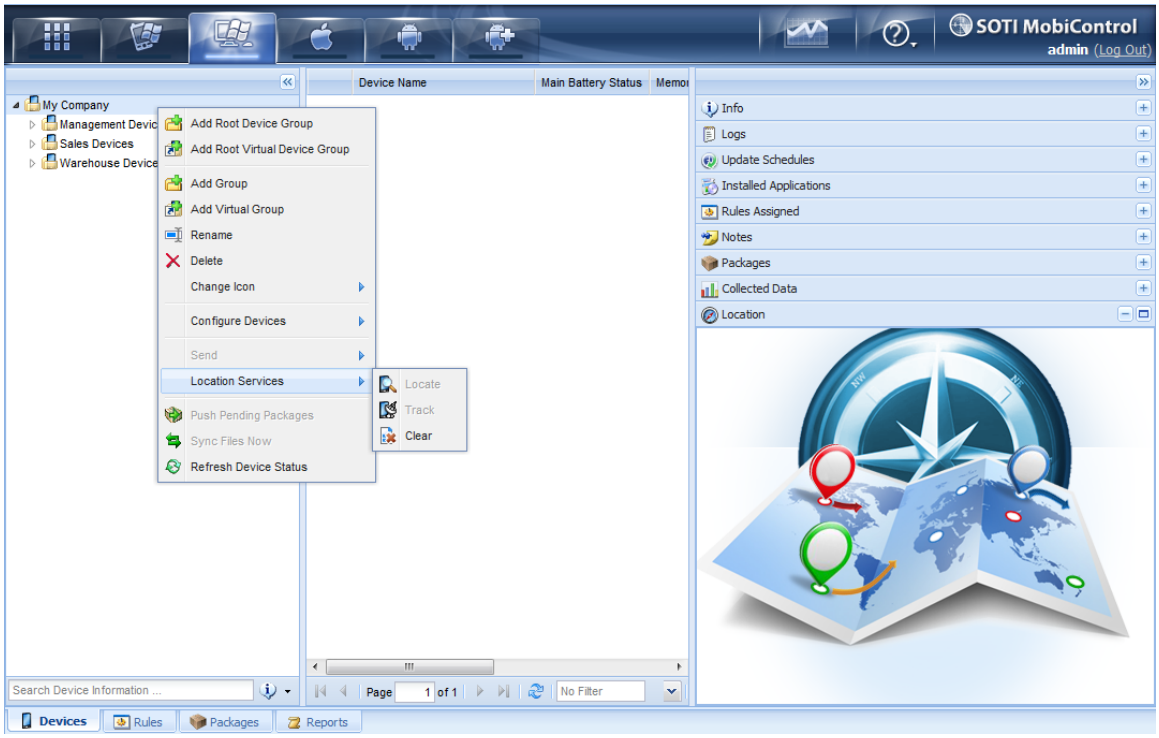
Field Name	Description
Once	The device will check for updates once at the specified date and time.

Field Name	Description
Weekly	The device will check for updates once a week, on a specific day at a specific time.
Periodically	The device will check for updates periodically, at the specified interval from the set start date and time.

Windows Desktop Location Services

MobiControl's Location Services provides the ability to locate and track mobile devices that are equipped with a GPS receiver that is internal or external to the unit. In order to locate a device, the GPS must be enabled and correctly configured on your device. The GPS determines the current location based on its position relative to orbiting satellites. In order for this to happen, the device requires a clear view of the sky. Determining location may not be possible if the device is inside buildings or has an obstructed view of the sky.

You can activate Location Services for a device in MobiControl by right- clicking on a device and selecting the **Location Services** option from the menu. The first time you select an option from the Location Services menu for a device, it will automatically use the next available license. If there are no more licenses available, you will be notified to contact SOTI for information on acquiring additional licenses for Location Services.



Windows Desktop Location Services

Please See the "Contact Us" page to contact us for more details on acquiring additional licensing.

NOTES:

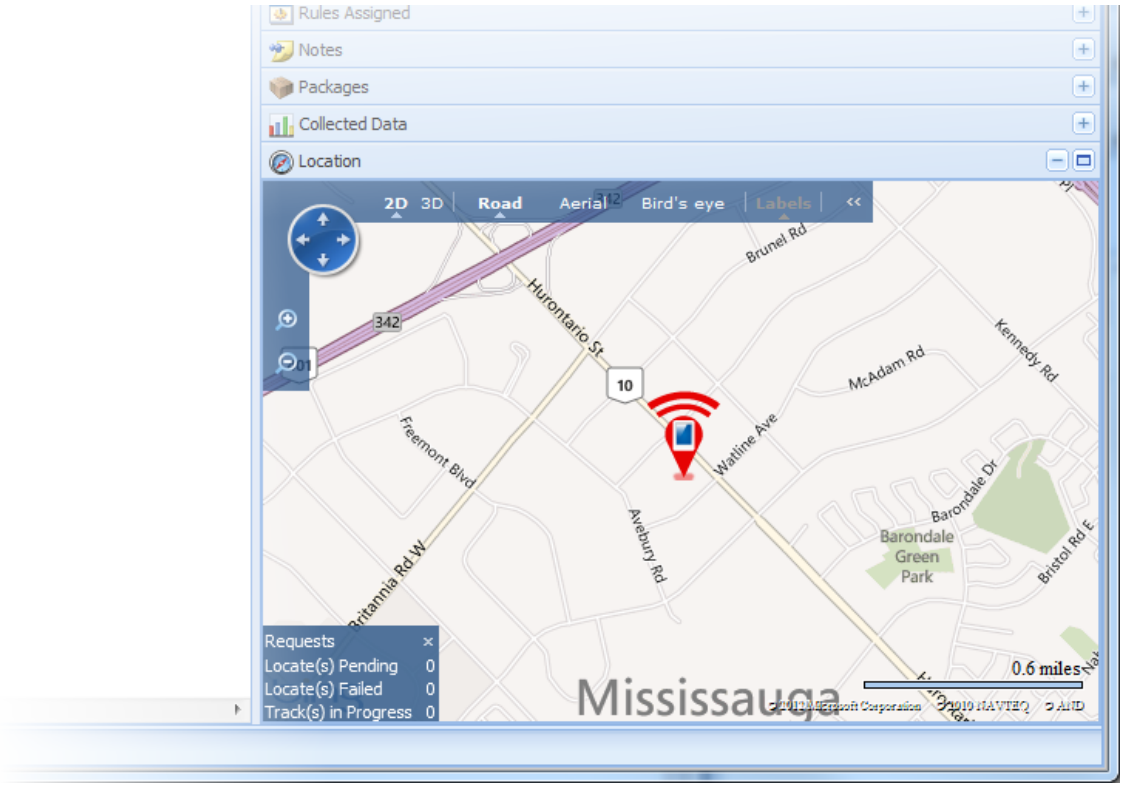
- When using Location Services in MobiControl to track devices, Internet Explorer 7 or higher is required.
- The Current Format for Regional and Language Options on your PC MUST be compatible with Bing Maps. Click here for a list of supported Bing Map control settings.

Windows Desktop Locate Feature

To use the Locate feature in MobiControl's Location Services, right-click on the device you wish to locate, select **Location Services,** and click **Locate.**

The locate feature will use the GPS unit associated with your mobile device to determine the current latitude and longitude of the device. These coordinates are returned to MobiControl and displayed in the Location panel using Microsoft's Virtual Earth. The coordinates plotted in the Location panel represent the exact position of the device at the time of the request. To follow the position of the device in real time, use the **Track** option under the **Location Services** menu.

You can locate the position of multiple devices at once: select the parent folder or hold the CTRL key and select all the devices you wish to locate, right-click, select **Location Services,** and click on **Locate.** In order to use the Locate feature, the device(s) must be online and communicating with the MobiControl Deployment Server. The status of the current (and completed) Locate and Track commands is displayed in the lower left hand corner of the screen.



Location Services locate user interface

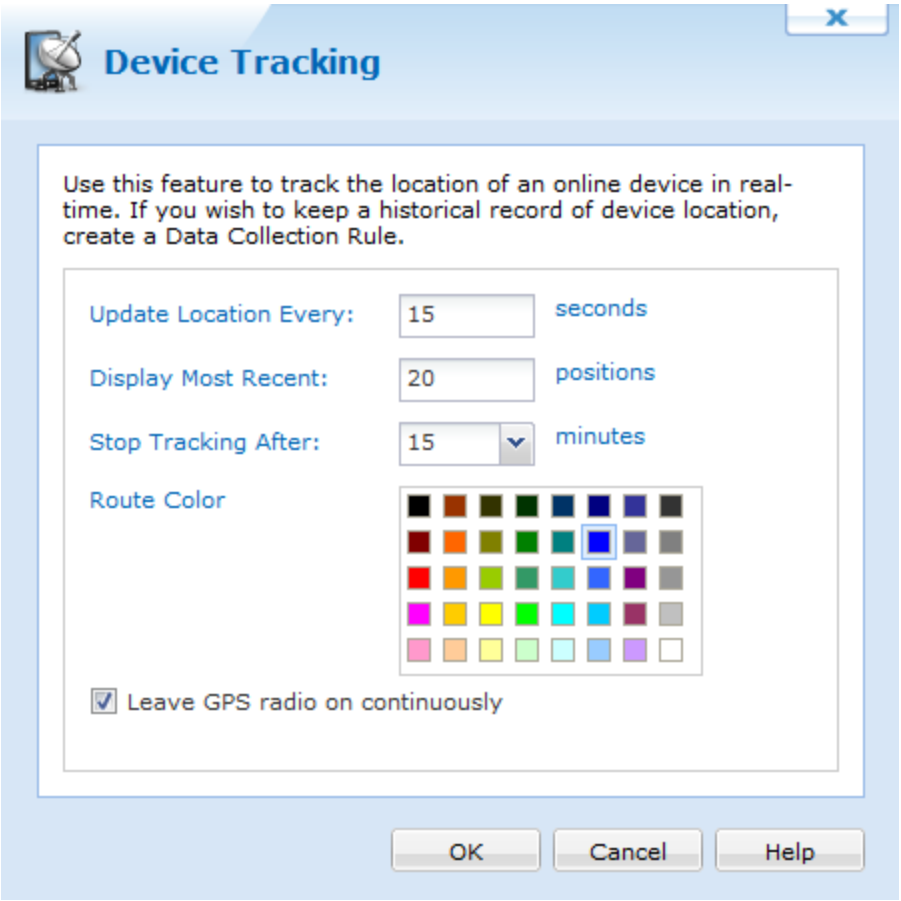
Th

NOTE:

If the MobiControl Manager is behind a proxy server and you are unable to use Location Services, please run the following command through the **Start** menu then **Run**:
`netsh winhttp set proxy -server="http=<ProxyServerIP>: <Port>; https=<SSLProxyServerIP>: <Port>"` (on Windows Vista, **with no spaces between the quotation marks**.)
This command will update the WinHTTP service with the settings from Internet Explorer.

Windows Desktop Tracking

To use the Track feature in MobiControl's Location Services, right-click on the device you wish to track, select **Location Services,** and click **Track.**



Device Tracking dialog box

The track feature will use the GPS unit associated with your mobile device to determine the current latitude and longitude of the device at a given schedule and send the co-ordinates back to the MobiControl Deployment Server. These co-ordinates are then displayed in the Location panel using

Microsoft's Virtual Earth. The co-ordinates plotted in the Location panel represent the exact position of the device at the time of the request along with where the device has been since the request was initiated. To view where the device has been in the past, you need to use the show history option within MobiControl's Location Services.

In order to use the track feature, the device must be online and communicating with the MobiControlDeployment Server.

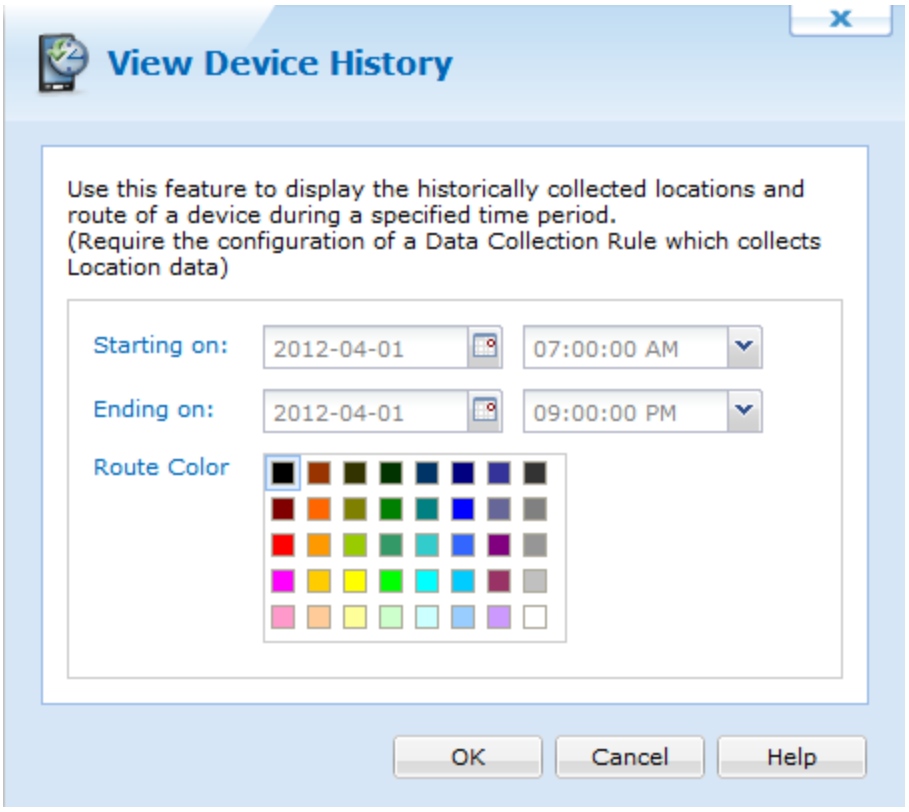
The following table describes each field in the dialog:

Feature	Description
Update Location Every	Set a time interval in seconds (5–86400) for how frequently you would like to have the device location reported.
Display Most Recent	Choose a value to represent the number of recent positions (maximum 100) that you would like to see plotted on the map of the device(s) that you will be tracking.
Stop Tracking After	Set the time interval in minutes (5– 60) for when you would like to end tracking the device.
Route Color	Identifies the device route you will be tracking
Leave GPS radio on continuously	For faster response time from the GPS radio on the device, you should enable this check box. The device's GPS radio will constantly be on.

Windows Desktop Show Tracking History

The show history feature will use the GPS unit associated with your mobile device, allowing you to view where the device has been over a given period of time. To use this feature, you need to set up a data collection rule that collects the location information from the device on a given schedule. The data will be sent back to the deployment server, or, if there is no active data connection on the device, it will be collected and stored in a temporary file and then sent back to the server the next time the device connects. The show history feature does not require the device to be online and communicating with the MobiControl Deployment Server. You can plot information from the history that has been transmitted back to the server during the last active connection.

To use the show history feature, right-click on the device you wish to view, select **Location Services,** and click **Show History.** You will then be prompted to enter the time period for which information is desired, and the route color. Once this is filled in, click **OK** and the path will be plotted.

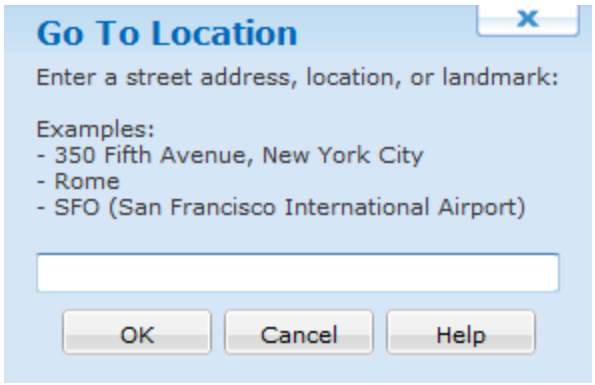


View Device History dialog box

Feature	Description
Starting On	Enter the date and time that you wish to start.
Ending On	Enter the date and time that you wish to stop.
Route Color	Select the color to be used on the map when connecting the co-ordinates.

Using Go To Location

Go To Location allows you to quickly centre and zoom the map to a specific location. Go To Location is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "Windows Desktop Location Services" topic on page 864 for more information.

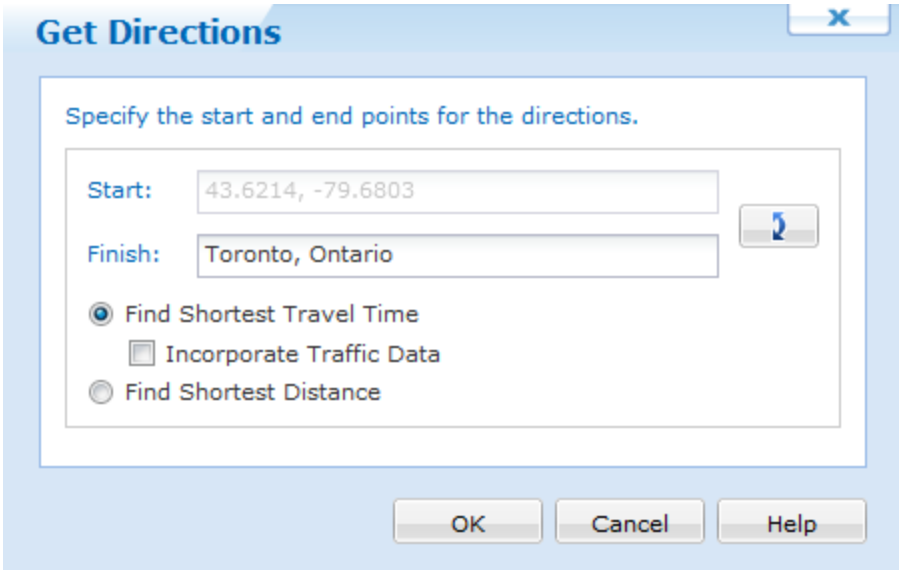


Go To Location dialog box

To use this feature, right click on the Location panel and select "Go To..." from the pop-up menu that appears to open the Go To Location window. You can then enter an address, location, landmark, or the name of an existing geofence. Once you have entered the location information, click the OK button and the map will reload centring on the information you provided. If you entered the name of an existing geofence, the map will change to the location of that geofence and display it on the screen in red.

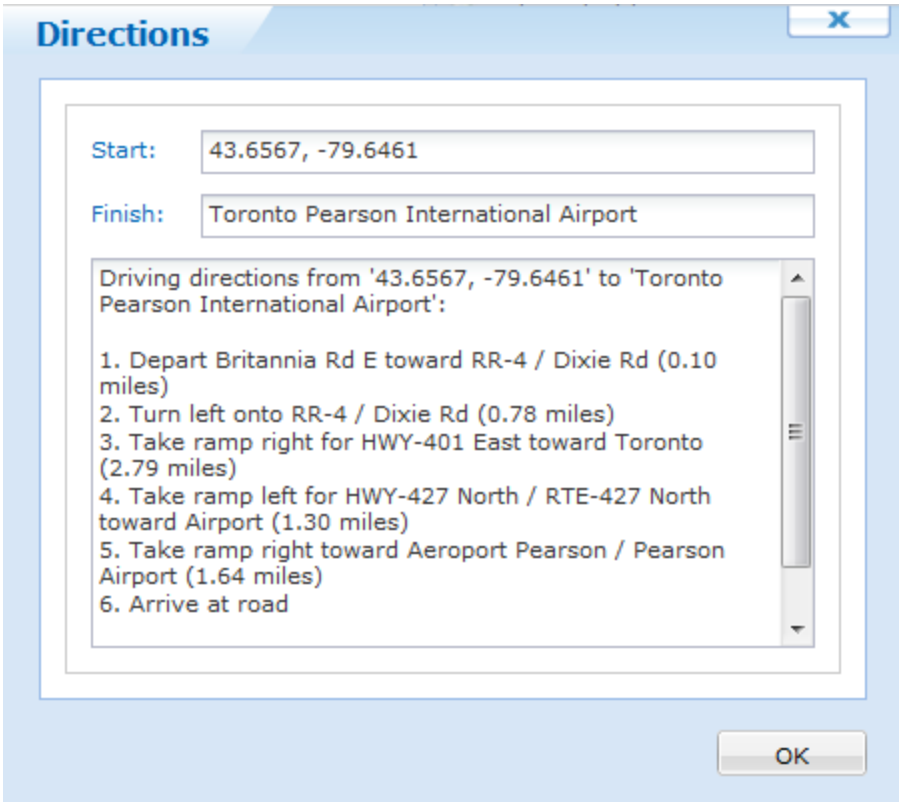
Get Directions

Powered by Microsoft's Bing Maps, MobiControl's Get Directions will return turn-by-turn directions between two locations on the map. These directions can be sent directly to the device, or they can be pasted into an email and sent to a larger group of people. Get Directions is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "Windows Desktop Location Services" topic on page 864 for more information.



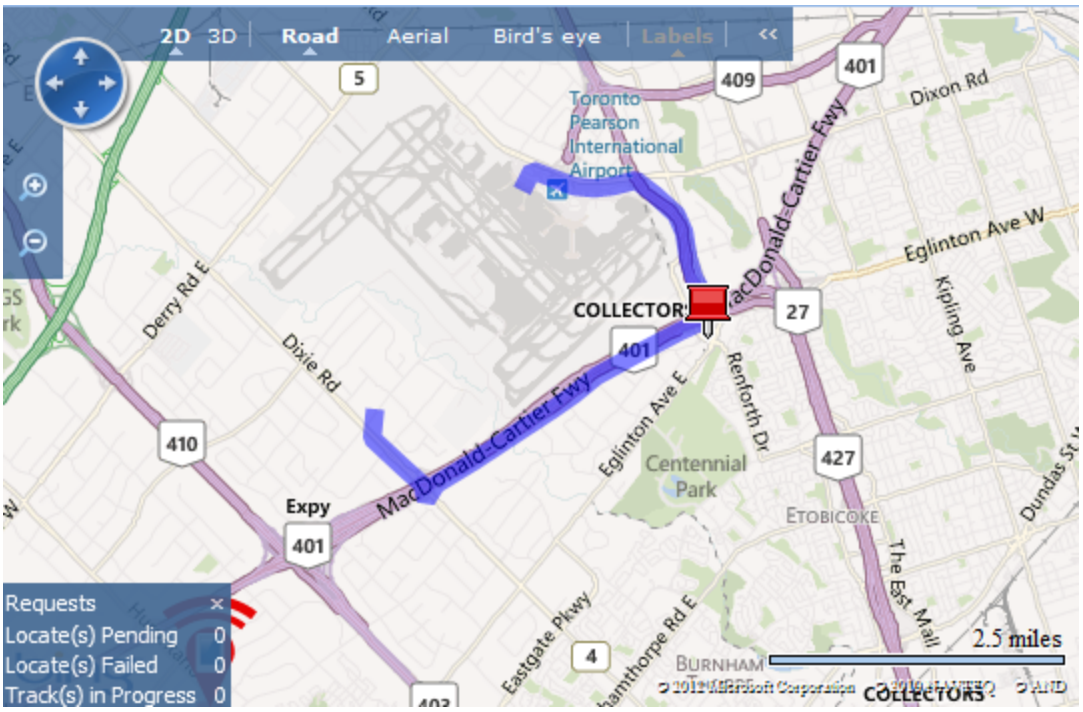
Get Directions dialog box

To use Get Directions, in the Location panel right click on any device or a point on the map and select "Get Directions" from the pop-up menu. The Get Directions dialog box will appear. Be default, the device or map location clicked on will be used as the starting point. To change this, click the double arrow button located to the left of the Start and Finish fields. You can enter GPS co-ordinates, landmarks, or an address. Directions can be optimised by selecting shortest travel time or shortest distance from the options list and press the OK button.



Driving Directions window

MobiControl will determine the turn-by-turn driving directions between the two locations you specified. The resulting directions will be displayed in the Driving Directions window. If you started by right clicking on a device, the "Send to Device" button will be enabled and you can send the instructions directly to the device. You can copy the directions from this window and paste them into an email or document or your choice.

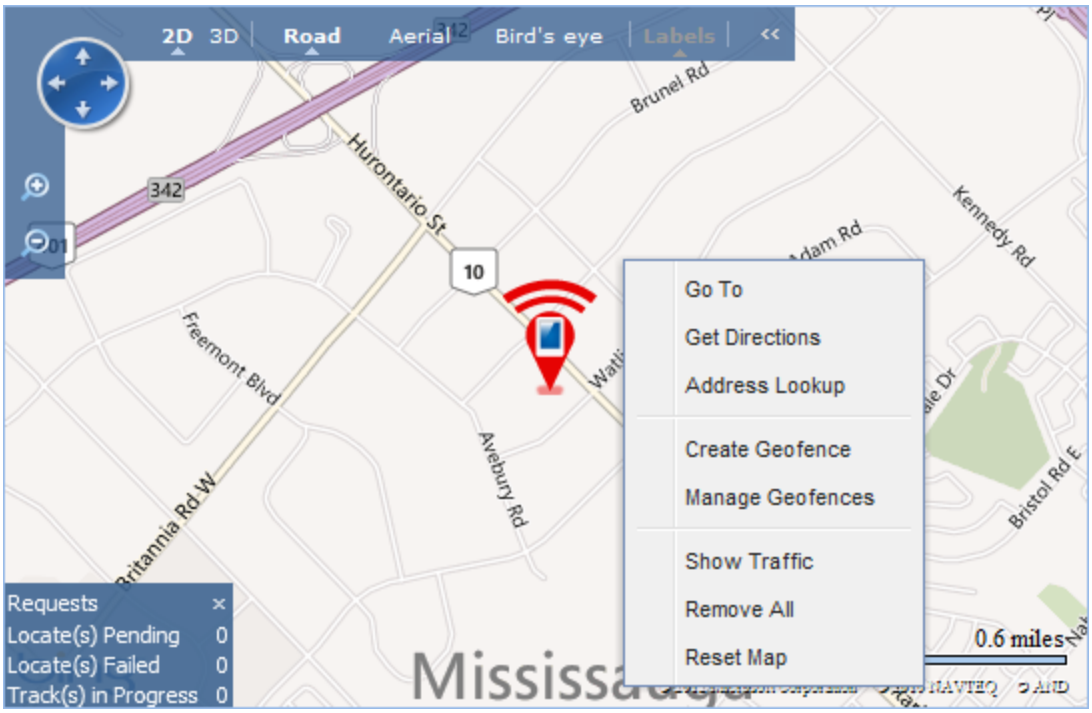


Driving directions displayed on the Map

The Location panel will reload the map to show the driving route highlighted. If the map is in Bird's Eye view, the highlight will not be displayed. Both Aerial and Road view will display the highlighted route.

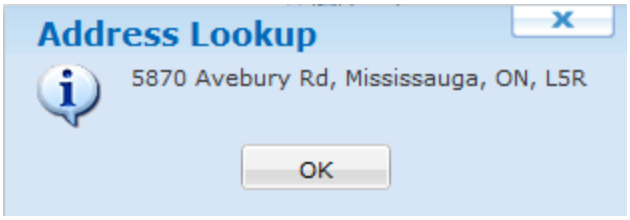
Address Lookup

The Address Lookup feature allows you to determine the address of a specific point on the map displayed on the Location panel. Address Lookup is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "Windows Desktop Location Services" topic on page 864 for more information.



Location panel right click menu with Address Lookup option

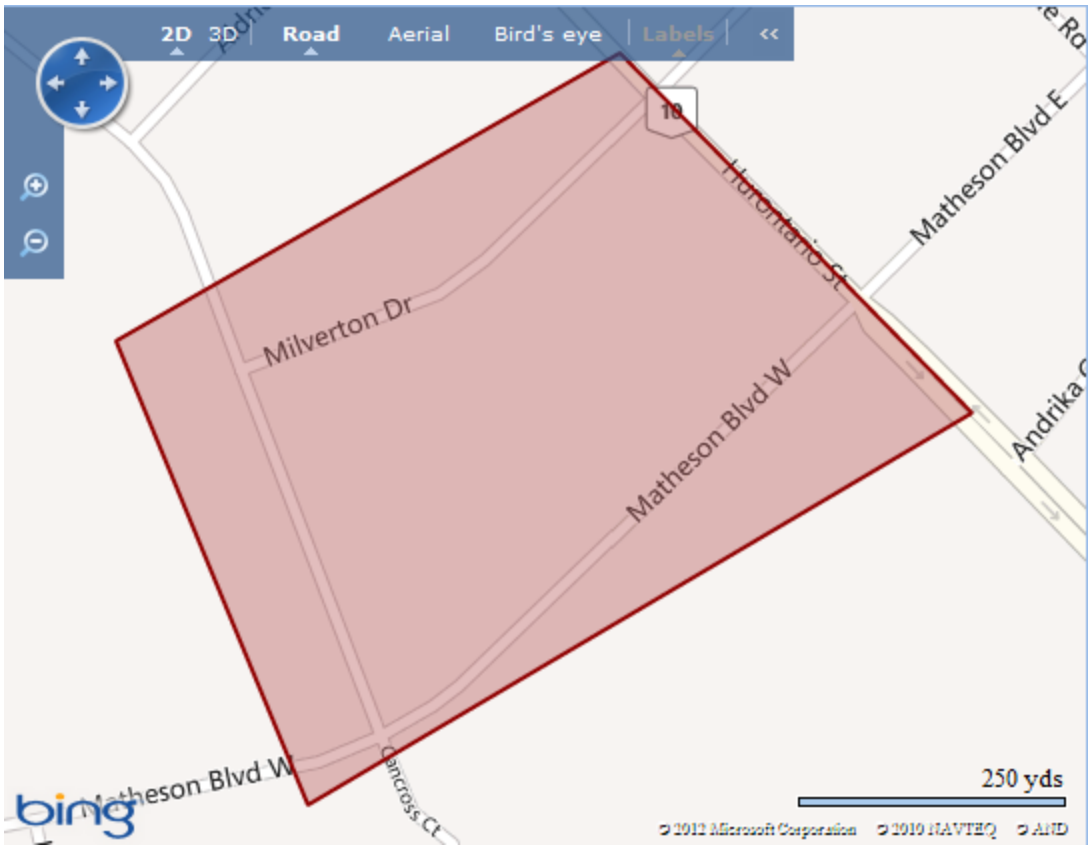
To use the Address Lookup feature, right click anywhere on the map in the Location panel and select the Address Lookup option from the menu that appears. The address of that location will be displayed in a new information window.



Address Lookup window

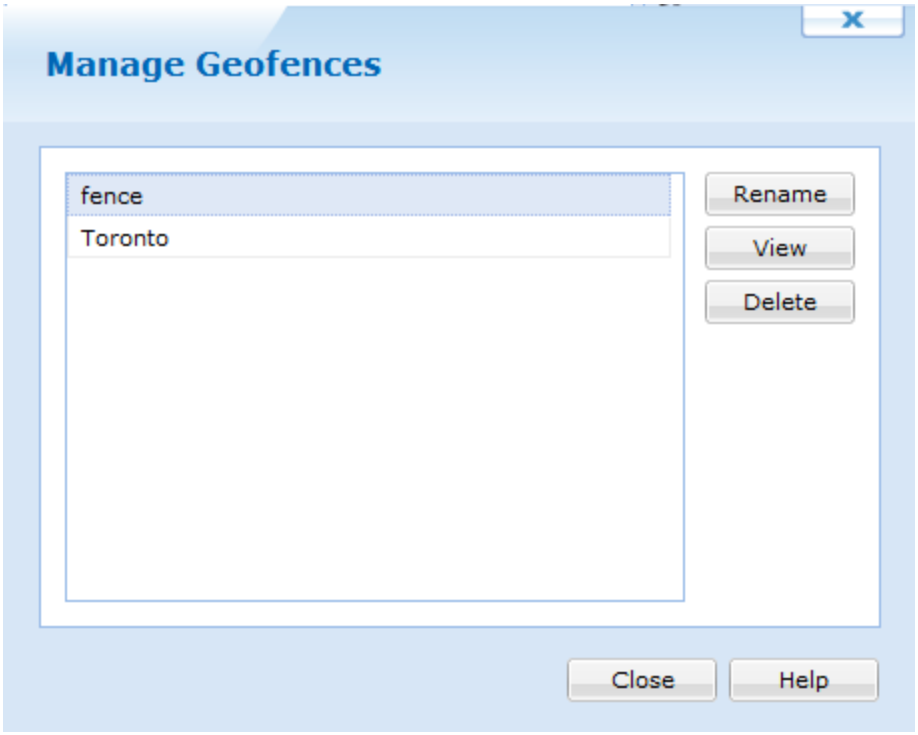
Using Manage Geofences

The Manage Geofences feature provides an area in which to rename, delete or view current created Geofences. You also have the option to create a new geofence from the drop down menu.



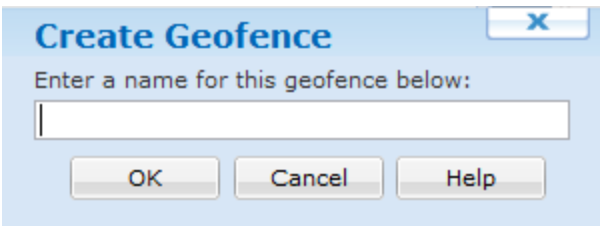
Location panel right click map and select Manage Geofence option

Selecting Manage Geofence brings up the following window.



Field Name	Description
Rename	Allows you to rename a Geofence
View	Allows you to view an already created Geofence on the map
Delete	Allows you to delete a Geofence **NOTE:** In order to Delete the Geofence, no Geofence Event can be associated with it

The **Create Geofence** option allows you to begin drawing on the map. The area drawn on the map will be defined as the Geofence. The defined area must be a complete geometric shape, which means the Start Drawing point will be the same as the End Drawing point. When you have completed a proper geometric shape you be asked to name your geofenced area.

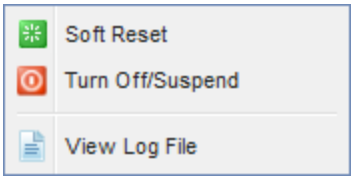


Windows Desktop Actions

MobiControlallows you to soft reset, turn off/suspend and view the log file of Windows Desktop devices. These options can be viewed when you right click a an online device and go to **Action**.

Device Level Actions

Selecting actions on a device level allows you to specifically send actions to that particular device. From here you can soft reset, turn off/suspend and view the log file of the device.



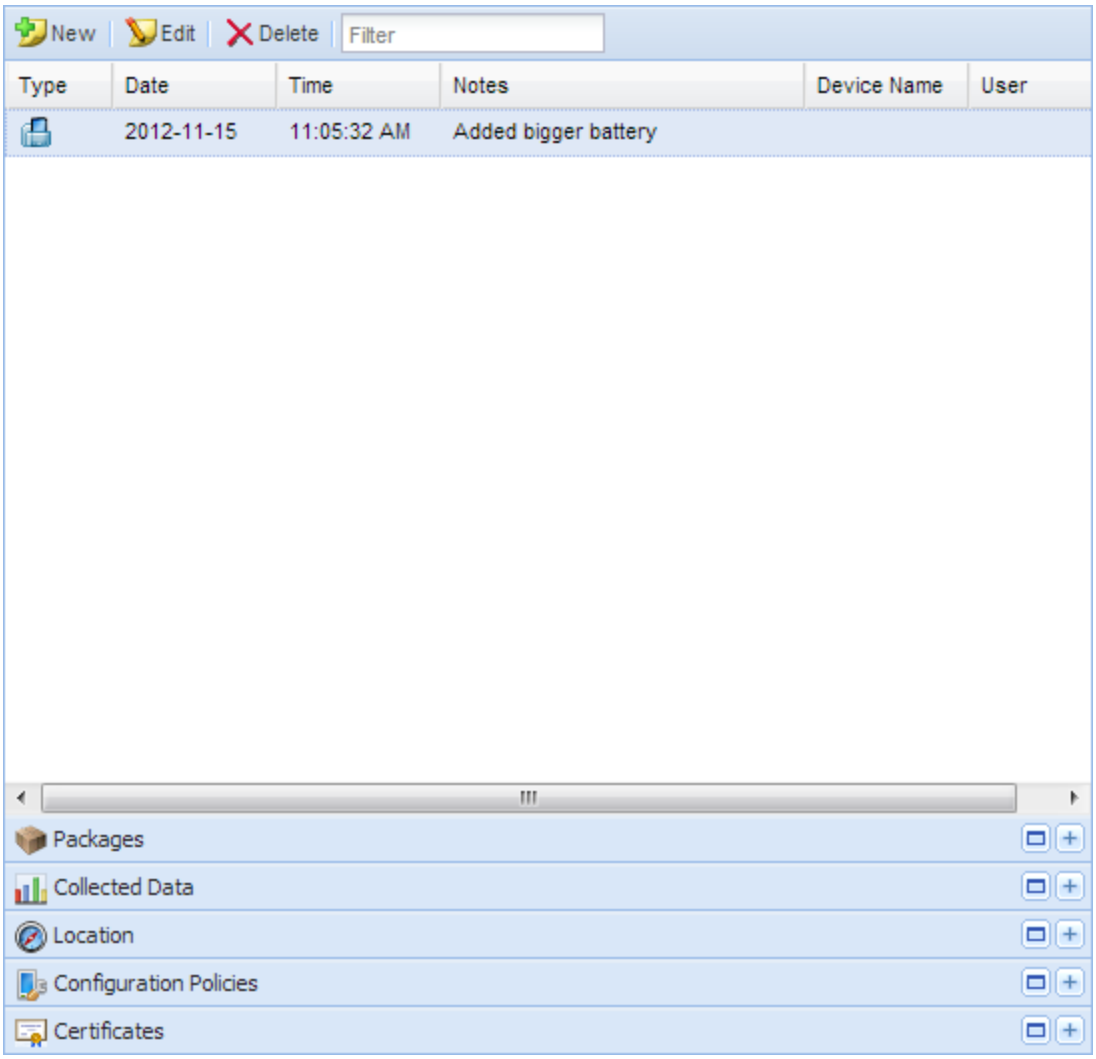
Windows Desktop Action Selections

Device Notes

The Device Notes feature allows you to create a note for a device and archive it for future reference and tracking purposes. Each note is editable and includes the date and time when the note was added or edited. The note includes the name of the user creating the note and can be assigned different colors for color-coded categorization.

This feature is useful for creating a "trouble ticket" for help desk tracking in an end-user support or CRM (Customer Relationship Management) environment. It also allows users with access to the MobiControl Web Console to document a device-specific issue and share their comments and memos related to that device with other users of the MobiControl Web console.

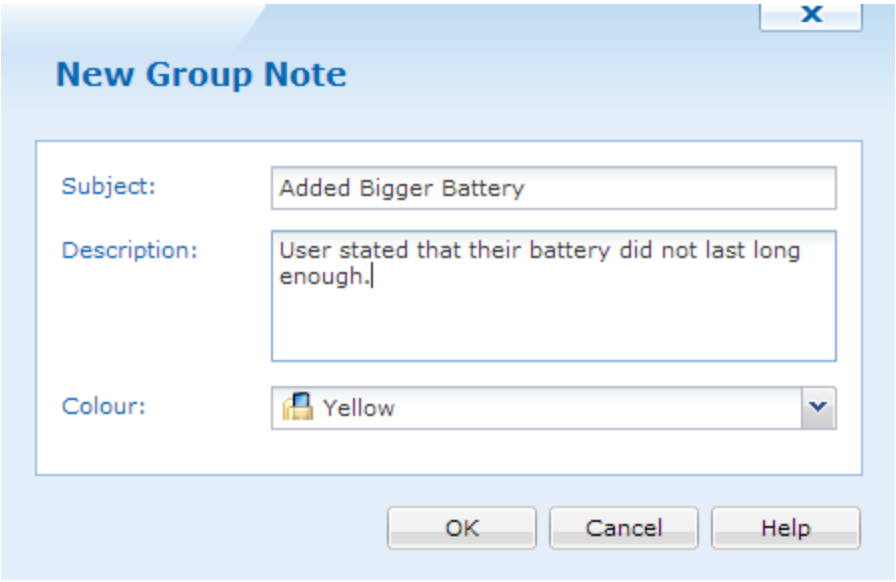
To view and edit notes for a device, select the Devices view (tab) in any of the All Devices, Windows Mobile, Windows Desktop, iOS, Android or Android Plus tab. Select a device and the notes for that device appear in the Notes panel.



Device Notes

Adding or Editing a Note

From within the Notes panel, click **New** to add a new note for the currently selected device or click **Edit** to make changes to an existing note.



Add Note dialog box

The following table describes the fields of the **Add Note** dialog box:

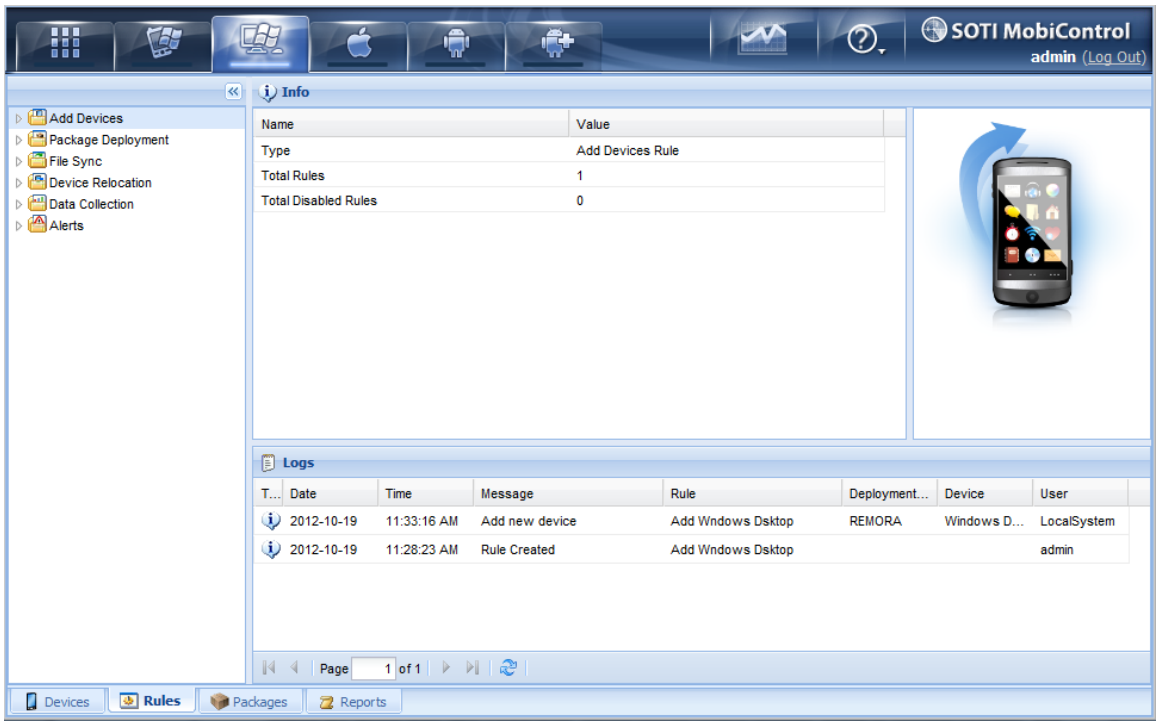
Field Name	Description
Subject	Text entered in the subject field appears in the Notes panel as the title of the note.
Icon	You can choose different colors for the icon to adopt a color-coding to indicate different priority levels or to distinguish between different departments or users creating the note. Notes can be sorted by icon color for a categorized view.
Description	The description field is available for viewing when the note is opened. This field can contain troubleshooting notes, administrative memos or any other device-specific information.

Device Group Notes

MobiControl now offers a way to place notes on a device group level. For example, if you are planning a roll out of devices across the country in phases based on location, you can add device group notes to state which phase each group is in. Therefore, when someone else logs into the MobiControl Web Console, they can see what part of the roll out each group should be in.

To create a device group level note, click a group on the left side of the MobiControl Web Console. After a group has been selected, expand the Notes panel on the right side, and click New.

Windows Desktop Rules Tab



Windows Desktop Rules Tab

MobiControl uses rules to simplify the tasks of device management and configuration. See Below for a description of each rule.

Add Devices

1. Create an add devices rule.

   An add devices rule allows you to configure the settings that MobiControl uses to set up and communicate with your devices. These settings include: the device group to which devices are added, how often the device is to check for updates, and the parameters to be used for remote control sessions. Please see the "Add Windows Desktop Devices" topic on page 880 for detailed information about creating an add devices rule.

2. Create a Device Agent.

   The Device Agent is the MobiControl software that resides on mobile devices and communicates with MobiControl Deployment Servers. Device Agents execute instructions received from MobiControl Deployment Servers, report status information, and send real-time information to Deployment Servers. Device Agents also restore the device state after a hard reset, service remote control sessions, install or uninstall packages, and synchronize the device clock. Please see the "Windows Desktop Device Agent Manager" topic on page 889 for detailed information about creating a Device Agent.

3. Install the Device Agent onto the devices.

   Once created, there are several options for installing the agent on to your devices. For example, installation can be accomplished via cradled ActiveSync, via a website download, via an SD card, or using an existing software distribution mechanism. Please see the "Windows Desktop Device Agent Manager" topic on page 889 for detailed information about installing the Device Agent.

Package Deployment

1. Create a package.

   A package is a set of software and data files that have been packed into a single compressed file. MobiControl provides a tool called MobiControl Package Studio that allows you to quickly and easily create packages. For complex packages, Package Studio allows users to add scripts that get automatically executed at various points in the installation or un-installation of the package. Please see the "Creating Packages" topic on page 414 for detailed information about creating packages using MobiControl.

2. Create a deployment rule.

   To deploy a package using MobiControl, you need to create a deployment rule. When you create a deployment rule, you need to specify the package(s) to be deployed, the devices to which the package(s) will be deployed, and the installation time. Please see the "Windows Desktop Package Deployment" topic on page 897 for detailed information about creating a deployment rule.

3. Check the rule execution status.

   Once you have created a deployment rule, you may want to confirm that all devices have been provisioned with the specified packages. The execution status of the deployment rule is graphically represented in the execution chart in the Rules view (tab). MobiControl also provides a report called the 'Deployment Rule Execution Summary Report'. Please see the "Windows Desktop Reports" topic on page 944 for detailed information about MobiControl Reports.

File Sync

1. Create a file sync rule.

   A file sync rule allows you to schedule file(s) to be synchronized between a set of devices and the Deployment Server. When creating a file sync rule, you will need to specify the file(s) you want synced (both their original location and their destination), the interval in between the syncs and which direction the sync should go in (either device to server, or server to device) and which devices should be involved in the sync. Please see the "Windows Desktop File Sync" topic on page 903 for detailed information about creating a file sync rule.

2. Check the rule execution status.

   Once the file sync rule has been created, you may want to confirm that the scheduled syncs occurred. You can do this by looking at the rule execution status or by checking the rule execution report in the Reports view (tab). Please see the "Windows Desktop Reports" topic on page 944 for more detail about reports.

Device Relocation

1. Create a device relocation rule.

   A device relocation rule allows you to automatically move your mobile devices among different device groups in the MobiControl device tree, based on the IP address or other custom criteria. This is useful for managing mobile devices in a deployment where the device tree represents different physical locations (e.g. retail stores, warehouses, regional offices, etc). Please see the "Windows Desktop Device Relocation" topic on page 916 for detailed information about creating a device relocation rule.

2. Check the device relocation rule execution status.

   Once the device relocation rule has been created, you may want to confirm its execution. You can do this by looking at the rule execution status or by checking the rule execution report in the Reports view (tab). Please see the "Windows Desktop Reports" topic on page 944 for more detail about reports.

Data Collection

1. Create a data collection rule.

   A data collection rule allows you to set up rules to collect data from your mobile devices automatically. Please see the "Windows Mobile Data Collection" topic on page 920 for detailed information about creating a data collection rule.

2. Check the data collection rule execution status.

   Once the data collection rule has been created, you may want to confirm its execution. You can do this by looking at the rule execution status or by checking the rule execution report in the Reports view (tab). Please see the "Windows Desktop Reports" topic on page 944 for more detail about reports.

Alert

1. Create an Alert Rule

   An Alert Rule allows Administrators and Users to be notified when events of interest arise on the system. Please see the "Windows Desktop Alerts" topic on page 927 for detailed information about creating an Alert Rule.

2. Check the Alert Rule execution status.

   Once the Alert Rule has been created, you may want to run a report to see what alerts have been generated. You can do this by looking at the Alert Rule Summary report in the Reports view (tab). Please see the "Windows Desktop Reports" topic on page 944 for more detail about reports.

Adding Windows Desktop Devices

Add devices rules allow MobiControl to name devices, place devices in the appropriate device group, and to generate a customized MobiControl Device Agent that, when installed onto devices, allows them to be managed by MobiControl.

When you generate a Device Agent for an add devices rule, MobiControl places an identifier for the rule (i.e. rule tag) into the `.cab` file for the generated agent. When the Device Agent is installed onto a device, it will connect to a MobiControl Deployment Server and supply the rule tag to the server. The server will then look up the add devices rule and configure the device accordingly.

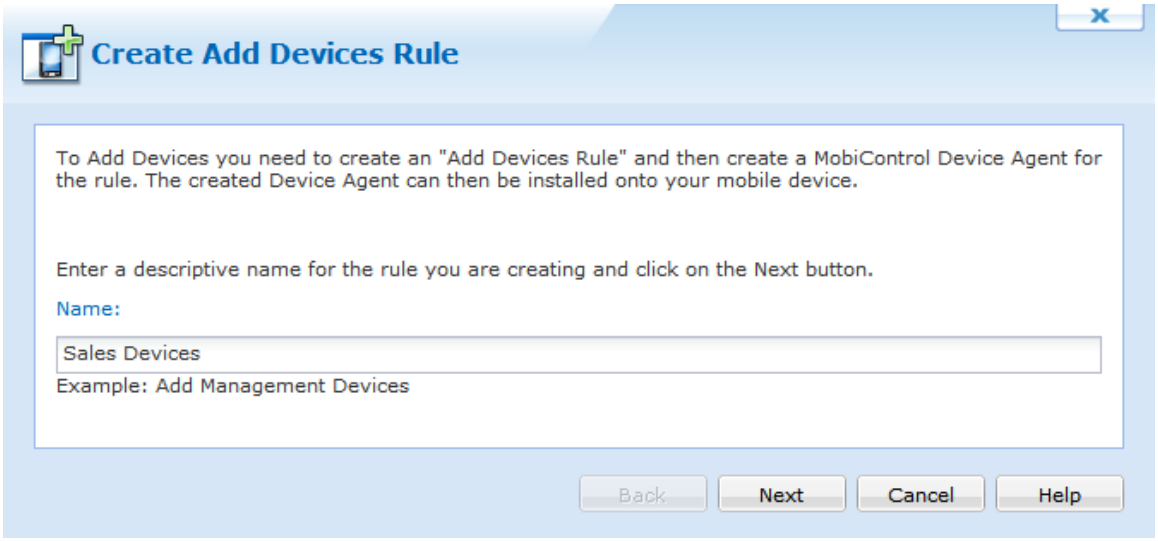
To create an add devices rule, select the Rules view (tab) within MobiControl Manager, then click the **Rule** menu, select **Create Rule**, and click **Add Devices Rule**. The Create Add Devices Rule Wizard will be displayed.

The six steps below describe how the Create Add Devices Rule Wizard can be used to create an add devices rule:

1. Start the wizard.

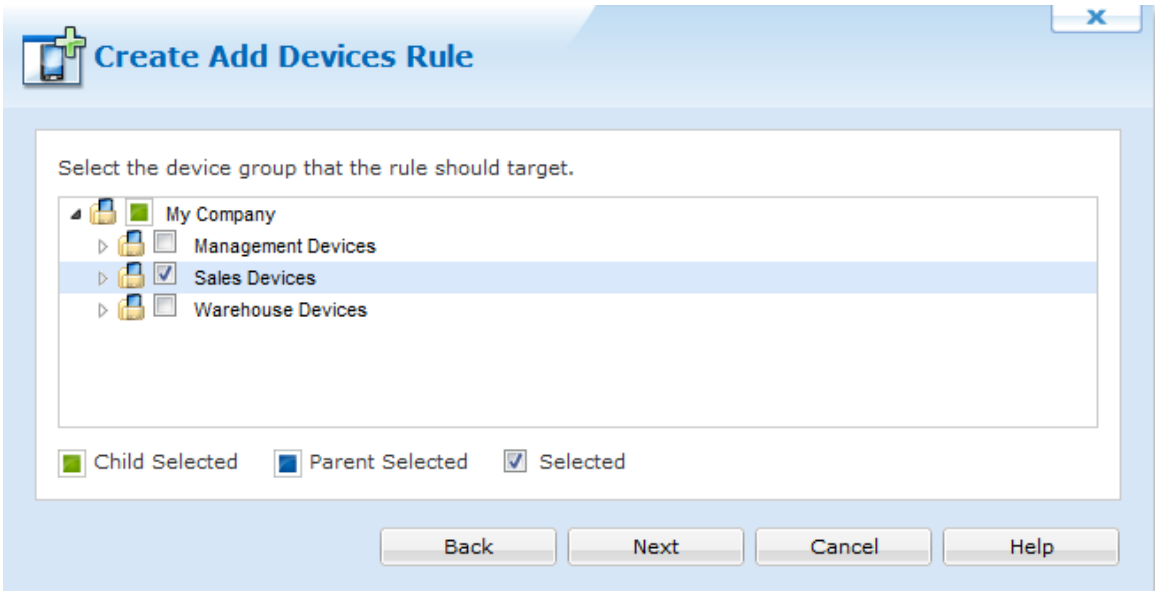
   Select the Rules view (tab), then click the **Rule** menu, select **Create Rule**, and click **Add Devices Rule**. The first page of the Create Add Devices Rule Wizard will be displayed.

   Enter a descriptive name for the add devices rule you are creating and click **Next.**



First page of the Create Add Devices Rule Wizard

2. Configure the device group.



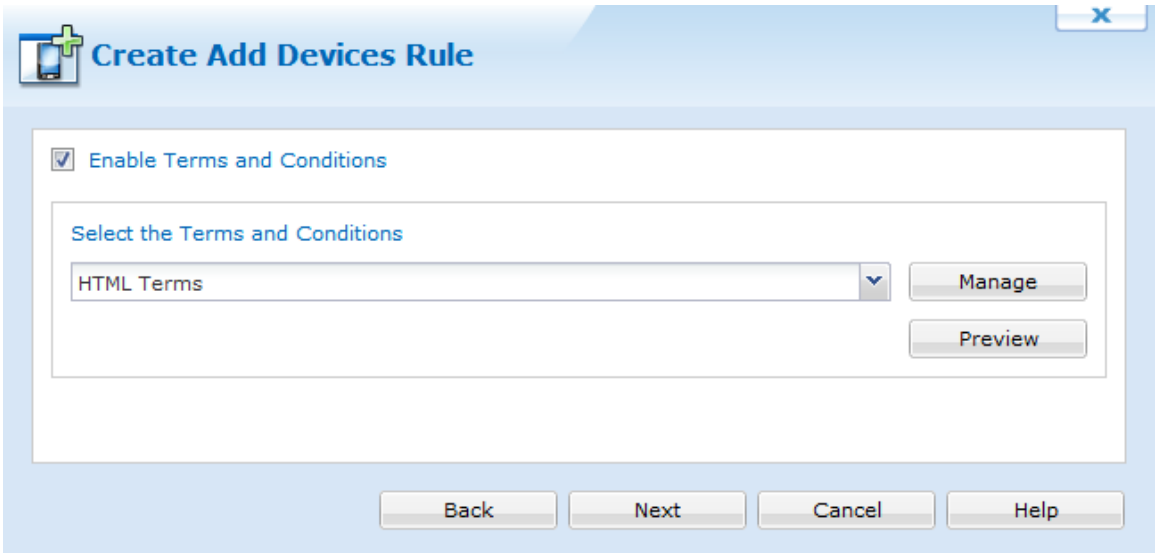
Device Group Selection page

First, select to which device group the devices configured by this rule will be added. The dialog box below displays the current device tree. Select the group where devices need to be inserted and then click **Next.** If you need to add a new group or change the structure of the device tree, exit the wizard, go to the Devices view (tab), edit the tree, and then begin the wizard again.

After selecting a device group click on the **Next** button.

3. Terms and Conditions

The terms and conditions page allows us to send terms and conditions to devices. Users must accept these terms before they are able to enroll their device to MobiControl. If they do not accept the terms and conditions, the device will not connect. If Terms and Conditions is required, click "Enable Terms and Conditions".



Terms and conditions

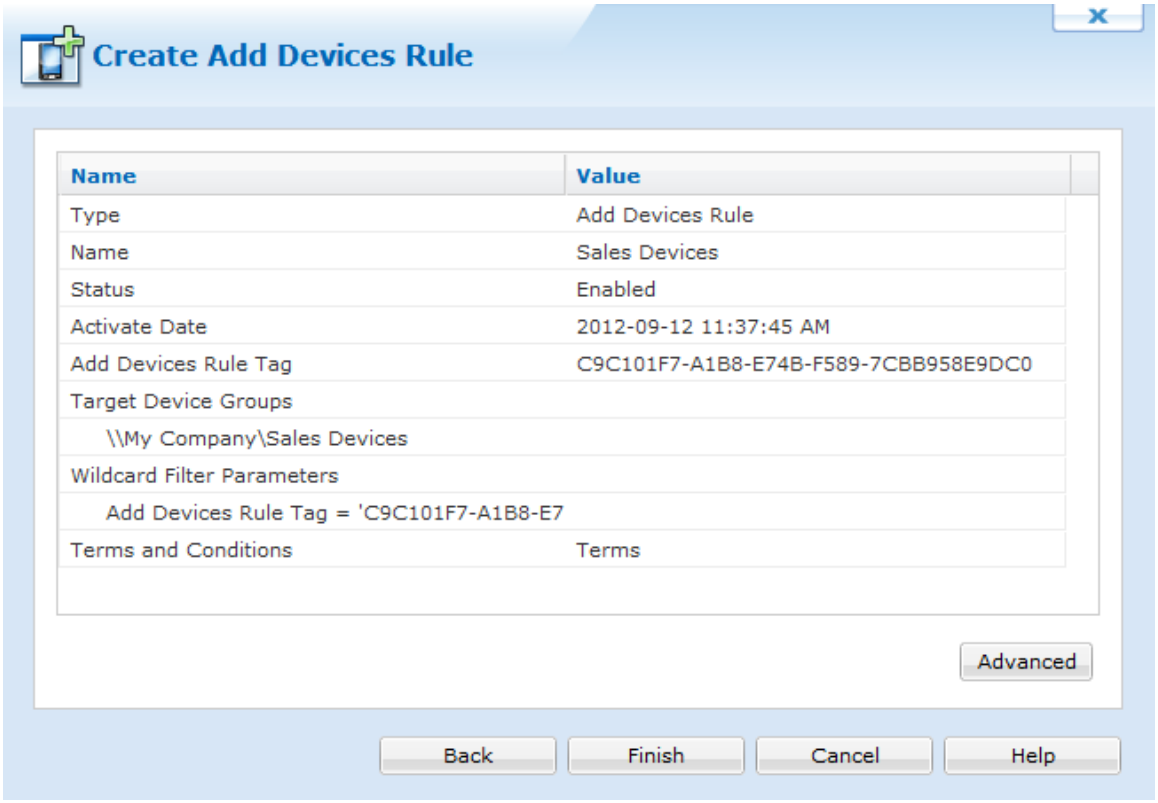
To add new Terms and Conditions to the Add Devices rule, click Manage. Once clicked, we can see the Terms and Condition Manager. Please see the "Terms and Conditions" topic on page 619 for more information.

After selecting the Terms and Conditions, click **Next** to continue the creation of the rule.

4. Review summarized information.

The **Rule Summary Information** page summarizes the settings configured on the previous pages of the wizard.

If you are satisfied with the configured settings, click on the **Finish** button to create the device rule, otherwise use the **Back** button to go to previous screens and make adjustments.

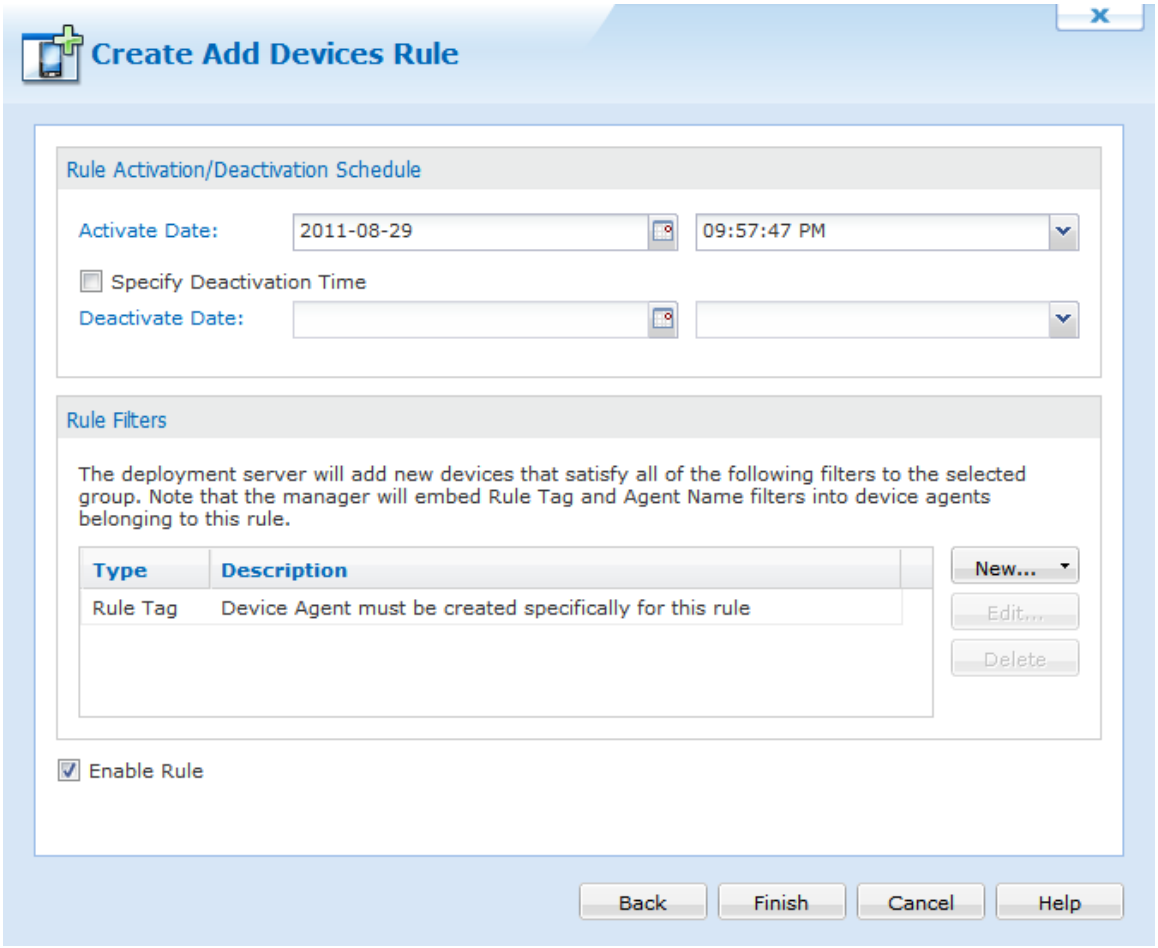


Rule Summary Page

5. Advanced Settings.

   The **Advanced Settings** button allows you to specify which devices are to be configured by this rule. By default, MobiControl will use this rule to configure only those devices that are running a Device Agent created specifically for this device rule. By using advanced settings filters, you can broaden or further restrict which devices get configured by this rule when they connect to MobiControl.

   Once you have made the changes, click **Next.**



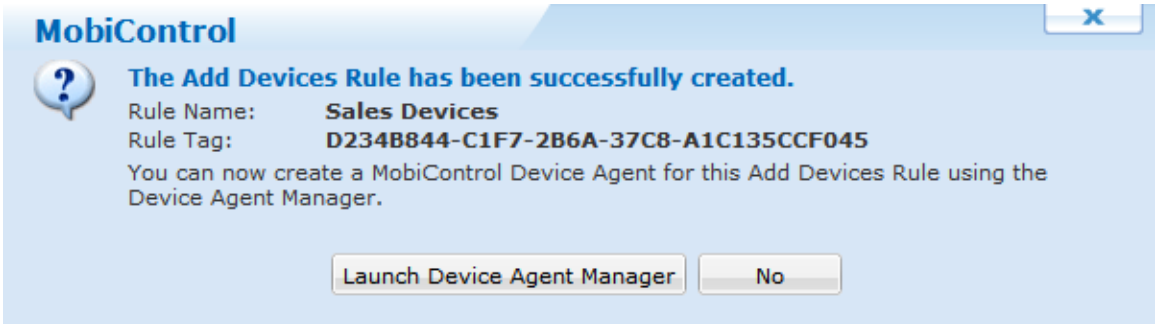
Advanced Settings Page

For additional information about **Rule Tags** see the appropriate section below.

6. Receive confirmation that the rule has been created.

   A notification of rule creation will be displayed once the device rule has been created. The message box confirms that the rule has been successfully created and allows you to immediately generate a MobiControl Device Agent for the rule.

   If you click the **Yes** button on the message box, the wizard to create a Device Agent will be launched. If you click on the **No** button, you can generate a Device Agent later.



Rule Creation Notification message box

NOTE:

You can access the Device Agent Manager from the Rules view (tab) in MobiControl Manager. Right-click on a specific add devices rule in the left pane, and then select **Device Agent Manager** from the pop-up menu.

Once you have created an add devices rule, the next step is to generate a MobiControl Device Agent. You can generate a Device Agent for an add devices rule immediately after creating the rule or at any time after creating the rule using the Device Agent Manager. The generated agent is customized for the specific add devices rule that you select. Please see the "Windows Moible Device Agent Manager" topic on page 755 for instructions on how to create a Device Agent using the Device Agent Manager.

Rule Tag Settings

The **Add Devices Rule Advanced Settings** are accessible from the Create Add Devices Rule Wizard by clicking the **Advanced Button** (Advanced Tab when editing a Rule.) This page allows you to specify which devices are to be configured by a specific Add Devices Ruleadd devices rule. By default when you create an Add Devices Rule, MobiControl will use the rule to configure only those devices that are running a Device Agent Device Agent created specifically for that Add Devices Rule. By using Advanced Settings filters, you can broaden or further restrict which devices get configured by a specific rule when they connect to MobiControl.

Types of Filters

- Rule Tag Filter

  The **Rule Tag filter** will cause the rule to configure only devices with a certain device rule tag. When a MobiControl Device Agent is generated, a unique identifier (rule tag) is inserted into the agent. When the Device Agent connects to a MobiControl Deployment Server, it presents the server with the rule tag. When this filter is used, the Deployment Server will only configure a device if there is a match between the rule tag presented by the agent and an add devices rule in the database. In this way, an add devices rule will be used to configure only those devices that are using an agent specifically created for that rule.

This is the default filter; it is automatically added when an add devices rule is created. If this filter is removed, then this rule can be used to configure devices that are using Device Agents created by third parties (i.e. When a MobiControl Device Agent is already installed on the device when it comes from the manufacturer) or Device Agents created for other device configuration rules.

- IP Address Filter

  The **IP address** filter causes the add devices rule to configure only those devices whose IP addresses are in the range specified. This rule is useful as an extra security blanket for limiting connections to only devices that have an IP within the authorized range of IP addresses. The rule may also serve as a means of segregating different sets of devices.

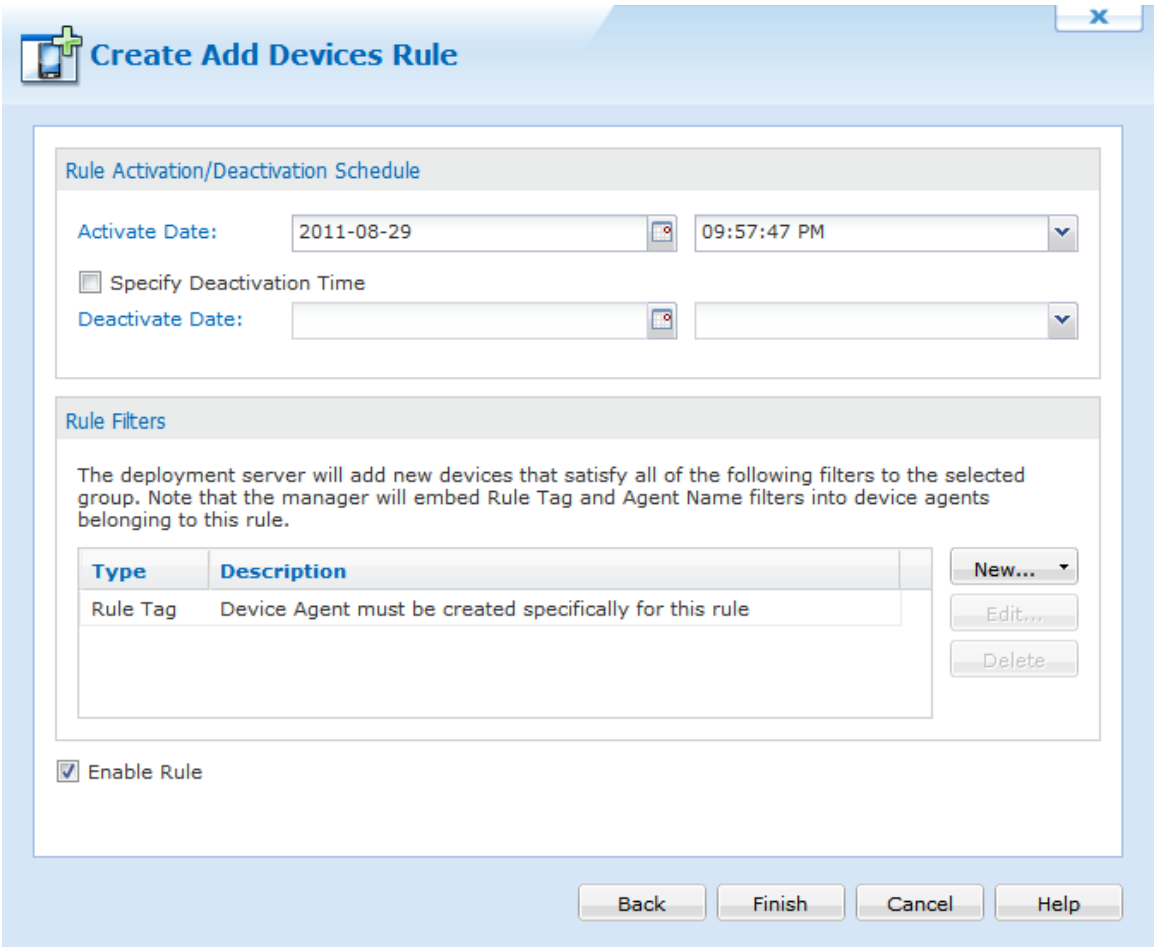
  EXAMPLE:

  If an IP address filter from 192.168.1.10 to 192.168.1.99 has been set, then only devices with an IP address in this range would be configured by this add devices rule. If a device with an IP address of 192.168.1.100 connects to MobiControl, it would not satisfy the IP address filter test for this rule and so, it would not be configured by this rule.

  The IP address filter is used for limiting connections to approved IP ranges. Please see the "Windows Mobile Device Relocation" topic on page 782 for dynamic relocation of devices from one device group to another and reconfiguring devices based on the IP address of the mobile devices (or other criteria).

- Agent Name Filter

  The **agent name filter** causes the add devices rule to affect only devices with the same agent name. When this filter is set, all agents generated for this rule will automatically be named appropriately. This rule is useful in the event you have a set of devices already equipped with Device Agents. Simply creating this rule will allow the Device Agents on those devices to connect to the Deployment Server.

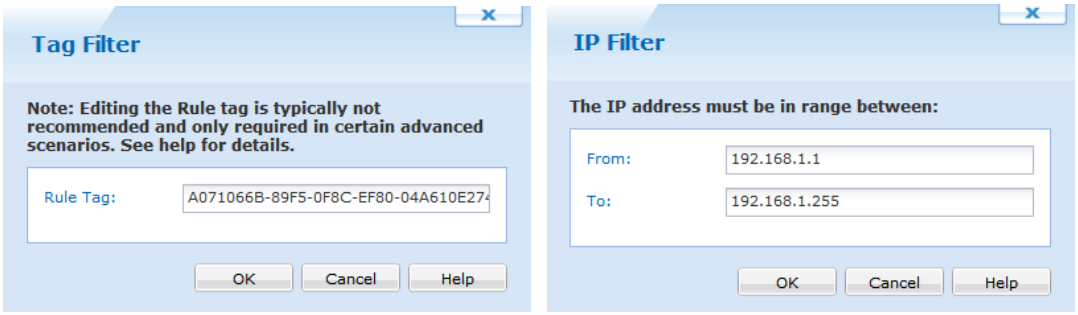


Add Devices Rule Advanced Settings dialog box

Adding a Filter

To add a filter, click the **New** button and select the appropriate filter type from the pop-up menu.

The dialog box displayed depends on the type of filter selected. If the **Add IP Address Filter** was selected from the menu, the **IP Address Filter** dialog box will be displayed. If an **Add Devices Rule** is created, the filter is automatically added. This option will not be available if this filter has already been added.



Rule Tag Filter and IP Address Filter dialog box dialog box

To complete the operation, fill in the information asked for in the dialog box and click the **OK** button.

Editing or Deleting a Filter

To edit or delete a filter, select the filter from the filter list and click the **Edit** or **Delete** button.

Creating Deployment Rules

Deployment rules allow administrators to automatically provision mobile devices with packages that contain software or data. The following series of steps describes how to use the Create Deployment Rule Wizard to create a deployment rule.

Creating the Agent with Device Agent Manager

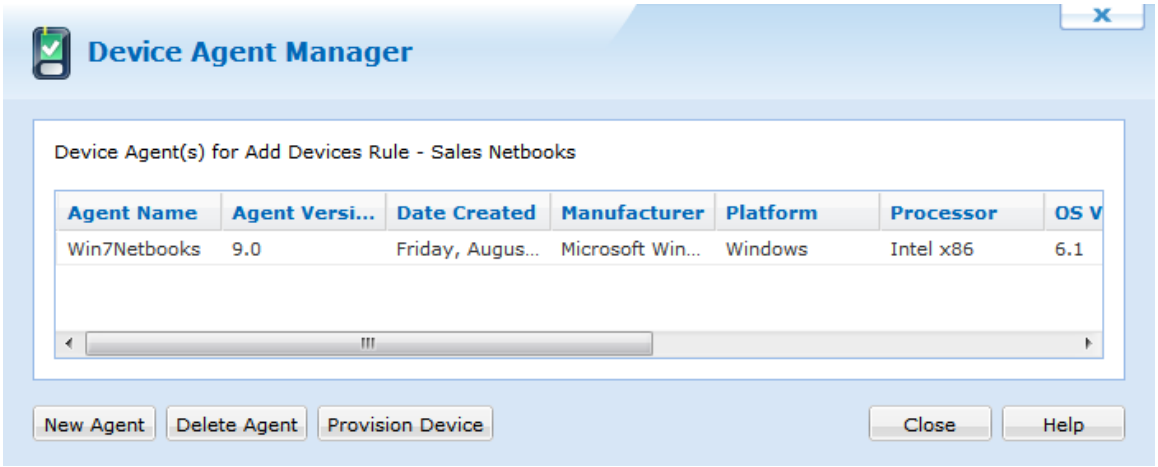
The Device Agent Manager is an interface that allows the user to manage the Device Agents that are installed to the devices. A Device Agent is a program that is installed on to the various devices that are to be managed by MobiControl. The software facilitates the server-client communications. The Device Agent Manager allows creation of custom Device Agents that have been specially configured to the settings of your MobiControl installation and the type of devices you have.

You can access the Device Agent Manager from the Rules view (tab) in MobiControl Web Console by right-clicking on a specific add devices rule in the left pane, and then selecting **Device Agent Manager** from the pop-up menu.

Once you have created an add devices rule, the next step is to create a MobiControl Device Agent. You can create a Device Agent for an add devices rule immediately after creating the rule or at any time after creating the rule using the Device Agent Manager. The created agent is customized for the specific add devices rule that you select.

The following steps outline how to create a Device Agent using the Device Agent Manager.

1. Create a Device Agent



Device Agent Managerdialog box

The MobiControl Device Agent Manager allows you to create a Device Agent for a specific add devices rule. The Device Agent Manager also allows you to view and copy files for Device Agents previously created. After creating a device rule, you can access the Device Agent Manager by clicking on the **Yes** button on the message box displayed immediately after the rule is created, or by going to the Rules view (tab) in MobiControl Manager, and then right-clicking on a specific add devices rule in the left pane, and then selecting **Device Agent Manager** from the pop-up menu.

The Device Agent Manager displays a list of the Device Agents that have previously been created for the selected device rule, and allows users to create new Device Agents, provision Device Agents onto devices (by directly installing, exporting or generating barcodes) and to delete obsolete Device Agents. For newly-created add devices rules, the list will be empty until an agent is created.

If an agent has been already created, select the Device Agent and click on **Provision Device**

The following methods can be used to provision the Device Agent on the devices.

You can download the agent installer by clicking on **Self-Extracting Executable** button

You can publish the Device Agent to your deployment server's website by clicking on **Device Agent URL Address**

To delete an agent, select the agent from the list and click the **Delete Agent** button.

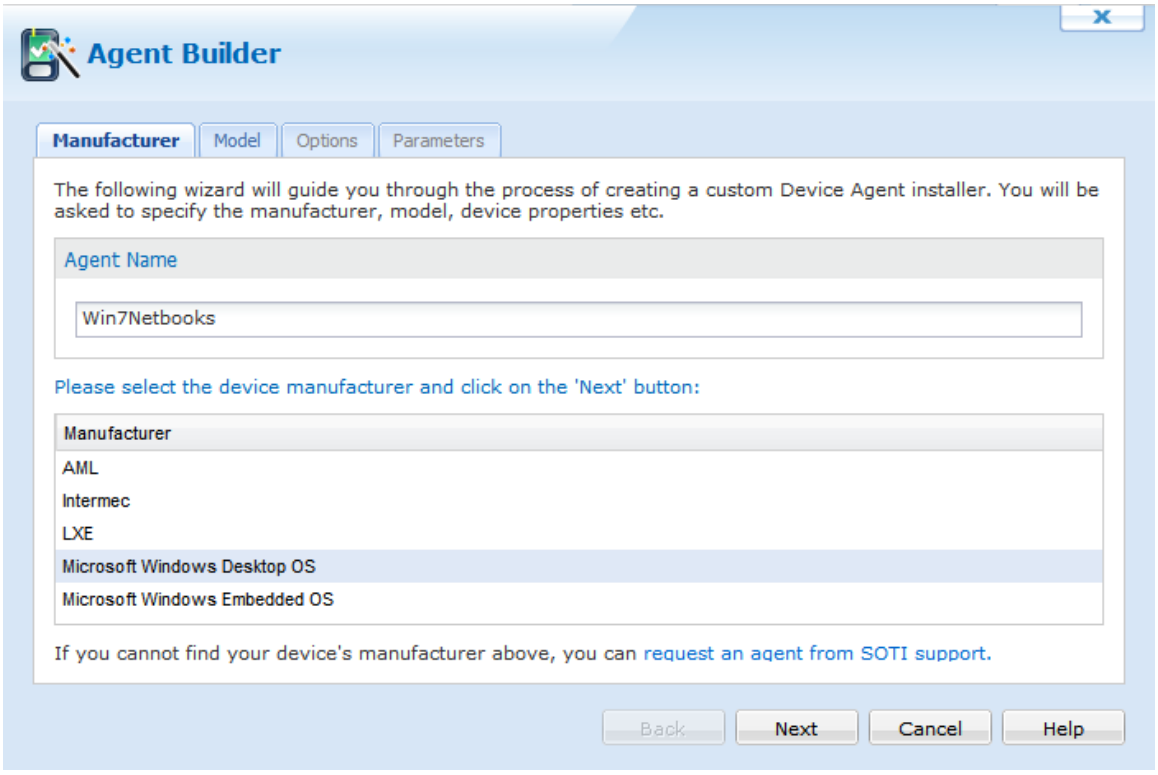
To create a new agent, click the **New Agent** button, the Device Agent Wizard will be displayed.

2. Name the Device Agent and specify the manufacturer.

This will allow you to add a custom name to the Device Agent, which will help to identify it.

Select the manufacturer of your device and click the **Next** button. If the manufacturer of your device is not listed you can try selecting the **Other Manufacturers** option and click the **Next** button or you can to make sure that your device is properly supported by contacting us.

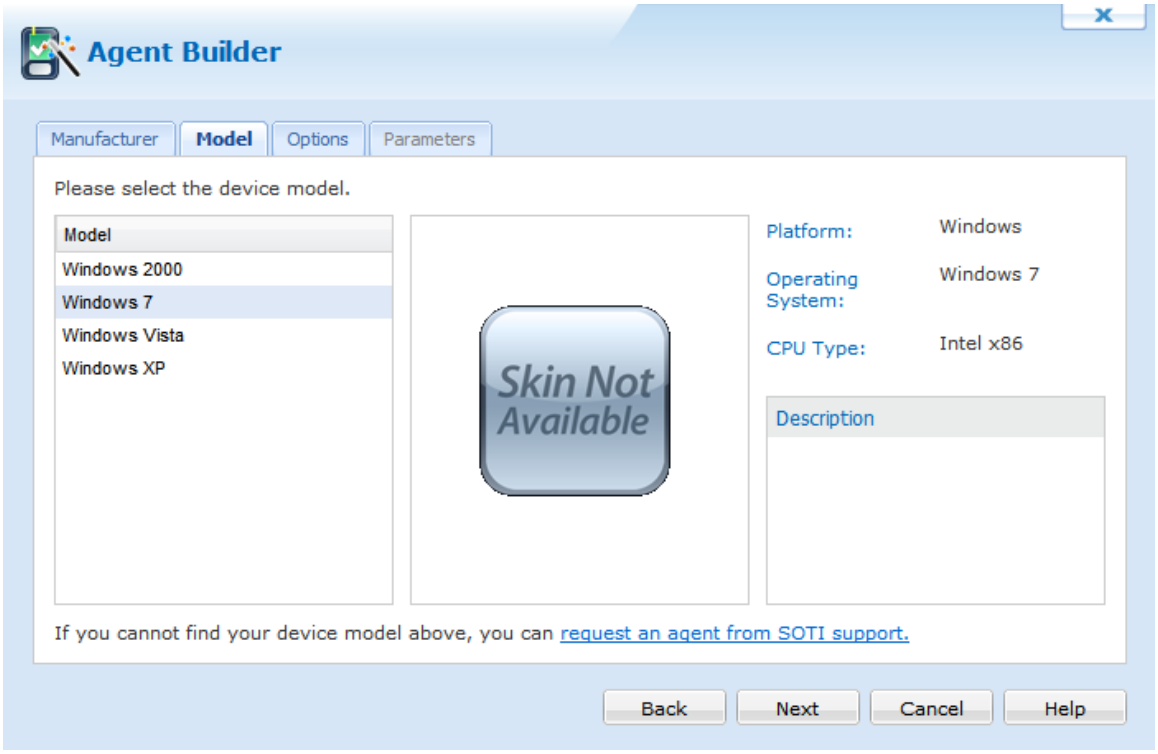
After providing the device name and selecting the manufacturer, click the **Next** button.



3. Select the device model and configure device type

From the second page of the Device Agent Wizard you will be prompted to select the appropriate device model based on your previous selection. In previous versions of MobiControl where OS and Processor type had to be inserted, this is now done automatically

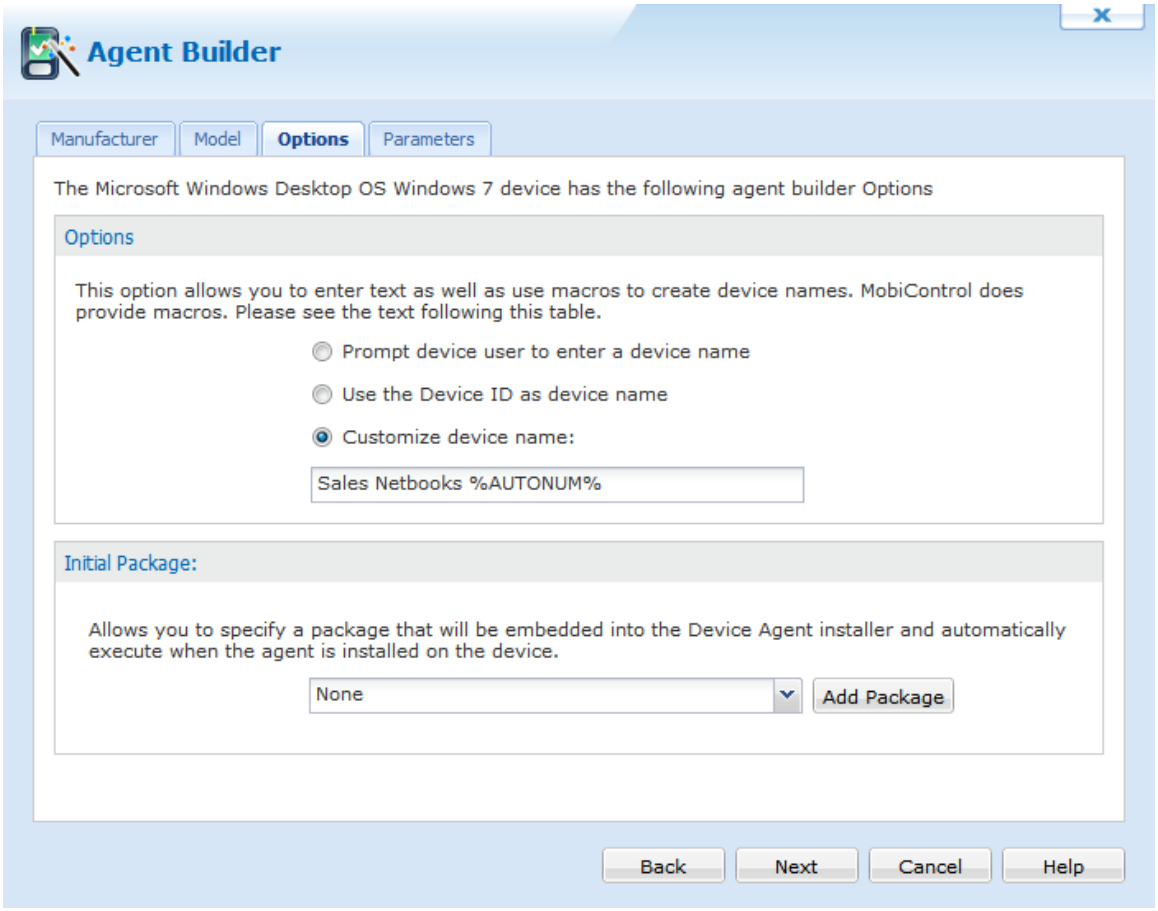
The **Device Type** dialog box allows you to configure platform, processor and operating system information about your devices. If you dock one of your devices via ActiveSync, and click on the **Detect Settings** button, the wizard can automatically detect most of the device settings. If your device is not docked you can enter the settings manually.



Manufacturer Selection page

4. Configure the device identifier and specify an initial package

The **Device Identifier Configuration** page allows you to select how devices are named and uniquely identified.



Method Selection page

The following table provides descriptions for the three device naming options:

Field Name	Description
Prompt Device User	When this option is selected, the Device Agent will prompt the user for a device name when it is first started.
Use the Device ID	When this option is selected, the device ID will be used as the device name. Since the device ID is a cryptic string that is not very readable (e.g. `0003000F-3EAC-0F94-0F00-0300AA3EE877`), we generally do not recommend this option.
Customize the Device Name	This option allows you to enter text as well as use macros to create device names. MobiControl does provide macros. Please see the text following this table.
Set Windows Device Name Checkbox	When this option is checked, MobiControl will set the Windows Device Name to be the same as the MobiControl Device Name configured above.

Macros

- **%AUTONUM%** allows you to automatically use a numbered sequence as part of the device name. For example, if the value of this field is set to `WH%AUTONUM%`, then the first device configured will be assigned a name of `WH00001`, the second device will have a name of `WH00002`, and so on. `%MAC%` expands to the MAC address of the device. This macro is suitable for use with devices that have a wireless or wired networking capability. The MAC address is a unique number that is built into the network hardware used on the device. In most cases MobiControl can retrieve the MAC address from the hardware. For example, if the value of this field is set to `DEV%MAC%`, then the device names configured would look similar to `DEV00A0F85324D4` and `DEV00A0F8533422`. When the MAC macro is used as the Device ID, the Wi-Fi radio must be enabled when the agent is installed in order for the macro to work.
- **%HOSTNAME%** expands to the local host name of the device. We recommend using this macro only in cases where unique hostnames have previously been assigned to devices before the MobiControl Device Agent software is installed.
- **%IP%** expands to the IP address of the device. We recommend using this macro only in cases where the mobile devices have wireless or wired networking capabilities and are using fixed IP addresses. The use of this macro is not suitable for situations in which the mobile devices are using dynamic IP addresses (i.e. DHCP) since when the IP address changes the device name will be incorrect.
- **%PHONENUMBER%** expands to the phone number of the device. We recommend using this macro only in cases where the mobile device is a Smartphone or Pocket PC Phone Edition. For some devices, the phone number may not be available.
- **%IMEI%** expands to the IMEI (International Mobile Equipment Identity) number of the device. We recommend using this macro only in case where the mobile device is a Smartphone or Pocket PC Phone Edition. For some devices the IMEI number may not available.
- **%ESN%** expands to the ESN (Electronic Serial Number) number of the device. We recommend using this macro only in case where the mobile device is a Smartphone or Pocket PC Phone Edition. For some devices the ESN number may not available.
- **%IMSI%** expands to the IMSI (International Mobile Subscriber Identity) number of the device. We recommend using this macro only in case where the mobile device is a Smartphone or Pocket PC Phone Edition. For some devices the IMSI number may not available.
- **%REG://%** expands to the registry in the device. This will allow custom names like serial number (read from registry key) to be used out of the box for device naming, e.g. `%REG://HKEY_LOCAL_MACHINE\Software\Apps\SOTI\MobiControl?VN=ESN%`
- **%TXT://%** will get the content of specified line of the text file (if LN is not specified, it assumes the first line), e.g. %TXT://\Device.log?LN=1%
- **%INI://%** will pull a value from a Section in an `.ini` file and make it the device name, e.g. `%INI://\pdb.ini?SC=Device&NM=DeviceName%`
- **%EXE://%** will get the exit code of the executable and make it the device name, e.g. `%EXE://\windows\system32\calc.exe%`
- **%STDOUT%** will pull the first line of STDOUT output of the Executable and make it the device name, e.g. `%STDOUT://cmd.exe /c dir%`

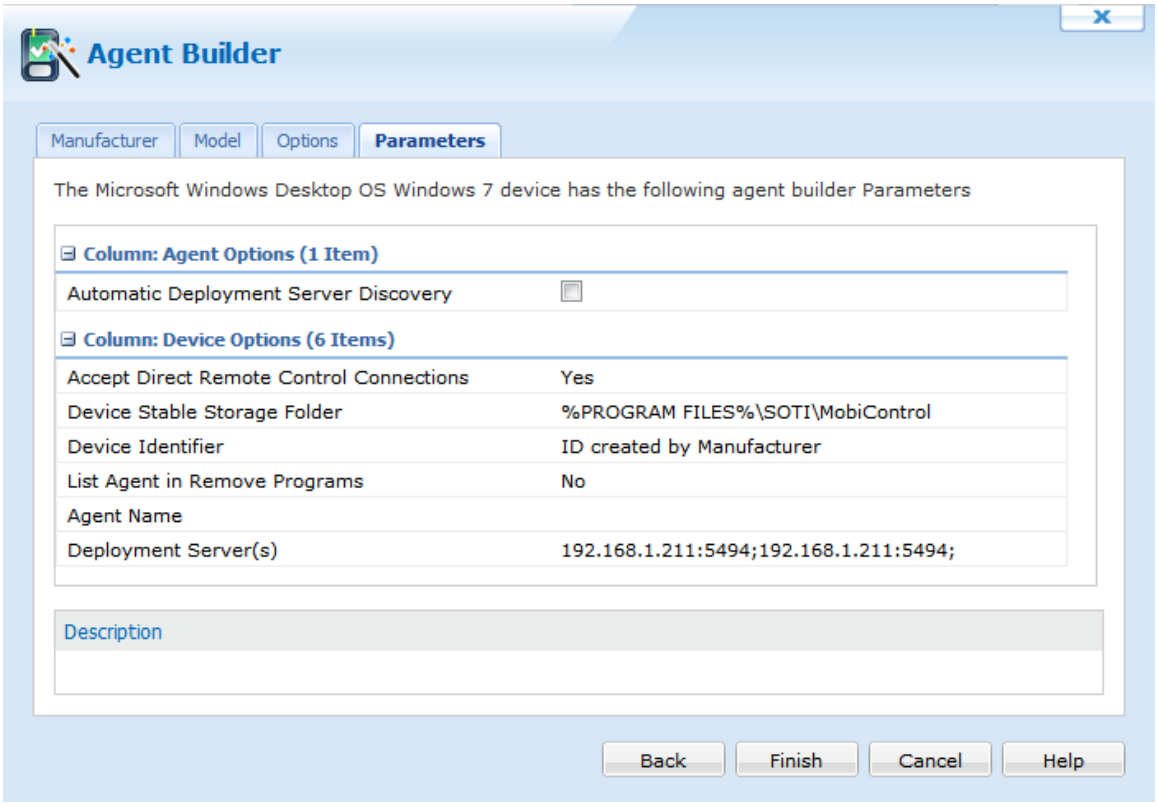
Include Initial Package

This feature allows you to specify a package that will be embedded into the Device Agent installer and automatically execute when the agent is installed on the device.

Click **Next** when you have completed the settings in this dialog box.

5. Configure software settings

The **Software Settings** page allows you to configure various parameters built into the agent. Click the **Next** button when you have completed the settings in this dialog box.

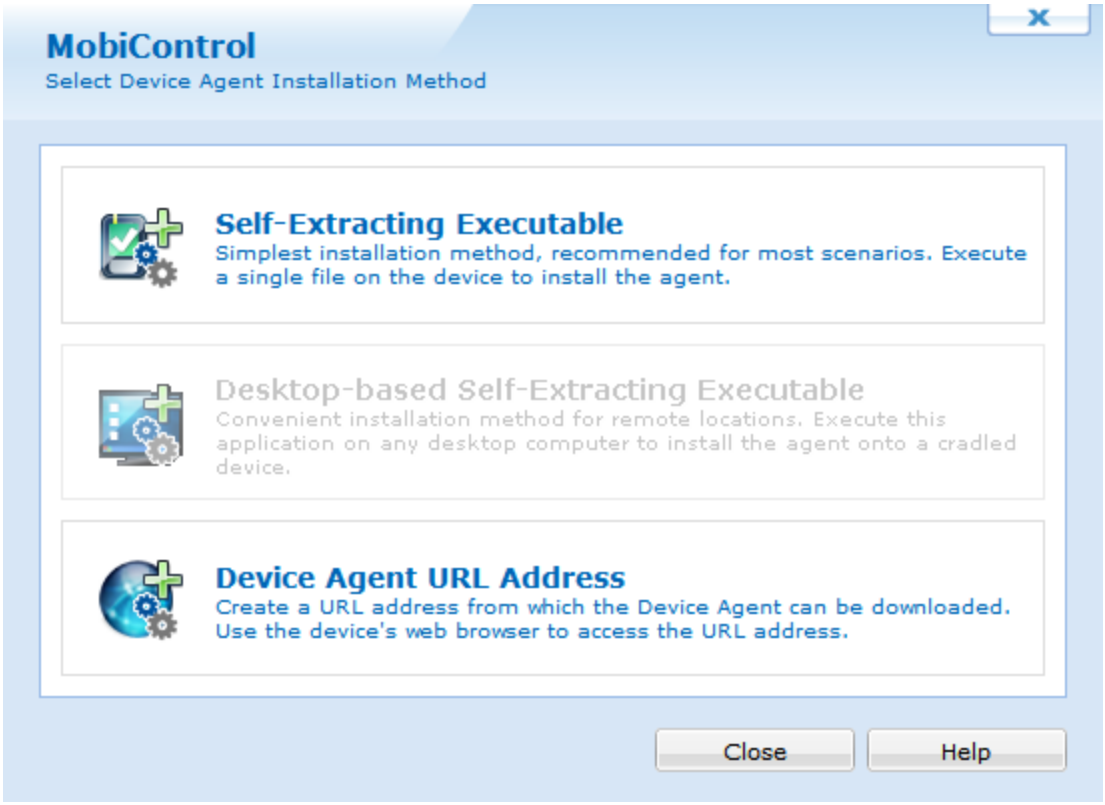


Device Agent Wizard - Software Settings page

Field Name	Description
Deployment Server(s)	Devices that have the MobiControl Device Agent software installed onto them connect to MobiControl Deployment Servers to receive configuration information as well as to get provisioned with software and data. It is crucial that the device is able to reach the IP address of the Deployment Server via the IP network to which the device is connected. If your device will be on a public network such as the Internet, you will need to setup an externally routable address for your Deployment Server. Please see the "Registering MobiControl" topic on page 608 for instructions on setting up an external IP address for the Deployment Server. **NOTE:** Configuration of the Deployment Server address should be performed before agents are created, as the address information will be embedded into the agent installer.

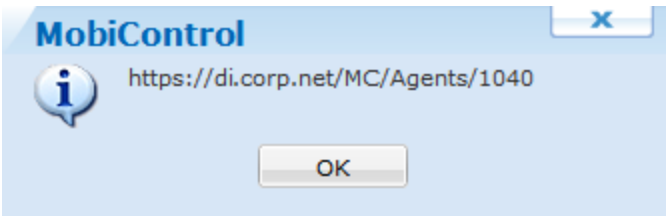
Field Name	Description
Automatic Deployment Server Discovery	When this option is enabled, MobiControl Device Agent(s) will attempt to discover Deployment Server(s) using UDP broadcasts when they cannot connect to configured servers. If you have multiple MobiControl installations on the same network, you need to set a unique site name for each installation so that the discovery process will not detect servers in a different installation.
Accept Direct Remote Control Connections	When this option is enabled, the Device Agent will accept direct remote control connections (TCP/IP remote control connection profile). A direct connection improves performance by reducing latency, however it requires the device to accept the connection without authentication unless SSL Security is enabled. (Please see the "Communication and Connection Security" topic on page 411 for more information about this.) Remote control is permitted via the TCP/IP(Server) remote control connection profile regardless of this setting.
List Agent in Remove Programs	When this option is disabled, no entry will appear for the agent in the Remove Programs settings applet on the device, thus preventing the agent from being uninstalled by the device user.
Device Stable Storage Folder	A stable storage folder is a special folder in the devices file system that is not erased when a device is hard reset. MobiControl uses the stable storage folder on the device to store data and packages so that MobiControl and packages and settings deployed via MobiControl can persist through hard reset.

6. Provisioning agent on a device



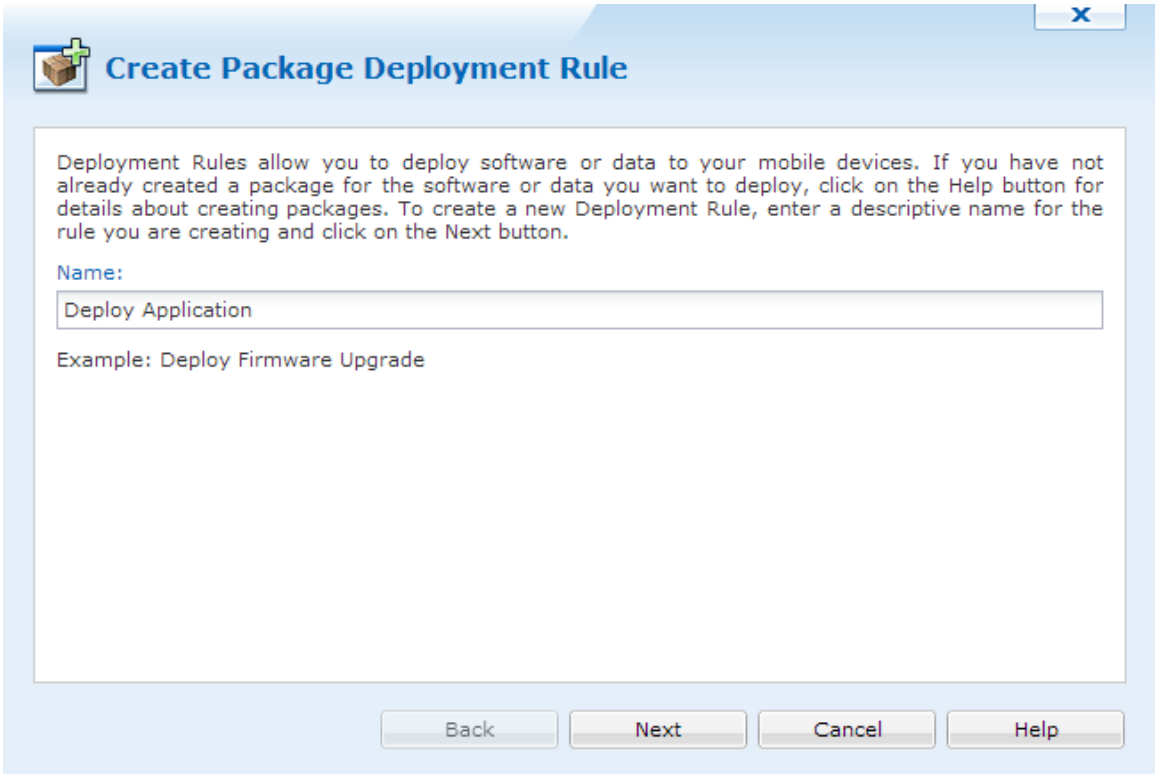
Provision Device Page

After the agent is created, you have three installation options.

Option	Description
Self-Extracting Executable	This is the simplest installation method and is recommended for most scenarios. A single executable file (`*.exe`) will be exported. To install the agent, simply deliver this file to the device and execute it. The self-extracting executable contains the agent's installation `.cab` file, as well as any other supporting files that may be required for targeted device platform.
Device Agent URL Address	This option posts the device agent's `.exe` file in a special directory on the MobiControl Web Console allowing you to send the URL to the end user to have them download and install the MobiControl Device Agent quickly and easily. 

Deployment rules allow administrators to automatically provision mobile devices with packages that contain software or data. The following series of steps describes how to use the Create Deployment Rule Wizard to create a deployment rule.

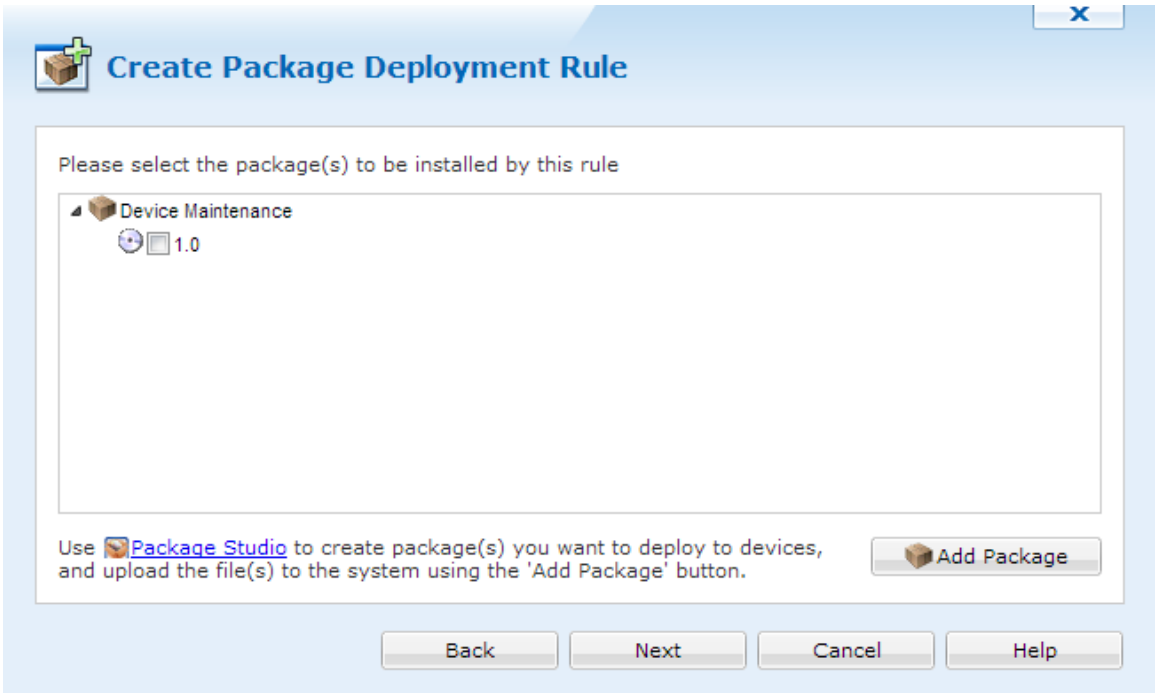
1. Start the wizard.



First page of the Create Deployment Rule Wizard

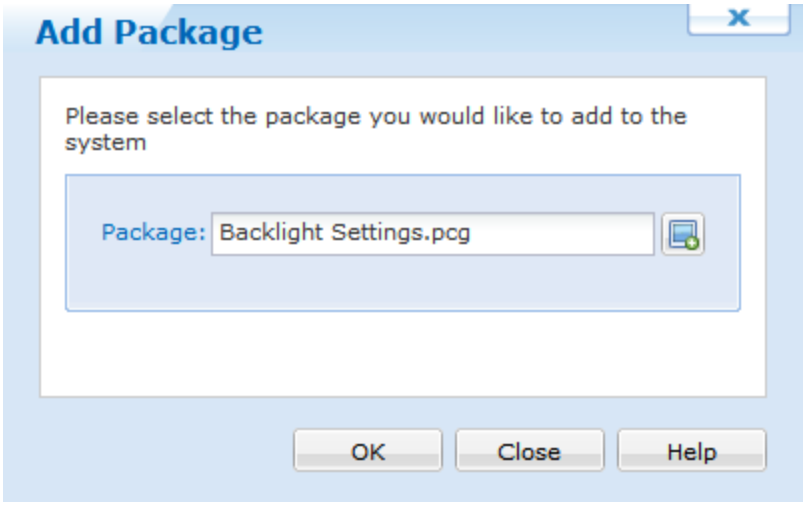
From MobiControl Manager select the **Rules view (tab)**, then click the **Rule** menu, click **Create Rule**, and click **Deployment Rule**. The first page of the Create Deployment Rule Wizard will be displayed. Enter a descriptive name for the deployment rule you are creating and click **Next**.

2. Select the package(s) to be deployed.



Select Package page

The dialog box displays a list of the packages that have been previously loaded into the MobiControl database. Select the relevant packages that need to be installed by this rule.

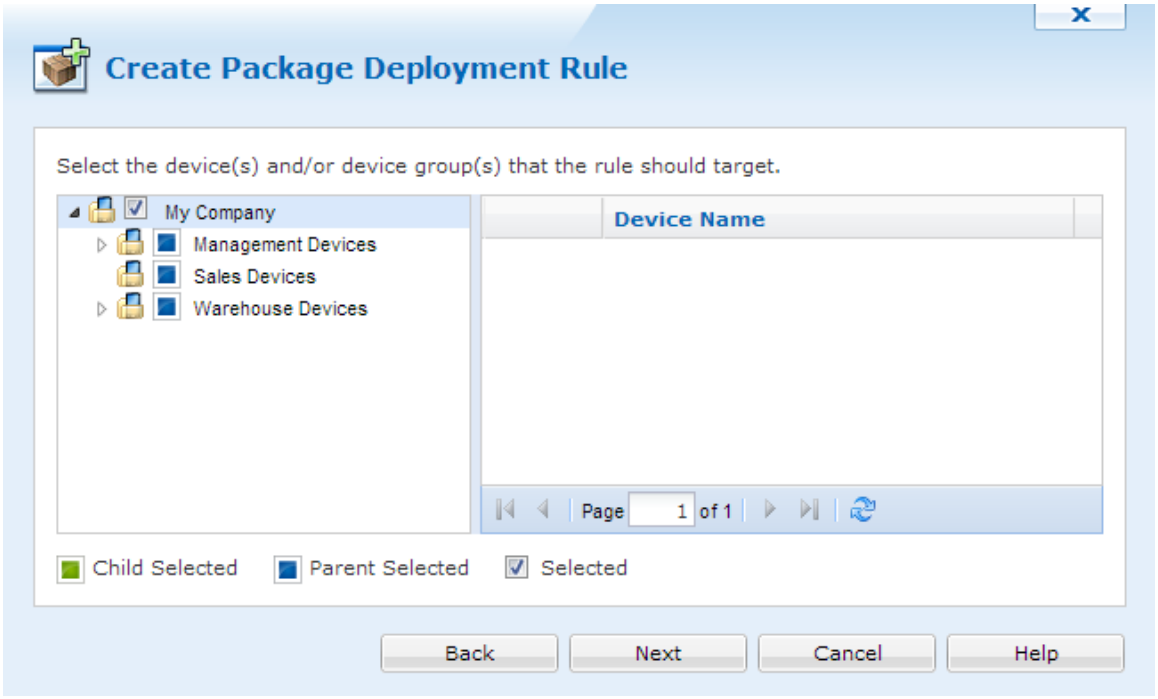


Add Package dialog

If the package to be installed has been created but not loaded into MobiControl, click the **Add Package** button and select the package file from the file system.

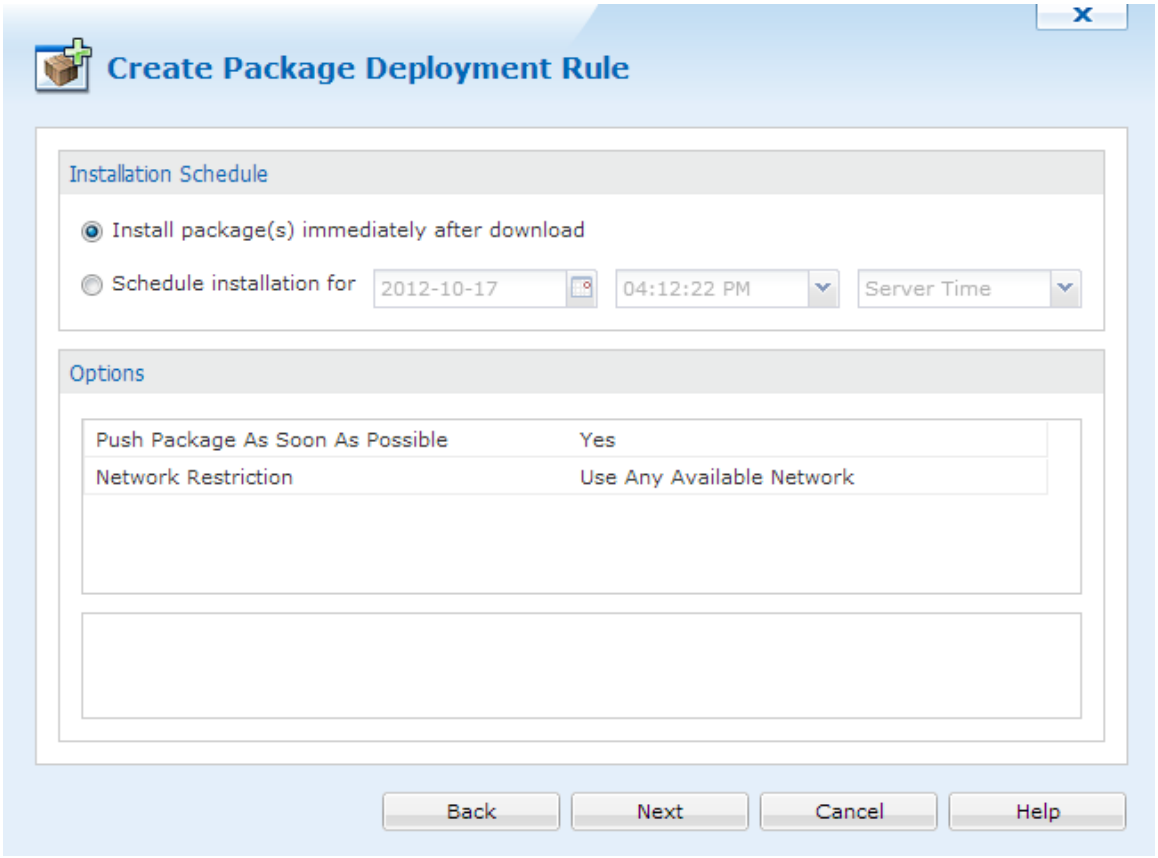
If the package has not yet been created, exit the wizard and use MobiControl Package Studio to create a package. (Please see the "MobiControl Package Studio" topic on page 413.)

3. Select where the package(s) will be deployed.
   Select the device(s) or group(s) to which the package(s) will be deployed and click the **Next** button.



Device Group Selection page

4. Configure deployment rule activation schedule and optional settings.



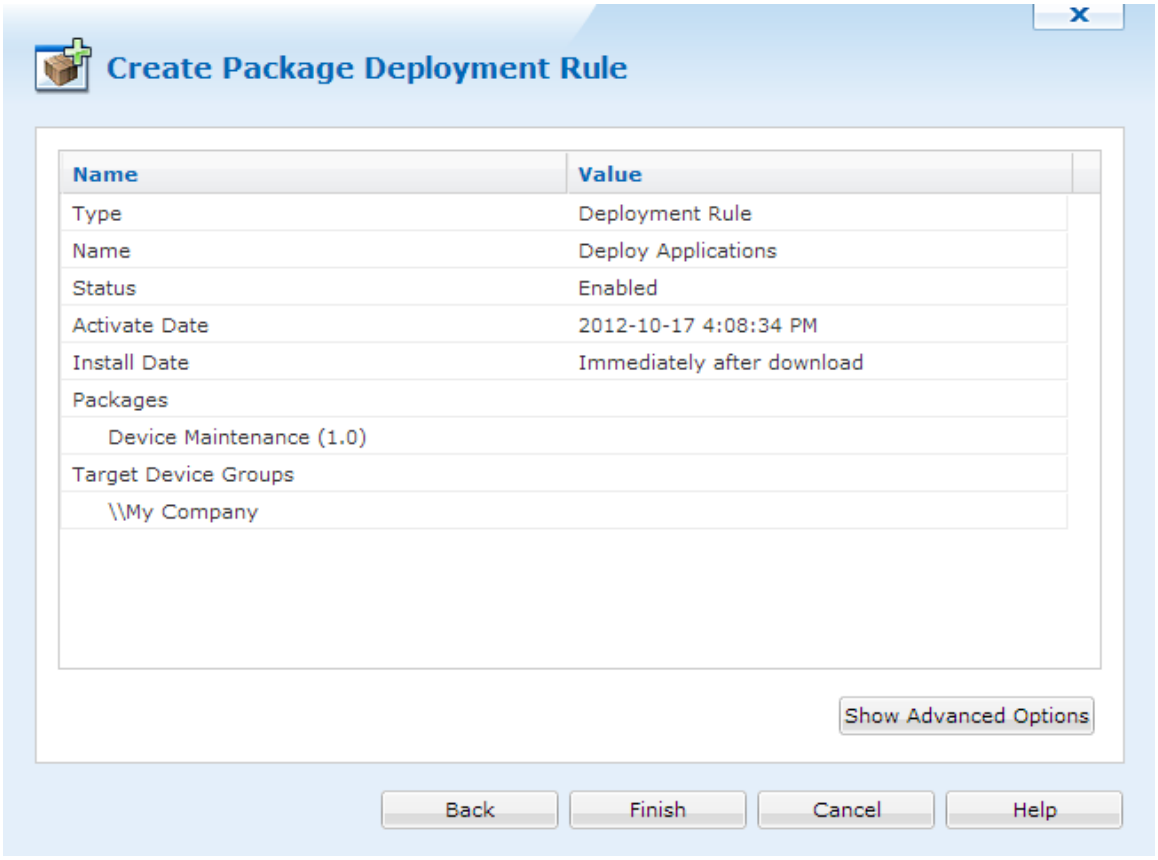
Device Settings Configuration page

The deployment rule can be deployed at real-time or at a pre-set time. The deployment rule, although set to be activated at a scheduled time, can also be set to be deactivated. The deactivation setting is optional.

Field Name	Description
Install immediately after download	If this checkbox is cleared, the installation of a downloaded package will be delayed till the specified Installation Date. The Installation Date must be after the Activate Date. If a package depends on another package that is scheduled to install at a later time, then the Deployment Server will not push the package unless it is also scheduled to install at the same time or later. Please see the "Windows Desktop Packages Tab" topic on page 1.
Push Packages As Soon As Possible	By default, packages will be deployed to the devices according to the device synchronization schedule. The device synchronization schedule is specified by the add devices rule used to add the device to MobiControl. If this option is selected, package(s) will be deployed to the target devices immediately. If the devices are currently offline, the package(s) will be deployed as soon as the device connects to MobiControl.
Network Restriction	Restrict whether package deployment should take place over cellular data networks.
Persistently Store Package(s)	For devices with stable storage, persistently storing packages allows them to be reinstalled after a hard reset, without needing to connect to the Deployment Server.
Uninstall Contents upon Rule Deletion	This is relevant when the rule has been deleted or is no longer assigned to a device, for instance because it was moved to a new group or the rule was edited to target a different group. • If **Yes** is selected, the package will be removed from the device, and the uninstallation logic of the packages will be executed. • If **No** is selected, the package will be removed from the device, but no uninstallation logic will be executed. The uninstallation logic depends on what the package contains, for example, when a rule that deploys a package containing a `.cab` file is deleted. • If the **Uninstall Package(s) upon Rule Deletion** option is set to **Yes,** the application installed by the `.cab` file will be removed. • If the **Uninstall Package(s) upon Rule Deletion** option is set to **No**, the application installed by the `.cab` file will remain installed.
Always Force Reinstall	Packages will be reinstalled on to the device regardless of whether they are already installed.
Rule Priority	This option allows you to prioritize the deployment of the package(s). Package dependencies (introduced in version 3.06) are the recommended means to ensure the order in which packages are installed on the devices. Please see the "Windows Desktop Packages Tab" topic on page 1 for more information.
Enable Rule	If you wish to activate the rule, that is, to install the package(s), then this field needs to be checked. This option is also made available by right-clicking the rule in the Rules view (tab). When you disable a deployment rule, MobiControl will attempt to uninstall the packages that were being deployed by that rule. If the package(s) that were being deployed contained `.cab` files, MobiControl will try to uninstall the `.cab` files as well.

5. Review the summarized information.

   A **summary** of the deployment rule is displayed. Review the settings you have chosen and click **Finish** to complete the wizard.



Summary page

NOTE:

After five unsuccessful attempts to deploy the package, deployment to that device is temporarily deferred. In order to start deployment of that package again, you must right-click the package from the Package panel and select **Force Re-install**.

Creating File Sync Rules

File sync rules allow you to synchronize files and folders between your devices and a server. File collection, also referred to as file uploading, is a very convenient method for gathering information from devices, for example a transaction log file. File dissemination, also referred to as file downloading, is a

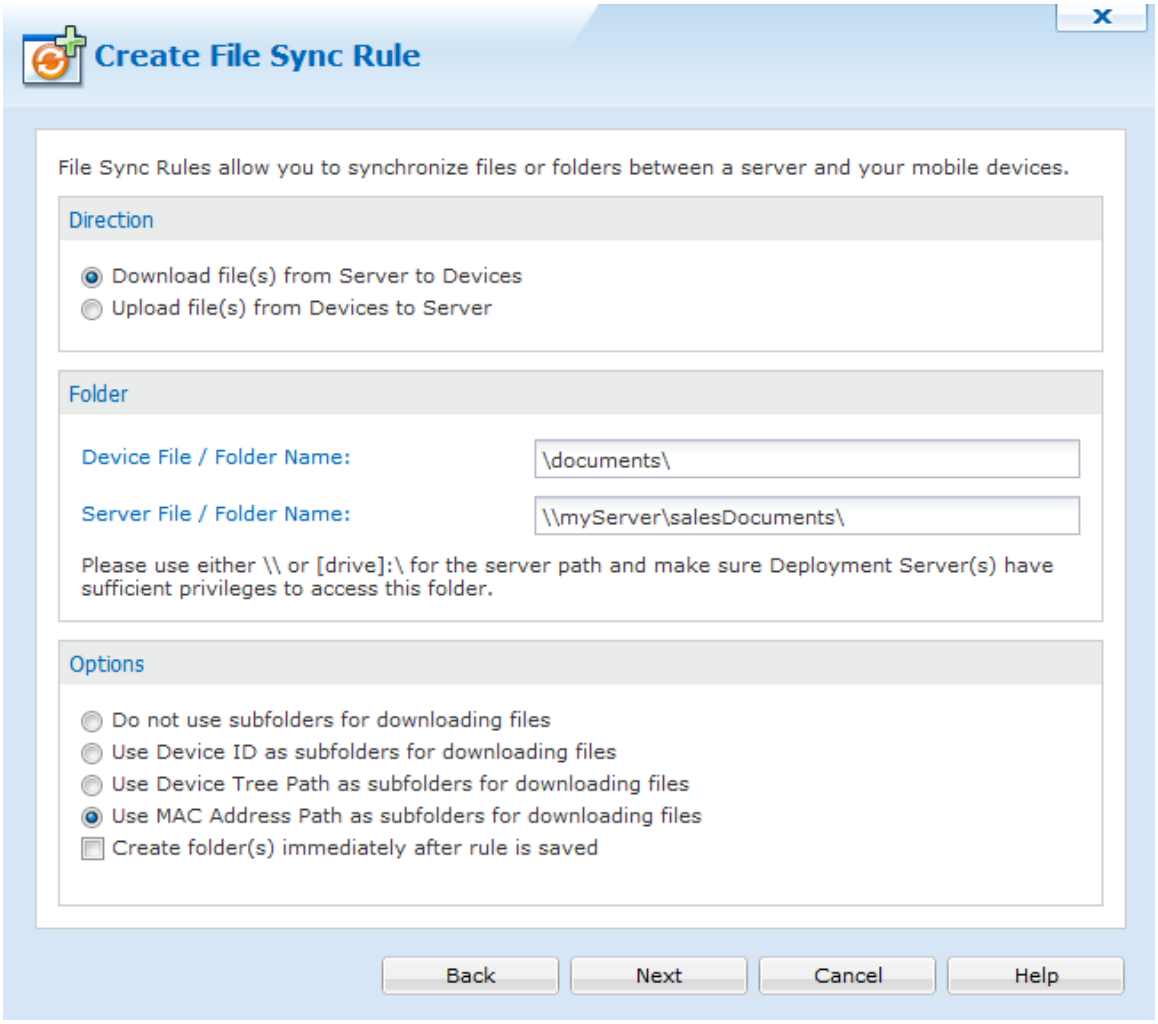
quick and easy way to send one or more files to a set of devices such as an updated product listing or configuration file.

1. Start the wizard.

   Select the Rules view (tab), then click **Rule,** point to **Create Rule,** and click **File Sync Rule.** Enter a meaningful name for the rule.

First page of the Create File Sync Rule Wizard

2. Configure file synchronization source and destination.



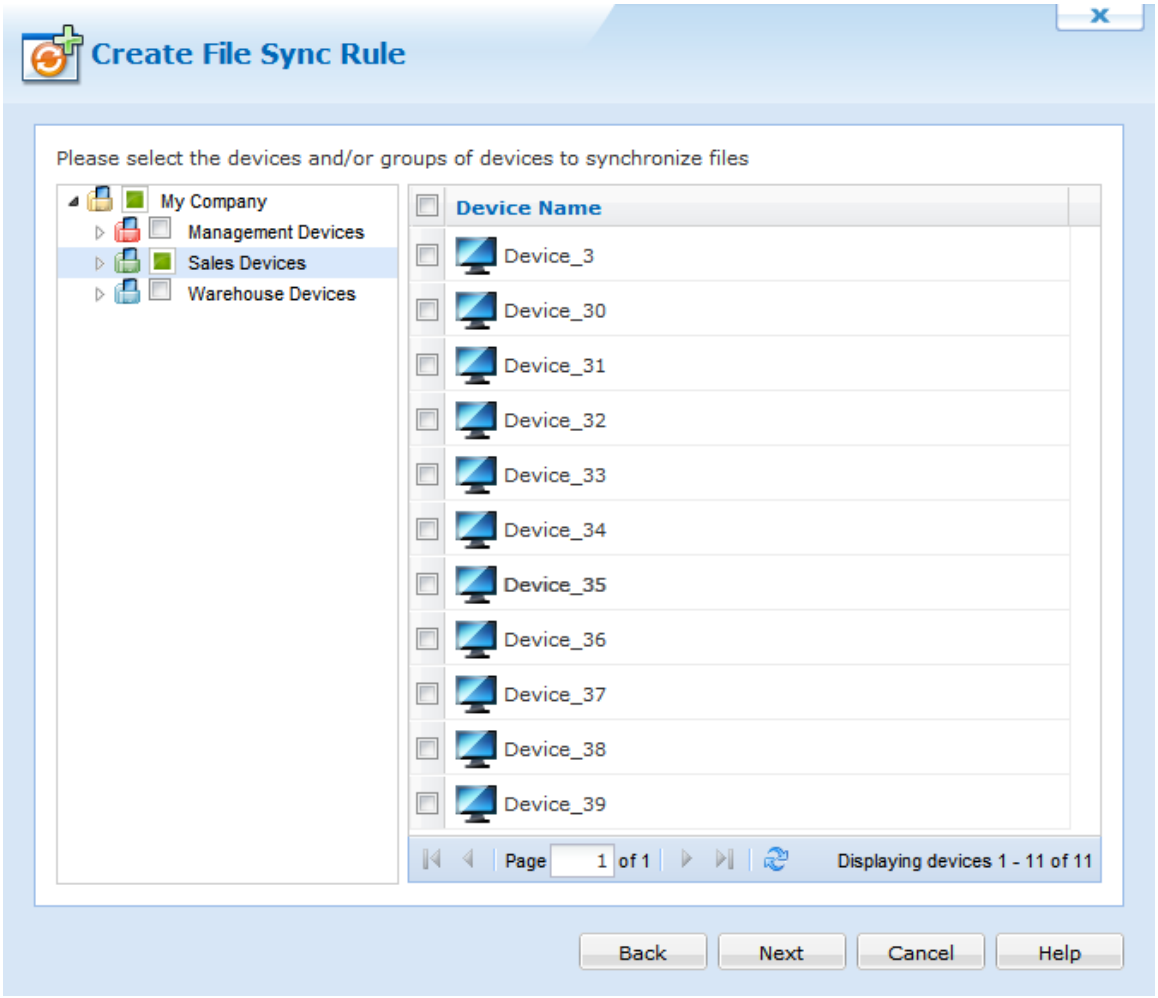
Configure file sync source and destination

The following table describes the fields of this page of the wizard:

Field Name	Description
Direction	• **Upload** (File collection) The rule will be used to upload files from the devices to a server. • **Download** (File dissemination) The rule will be used to download files from the server to devices.
Device File/Folder	Specifies the complete file system path to the files or folders being synchronized on the device
Server File/Folder	Specifies the complete file system path to the files or folders being synchronized on the server It is strongly recommended that a UNC (Universal Naming Convention) path be used. A local path (i.e. `C:\MyFiles`) can be used if only one Deployment Server is being used and the local path is on the computer running the Deployment Server. **NOTE:** It is important that the Deployment Servers have sufficient permission to read and write to the source or destination UNC path. Best practice is to run the Deployment Server under its own Active Directory user profile.
Server-side Folder Options	For **upload rules,** files collected from the devices can be written to: • A single shared folder, meaning files could potentially be overwritten if they have the same name. • A per-device subfolder, named using the device ID (i.e {00135304-41D7-019E-5800-0050BF3F5173}) • A per-device subfolder, named using the device tree path (i.e. `.\Management Devices\Device 0001`) For **download rules,** files disseminated from the server can be read from: • A single shared folder, meaning all devices get the same file(s). • A per-device subfolder, named using the device ID (i.e. {00135304-41D7-019E-5800-0050BF3F5173}) • A per-device subfolder, named using the device tree path (i.e. `.\Management Devices\Device 0001`) When the **Create folder(s) immediately after rule is saved** option is enabled, the server-side folders will be created immediately after the file sync rule is saved. This allows adding files to the folders on the servers that are synchronized with the devices when the file sync event occurs.

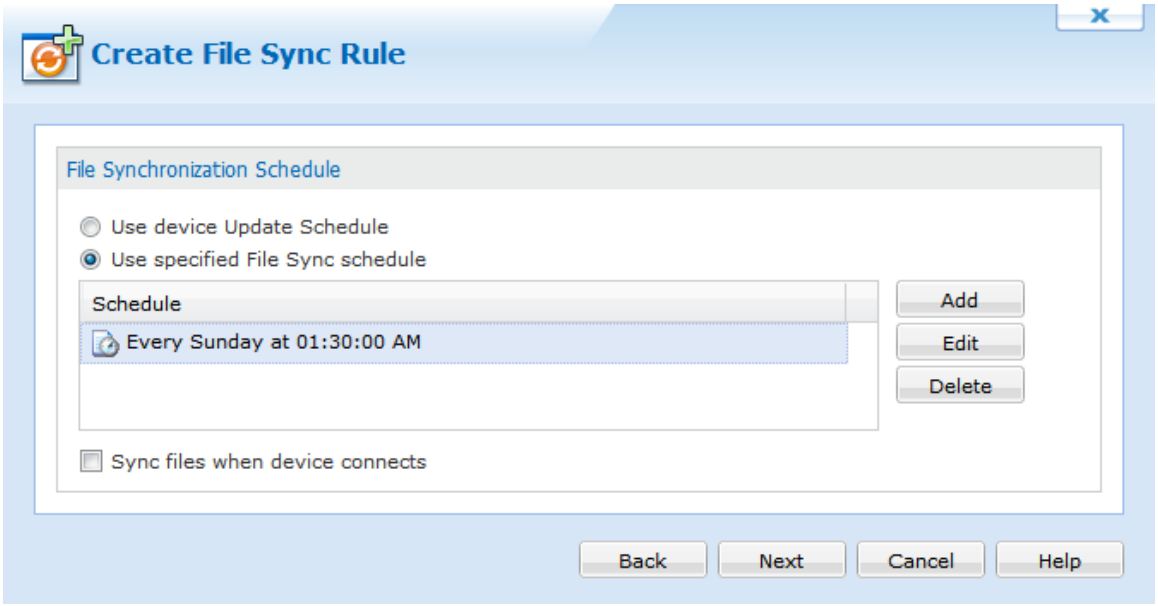
3. Select devices.

   Select the device(s) and group(s) for which the file sync rule will apply.



Device Group selection page

4. Specify the synchronization and activation or deactivation schedule.



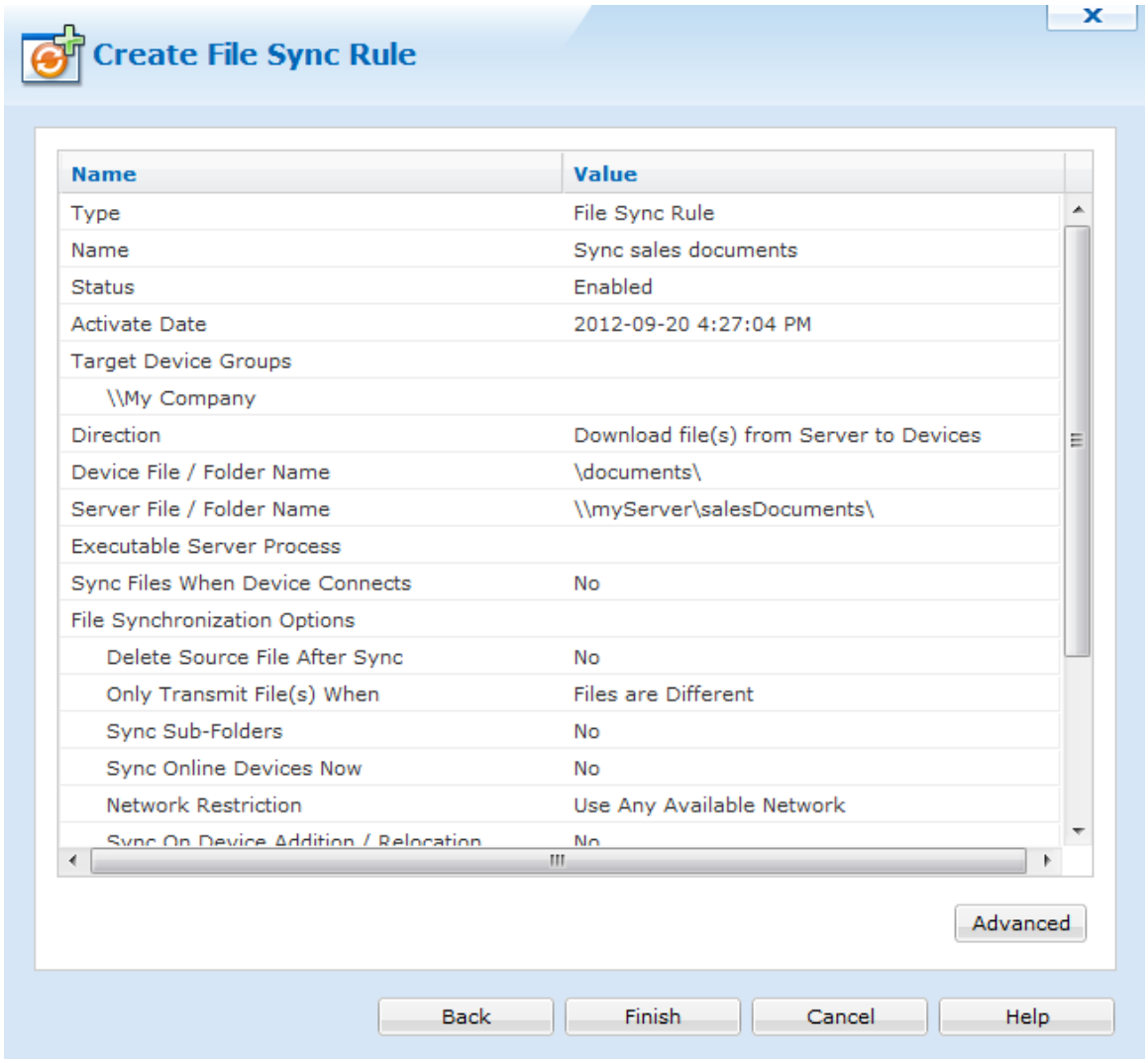
Rule activation schedule

Field Name	Description
Use Device Update Schedule	By default, the device update schedule (specified by the file sync rule used to add the devices to the system) triggers file synchronization
Use Specified File Sync Schedule	If you specify a file synchronization schedule in this dialog box, only that schedule will be used, and the device synchronization schedule will not trigger file synchronization. To Specify the custom schedule click the **Add** button. Please see the "File Synchronization Schedule" topic on page 914 for more information about creating a custom file sync schedule.

By default, the file sync rule will be activated immediately upon completion of the wizard. If you wish to delay the activation you can modify the activate date. A deactivate date can optionally be entered to specify a date from which the rule will be disabled. A file sync rule can also be explicitly disabled by clearing the **Enable Rule** check box.

5. Review summarized information.

Review information on the **file sync rule summary page**. This page gives you an opportunity to review the settings of the file sync rule before committing them. If you wish to make any corrections, click the **Back** button.



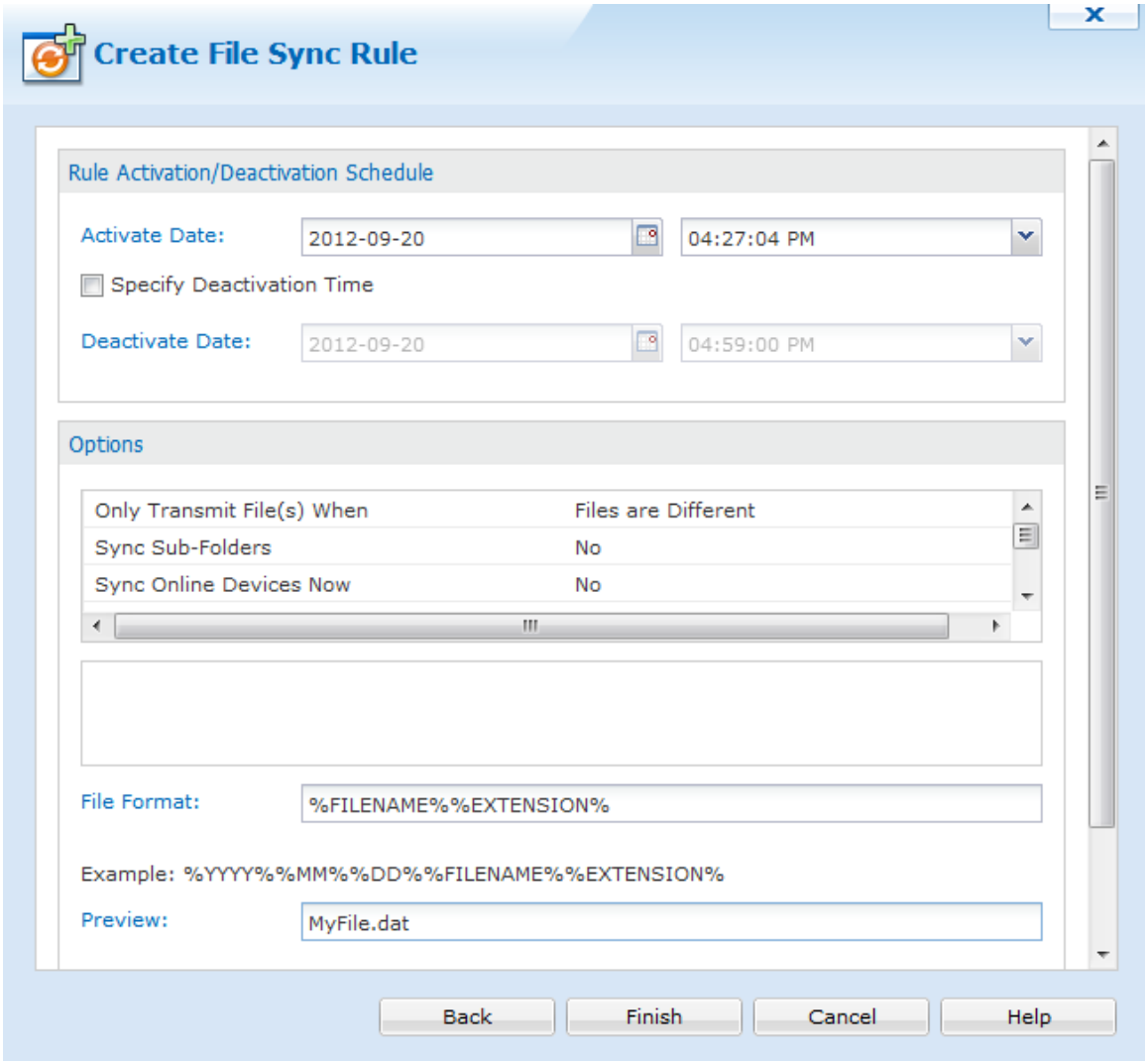
Summary page

6. Specify the synchronization options.

The following table describes the file synchronization options on this page of the Create File Sync Rule Wizard:

Field Name	Description
Delete Source File After Sync	(This applies only to upload rules.) When selected, the source file(s) on the device are transmitted to the server and then deleted from the device.

Field Name	Description
Only Transmit File (s) when	• The **Always Transmit** option will cause file(s) to be uploaded or downloaded regardless of whether or not the source and target are different or the same. • The **Files are different** option will cause file(s) to be uploaded or downloaded only if the source file is different from the destination file. • The **Source file is newer** option will cause file(s) to be uploaded or downloaded only if the source file has a more recent date-time stamp. • The **Destination file does not exist** option will cause file(s) will cause file(s) to be uploaded or downloaded only if the destination file does not exist.
Sync Sub-Folders	Synchronize files in sub-folders in addition to the files located in the target folder
Sync Online Devices Now	File synchronization will be executed immediately following the completion of the wizard for online devices.
Sync On Device Addition or Relocation	Perform file synchronization when a device is added or relocated to a device tree group for which this rule has been configured This setting is useful to easily invoke file synchronization when a device is moved from one group to another in the device tree.
Network Restriction	Restrict whether file synchronization should take place over cellular data networks (i.e. GPRS)
Upload File Name Format	Allows you to customize the names of the files that are uploaded from the devices For example, you can augment a file name with the date-time stamp of when it was uploaded. These are available file-name macros: • **%YYYY%** is for the year (e.g. 2006). • **%MM%** is for the month of year (e.g. 12 is December). • **%DD%** is for the day of month (e.g. 31). • **%H%** is for the hour in the 24-hour format (e.g. 14). • **%M%** is for the minutes (e.g. 30). • **%S%** is for the seconds (e.g. 55). • **%FILENAME%** is for the original file name (e.g. `mylogfile`). • **%EXTENSION%** is for the original file extension (e.g. `.txt`).
Use Common Cache Mode	The option to use the new, advanced caching mode of the files being disseminated is applicable only when syncing files from the server to the device. This option is set to **Yes** by default. When enabled, a single, shared, cached copy of each file being disseminated is stored on the Deployment Server. If you are experiencing issues with file synchronization, set this option to **No.**



File synchronization options

Click the **Scripts** button to configure file synchronization scripts.

File Synchronization Scripts

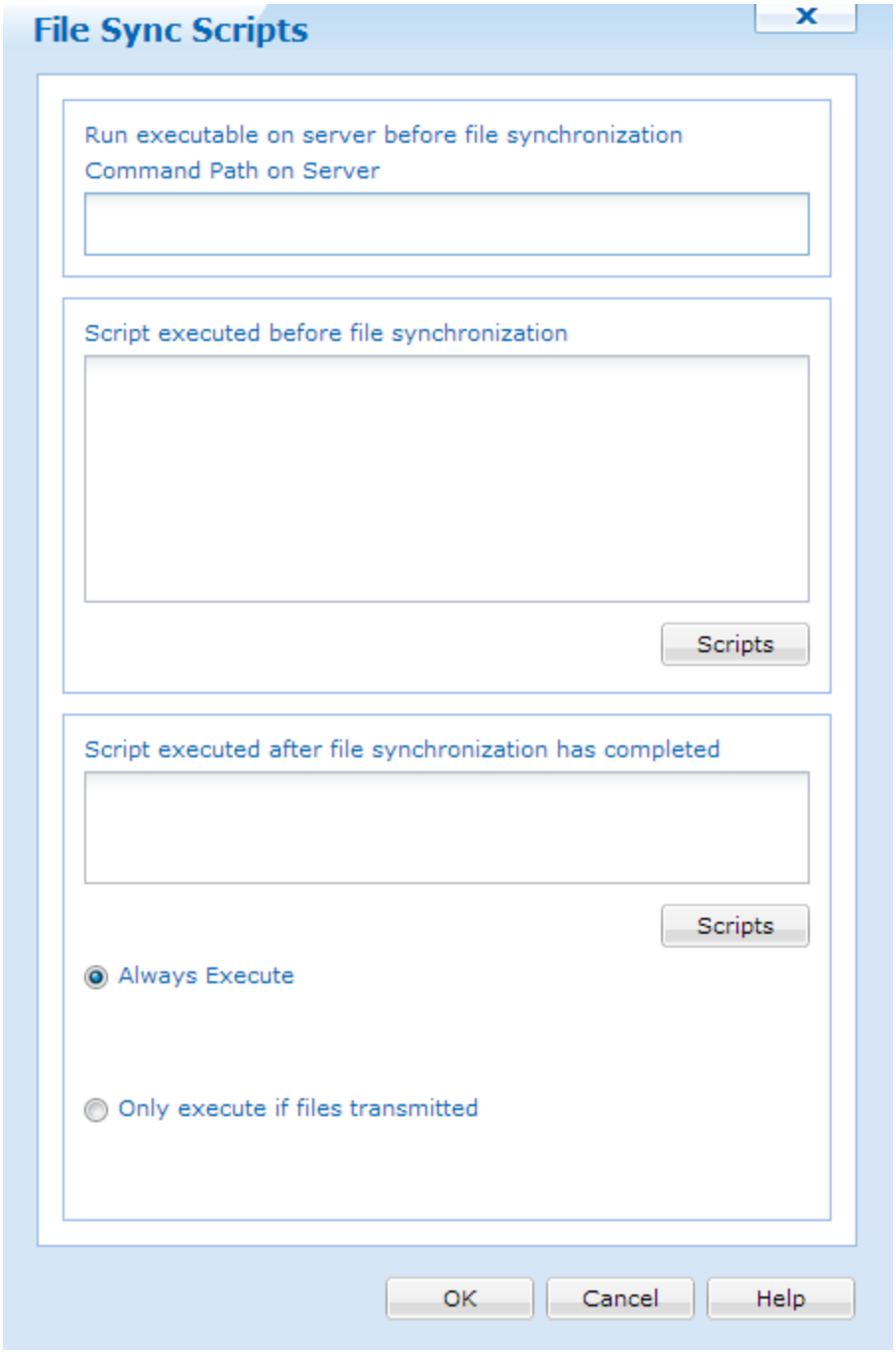
File synchronization scripts provide flexibility in automating actions on the server before the file sync or on the device pre or post file synchronization.

EXAMPLE: RUN EXECUTABLE ON SERVER

MobiControl contains plenty of server side utilities used to manage devices in the deployment server. One of these utilities is a device move. If this utility is ran before the file sync, we can ensure that all the devices are in the proper location before syncing the files down. For additional help with this utility and more, please contact us.

EXAMPLE: PRE AND POST FILE SYNC

Before collecting a log file from the device, stop a certain running process (e.g. `kill abc.exe`). After the file has been collected, restart the process (e.g. `start abc.exe`).



File synchronization advanced options

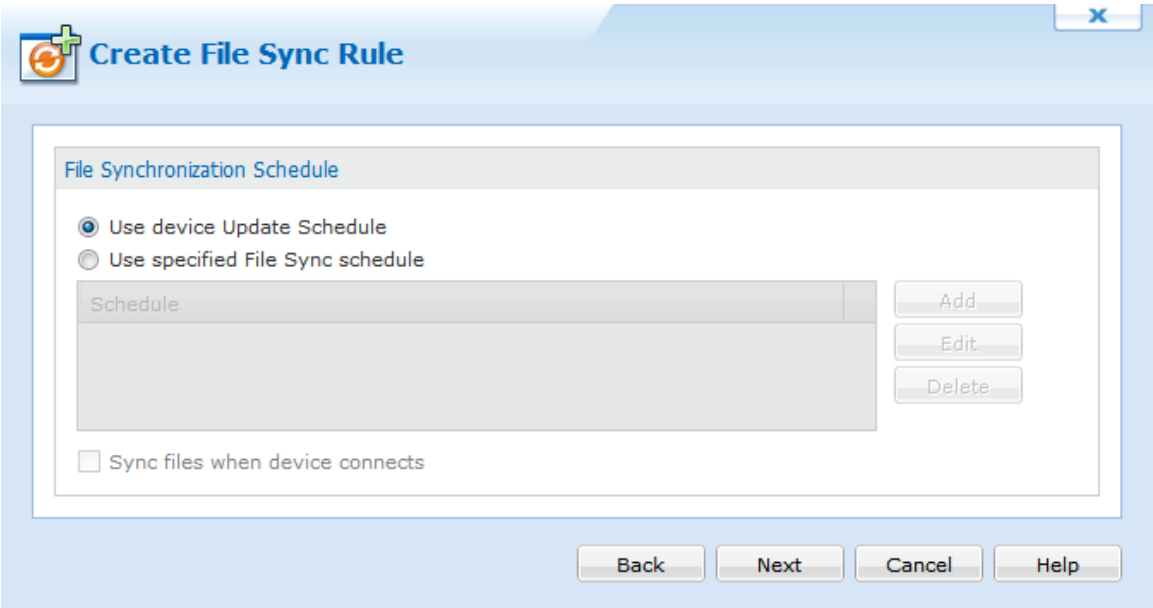
Field Name	Description
Always execute	Will execute the script every time there is a scheduled sync, even if the files are updated or not
Only execute if files transmitted	Will execute the script when files have been updated by the sync schedule
Scripts	Will allow you to import previously created scripts

File Synchronization Schedules

The file synchronization schedule specifies when the Deployment Server(s) should check device(s) for synchronization.

If the Deployment Server identifies an inconsistency, such as a mismatch in the file size or finds the new file, the Deployment Server will act according to the file sync rule.

By default, the device synchronization schedule, specified by the add devices rule used to add the devices to the system, is selected for file synchronization. You may add, edit or delete the custom schedule using the following dialog box.



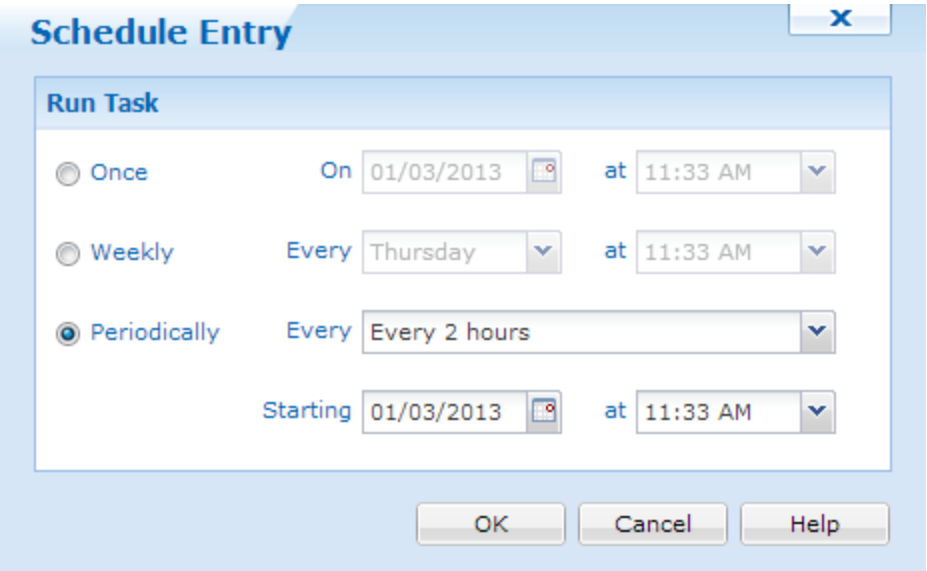
Create File Sync Rule Wizard dialog box

The following table describes the fields of the Create File Sync Rule Wizard dialog box.

Field Name	Description
Add	Specify your own file synchronization intervals. When you select **Add,** the **Schedule Entry** dialog box is displayed. **EXAMPLE:** To sync twice a week (Monday at 06:00 and Friday at 19:00), create two weekly schedule entries.
Edit	Select **Edit** to modify an existing schedule entry. The **Schedule Entry** dialog box is will be displayed.
Delete	Permanently remove a file sync schedule entry from the dialog box
Sync Files when device connects	Sync whenever devices under this rule connect to a Deployment Server (i.e. transition from offline to online)

Schedule Entry

The **Schedule Entry** dialog box allows you to specify schedule entries as one-time or periodic events.



Schedule Entry dialog box

Field Name	Description
Once	Device will check for file synchronization once at the specified date and time.
Weekly	Device will check for file synchronization once a week, on a specified day and time.
Periodically	Device will check for file synchronization periodically at the specified interval from the set, start date-time.

Windows Desktop Device Relocation

Dynamic device relocation allows you to set up rules to move your mobile devices automatically between different virtual groups or device groups in the MobiControl device tree based on the IP address or other custom criteria. This is useful when managing mobile devices in a deployment where the device tree is set up to represent different physical locations (e.g. retail stores, warehouses, regional offices, etc.).

In a deployment that has mobile devices connecting from and moving frequently between several different sites, properties or regions, the administrator needs visibility over the movement of mobile devices across different locations. Dynamic device relocation allows the MobiControl device tree to be updated automatically when a device moves to a different location (e.g. a mobile device that has moved from a warehouse or site in Chicago to a site in New York will automatically be relocated in the device tree on reconnection and will appear in the device group for devices in New York based on the new IP address information). Additionally, the devices can also be automatically reconfigured and any modifications to the mobile device settings, specific to the new location, will be sent to the device automatically.

The devices are relocated based on the IP address ranges specified for each location. You can also create a custom data identifier which can be the criterion that will be utilized to relocate the devices to the appropriate device group. (Please see the "Windows Desktop Custom Data" topic on page 839 for detailed information on custom data identifiers.)

1. Start the wizard.

   From MobiControl Manager, select the Rules view (tab), then click **Rule,** select **Create Rule,** and click **Create Device Relocation Rule.** The first page of the Create Device Relocation Rule Wizard will be displayed. Enter a meaningful name for the rule and click **Next** to continue.

Create Device Relocation Rule Wizard startup dialog box

2. Review the device relocation mappings.

This page lists **device relocation mappings** that determine how the devices would be relocated and in which groups they would appear if the specified criteria is met. When a device connects to the MobiControl Deployment Server, its IP address and custom data information will be checked against all device relocation rules configured, and it will be moved to the appropriate device group based on the information in the relocation mappings.

NOTE:

Devices that are already connected and online in MobiControl will be relocated when they disconnect and re-connect to the MobiControl Deployment Server.

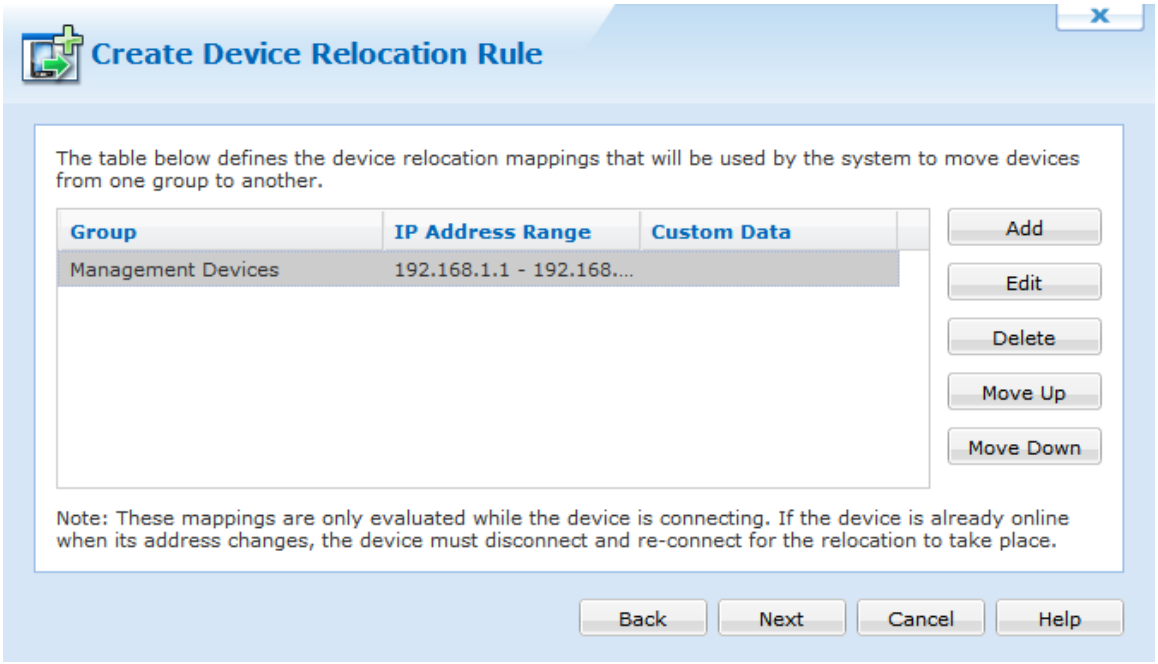
Edit Device Relocation Rule dialog box

The buttons on the **Edit Device Relocation Rule** dialog box are explained below:

Button Name	Description
Add	Click the **Add** button to add an entry for the relocation mapping.
Edit	Click the **Edit** button to change the settings for an existing relocation mapping entry.
Delete	Click the **Delete** button to delete a relocation mapping entry.
Move Up / Move Down	Click these buttons to change the order of the relocation mappings. The entry listed higher in the list have a higher priority and take precedence over entries listed lower in the list. For more details, read about relocation mappings priority below.

A relocation mapping can use just the IP address or the custom data entry to specify the relocation rule for mobile devices. If a relocation mapping has both the IP address and custom data entry specified as the criteria, the mobile devices would be relocated only if both these conditions are satisfied. If a device is affected by more than one relocation mapping, the one

higher in the list of mappings will have a higher priority and will be effective. You can use the **Move Up** and **Move Down** buttons to change the precedence of the relocation mappings if multiple mappings apply to a device.

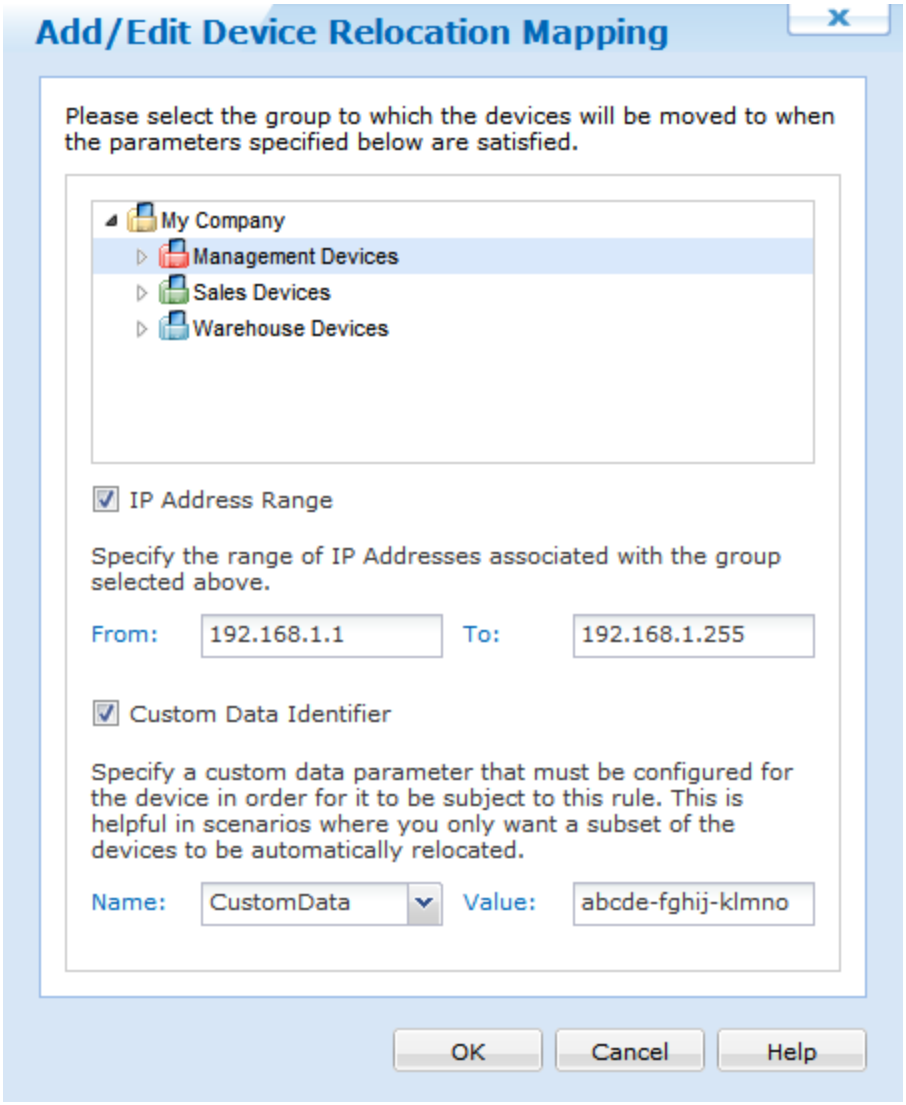


Device Relocation Mappings dialog box

The first two relocation mappings in the previous screenshot have been defined: one is for relocating all devices with IP addresses between 192.168.1.1 and 192.168.1.255 to the Management Devices group and another mapping for relocating all the devices for which the custom data item "Location" has a value of "Region A" to the Warehouses group. Since the relocation mapping with the IP address filter is listed above the mapping with the custom data filter, the IP address mapping will take precedence. If a device satisfies both conditions (e.g. has an IP address 192.168.1.10 and a value "Region A" for "Location"), it will be relocated to the Management Devices group.

3. Add or edit device relocation mappings.

   A relocation mapping includes the target or destination group (which can be a virtual group) to which the devices would be relocated. It also includes the conditions or the relocation parameters that must be satisfied for a device to be relocated.



Add/Edit Device Relocation Mapping dialog box

The **target group** is the group, sub-group, or virtual group to which devices will automatically be relocated when connecting to the Deployment Server if the conditions specified in the relocation parameters are met.

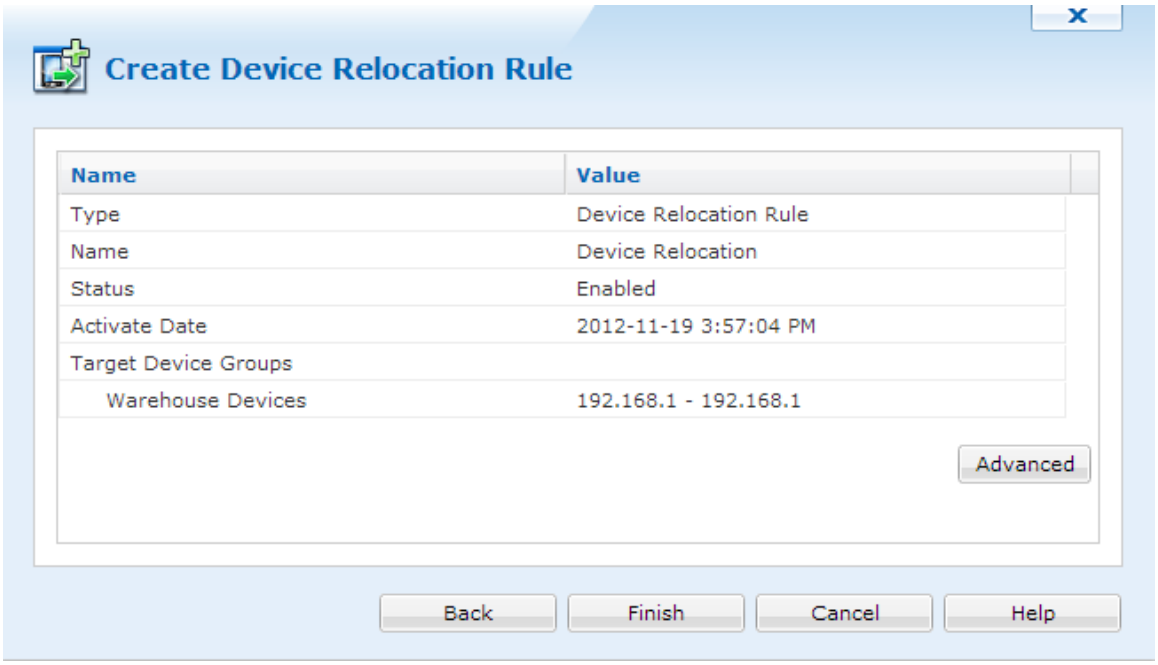
Multiple **relocation parameters** can be specified to manage the dynamic relocation of devices. A single parameter can be specified or both parameters can be used for a relocation mapping, in which case the device will be relocated if it satisfies both parameters.

The following table describes the fields of the **Add/Edit Device Relocation Mapping** dialog box:

Field Name	Description
IP Address Range	Devices can be automatically relocated based on the IP address information of the device at the time it connects to a Deployment Server. A range of IP addresses can be specified and if the device's IP is within that range, the device will be relocated to the target group.
Custom Data Identifier	You can use a custom data value as one of the criteria for relocating devices from one device group to another. MobiControl allows you to retrieve arbitrary data from the device's registry, files on the device and other sources using custom data. Please see the "Windows Desktop Custom Data" topic on page 839 for more information.

4. Review the summarized settings.

   This page gives you an opportunity to review the settings of the device relocation rule before committing them to the database. If you wish to make any corrections, click the **Back** button, otherwise click **Finish** to complete the wizard.



Edit Device Relocation Rule Summary dialog box

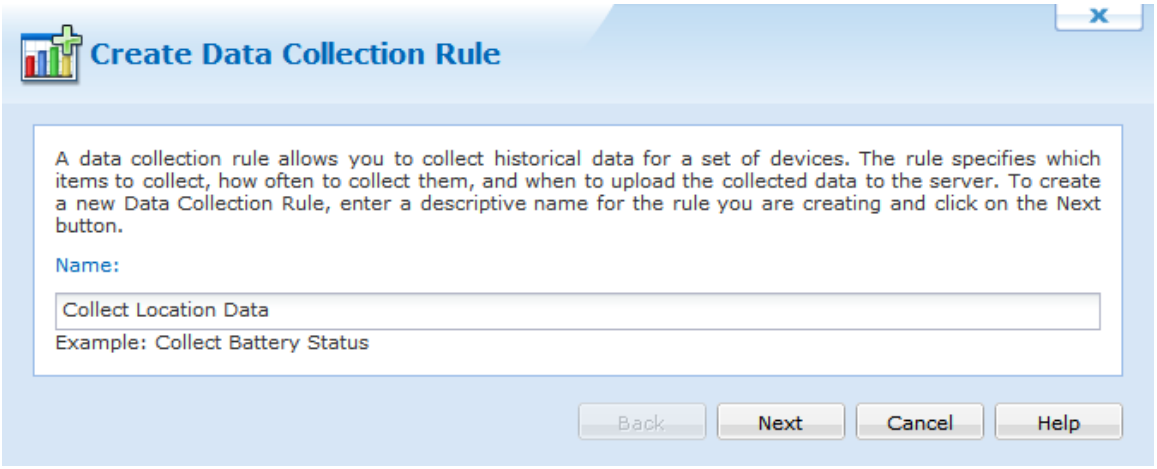
Windows Desktop Data Collection

Data collection rules allow administrators to automatically collect a variety of data from mobile device(s).

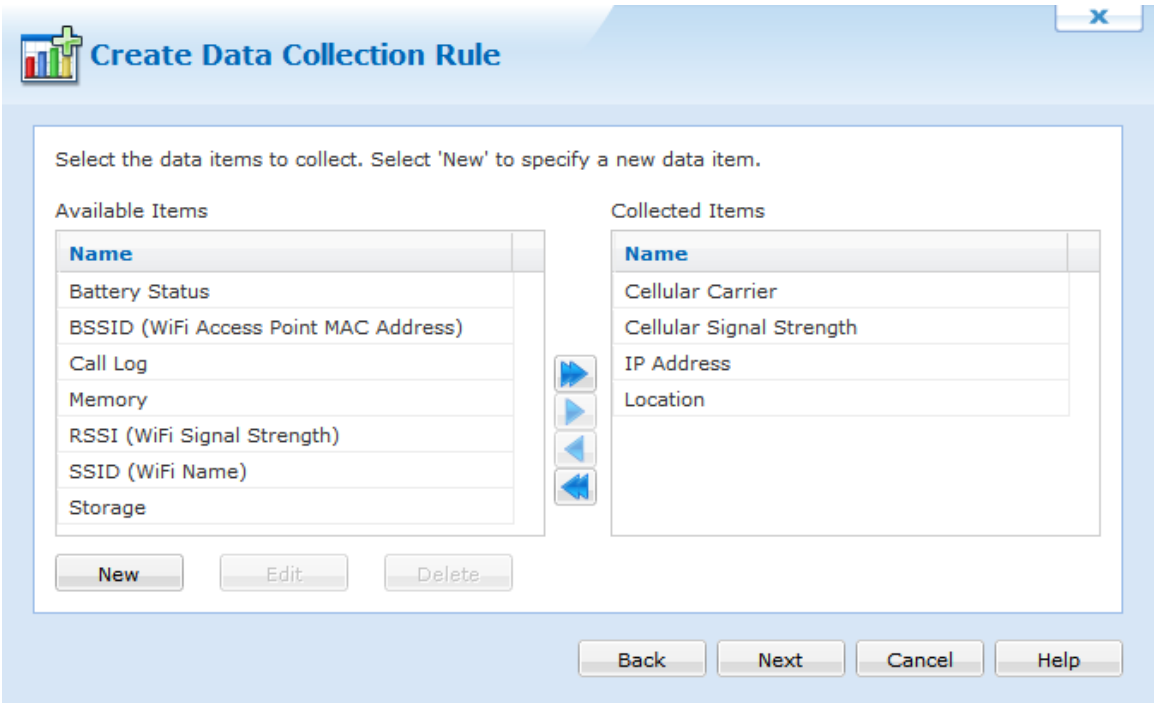
The following series of steps describes how to use the Create Data Collection Rule Wizard to create a data collection rule:

1. Start the wizard.

   From MobiControl Manager, select the Rules view (tab), then click **Rule,** click **Create Rule,** and click **Data Collection Rule**. Enter a meaningful name for your new data collection rule and then click **Next**.



2. Select data items to collect.



   Select individual items or all items from the **Available Items** list by highlighting and then select the corresponding direction arrow(s). These items will move to the **Collected Items** list. If you have added something that you would like to remove from the **Collected Items** list, simply select the

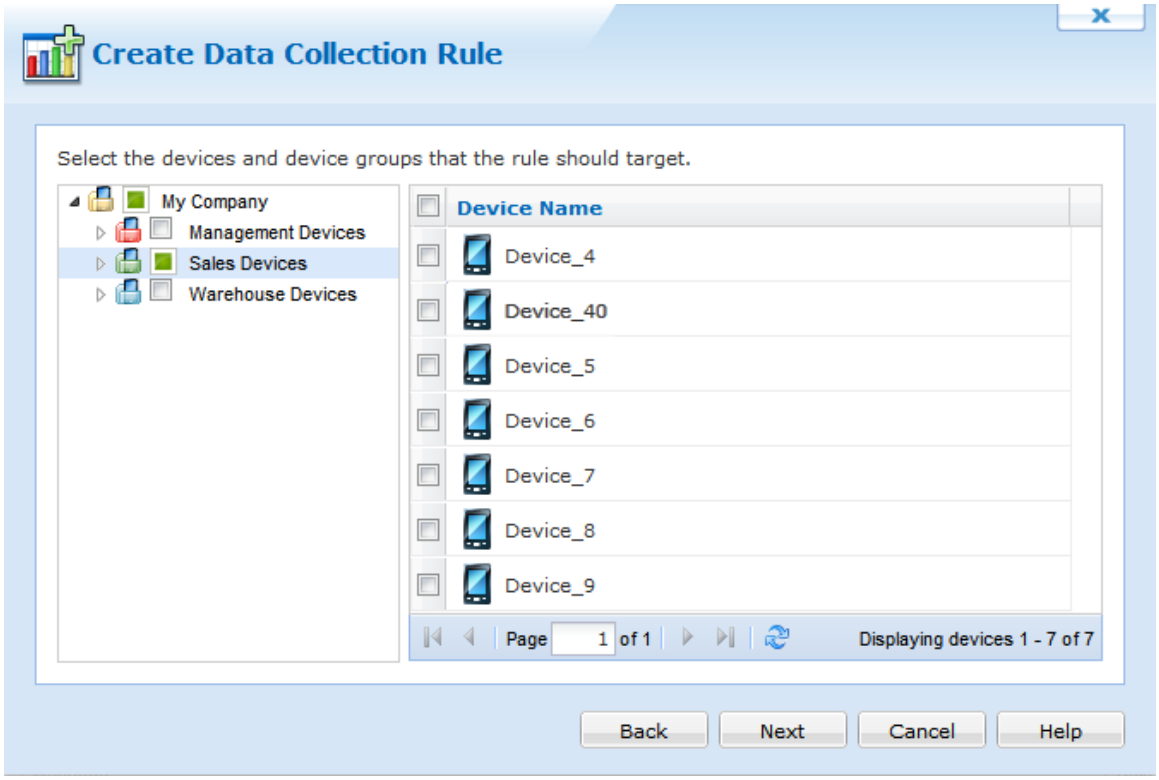
item and then click the direction arrow(s) to place the item(s) back into the **Available Items** list.

Item Name	Description
Available Memory	Shows the collected data is the combination of device memory, storage memory and virtual memory on the device
Available Storage	Shows the amount of room that is left on the main memory of the device
Battery Status	Shows what percent the battery was at the time the data collection rule ran
Call Log	Shows the incoming, outgoing and missed calls with call duration
Cellular Carrier	Shows what carrier the device is connected to at the time the data collection rule ran
Cellular Signal Strength	Shows what the signal strength is of the device at the time the data collection rule ran
IP Address	Shows the IP address of the device at the time the data collection rule ran
Location	Shows the GPS latitude, longitude, speed and heading
SSID	Shows the SSID that your device is currently connected to
Wi-Fi Signal Strength	Shows the signal strength of a wireless connection. A value of 0 is collected when there is no Signal listed in Manager

After selecting the choice(s), click the **Next** button.

3. Select devices.

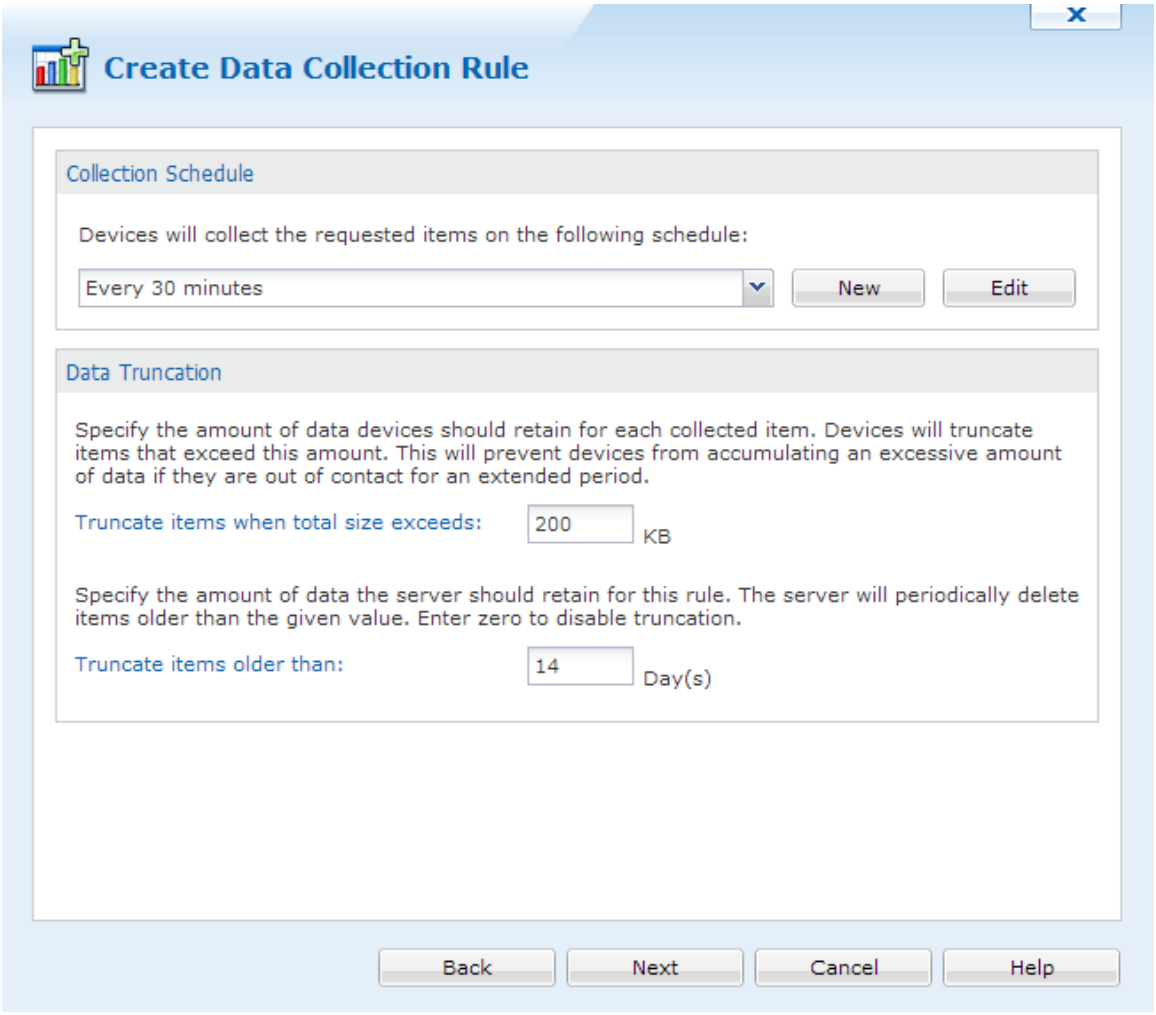
   Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.

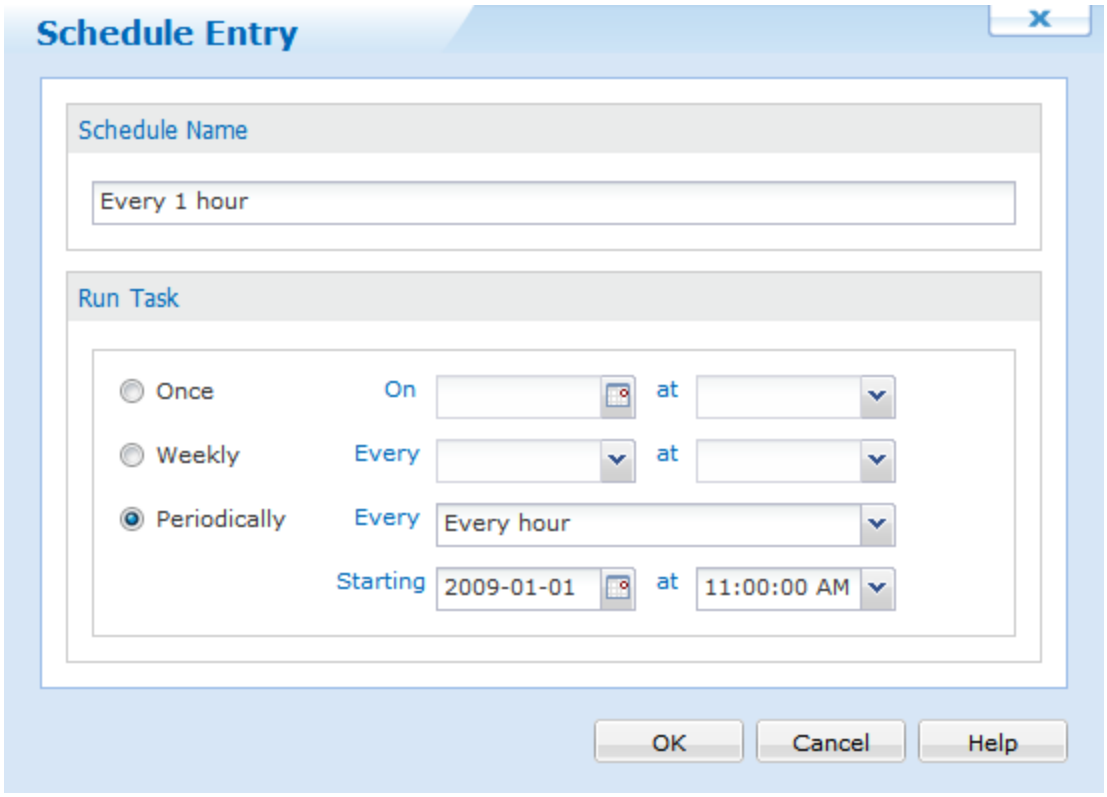


4. Configure data collection rule schedule and optional settings.

   Select the time interval the devices will collect the data and choose the size of the data being collected. This helps control memory used on the device and the number of days you would like to retain the data in the database.

   To set up a new schedule, click New.




Schedule Entry
Schedule Name
Every 1 hour
Run Task
Once
On
at
Weekly
Every
at
Periodically
Every
Every hour
Starting
2009-01-01
at
11:00:00 AM
OK
Cancel
Help

Section Name	Description
Collection Schedule	This option enables you to create a custom data collection schedule with a custom date and time. Select the **New** button to create the new schedule. This will open up the second dialog box above. If you already have a previously created schedule, you can select edit to open the second dialog box above.
Schedule Name	Enter a meaningful schedule name that will be used to identify your custom schedule(s).
Run Task	Select the frequency for which you want to initiate the data collection on your device(s).
Delivery Schedule	This option will deliver the data collected from the device to the Deployment Serverbased upon the set update schedule. Currently, this option uses device schedule as the delivery schedule and is not configurable.

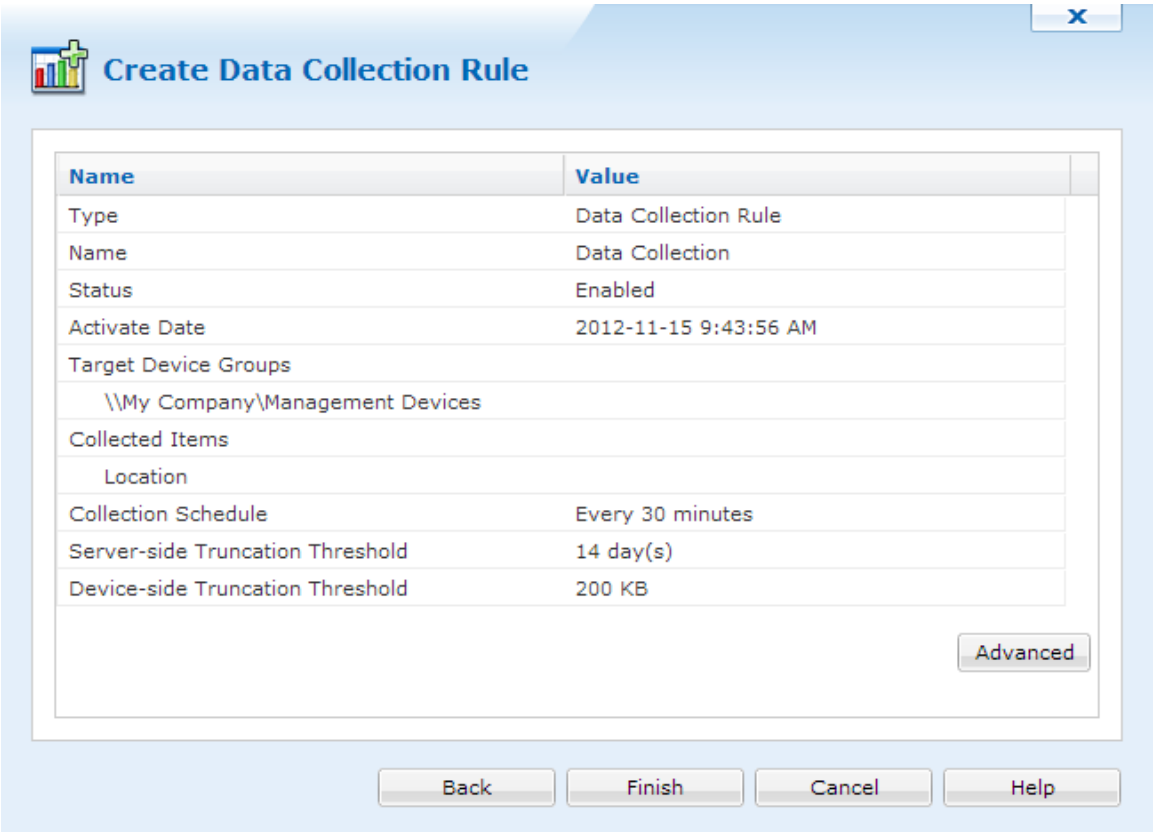
Section Name	Description
Device-Side Data Truncation	Specify the maximum size of data to be stored from the data collection ruleon the device(s).
Database Data Truncation	Specify the number of day(s) that you would like to retain the information in your database. Data collected older than the number of days listed will be deleted from the database

NOTE:

Creating a frequent collection schedule may affect the device's battery life. Also, frequent data collection can be managed with the truncation options available. This will help control how much data is kept on the device and in the database.

After entering your choice(s) in the above dialog box, click the **Next** button.

5. Review the summarized information.



The data collection rule can be deployed real-time or at a pre-set time. The data collection rule, although set to be activated at a scheduled time, can also be set to be deactivated. The deactivation setting is optional.

Click **Finish** to complete the wizard.

Windows Desktop Alert Rules

Alert Rules allow Administrators to be notified when events of interest arise on the system. This notification system allows Administrators to quickly and effortlessly communicate an event message to large groups of people via email, and notifies users via the MobiControl Manager Alert popup window. For every type of scenario, whether it is a Rule Change or a Device Error, the system will rapidly deliver your message to a designated audience.

To create an Alert Rule, select the Rules view (tab) within MobiControl Manager, then click the **Rule** menu, select **Create Rule**, and click **Alert Rule**. The Create Alert Rule Wizard will be displayed.

NOTE:

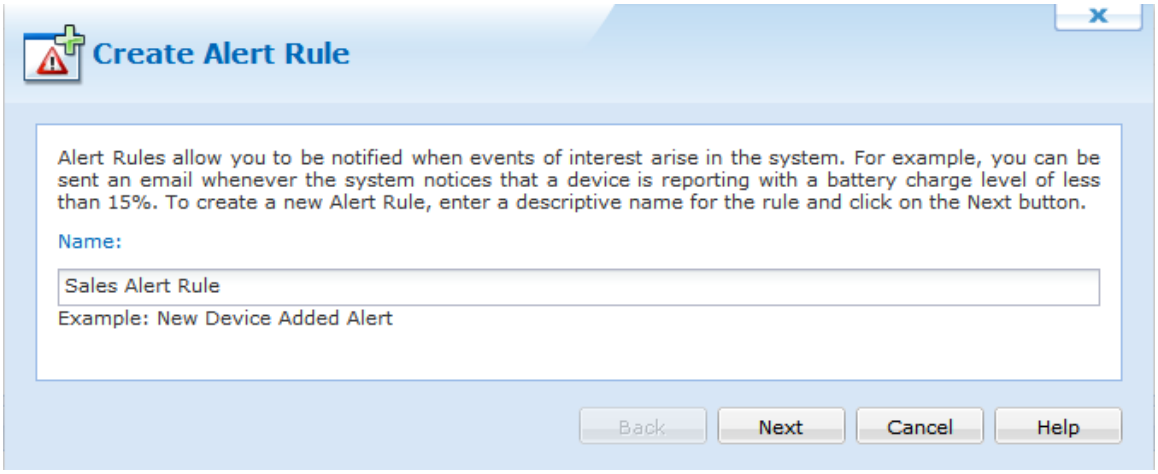
The Deployment Server must be online in order for Alerts to be generated and sent out.

The steps below describe how the Create Alert Rule Wizard can be used to create an add devices rule:

1. Start the wizard

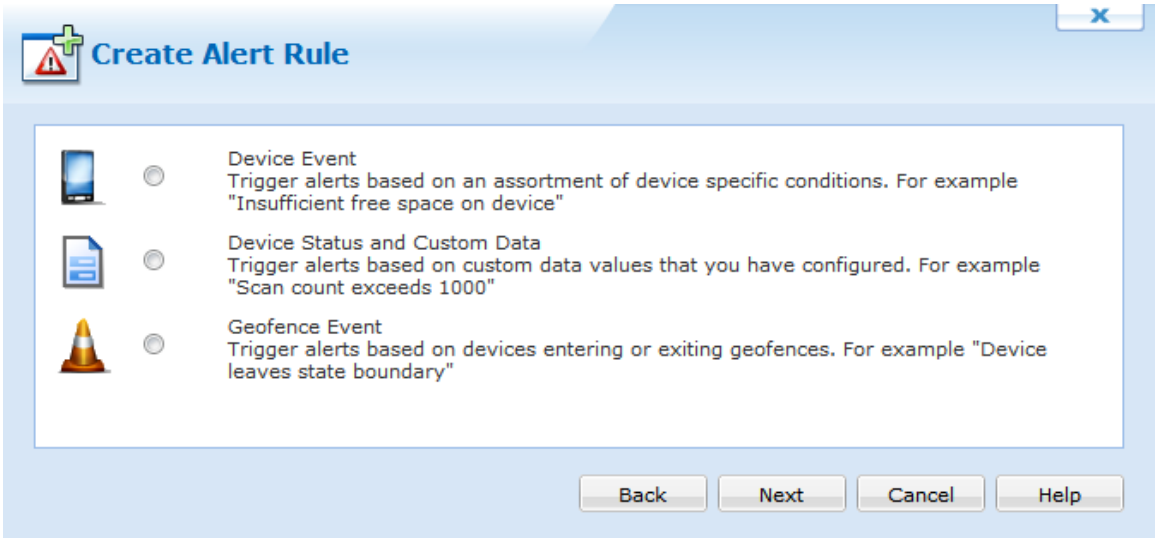
   Select the Rules view (tab), then click the **Rule** menu, select **Create Rule**, and click **Alert Rule**. The first page of the Create Alert Rule Wizard will be displayed.

   Enter a descriptive name for the Alert Rule you are creating and click **Next.**



First page of the Alert Rule Wizard

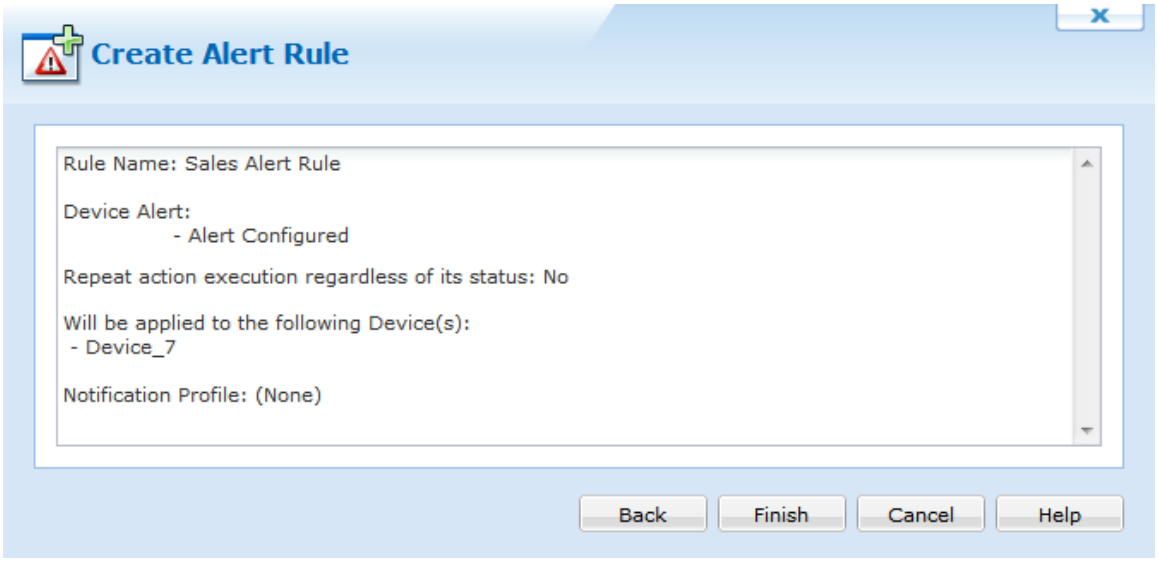
2. Select the Alert Rule Type.



Select the Alert Rule Type and click Next.

Type	Description
Device Event	Trigger alerts based on an assortment of device specific conditions.
Device Status and Custom Data	Trigger alerts based on Custom Data vales that you have configured.
Geofence Event	Trigger alerts based on devices entering or exiting geofenced areas.

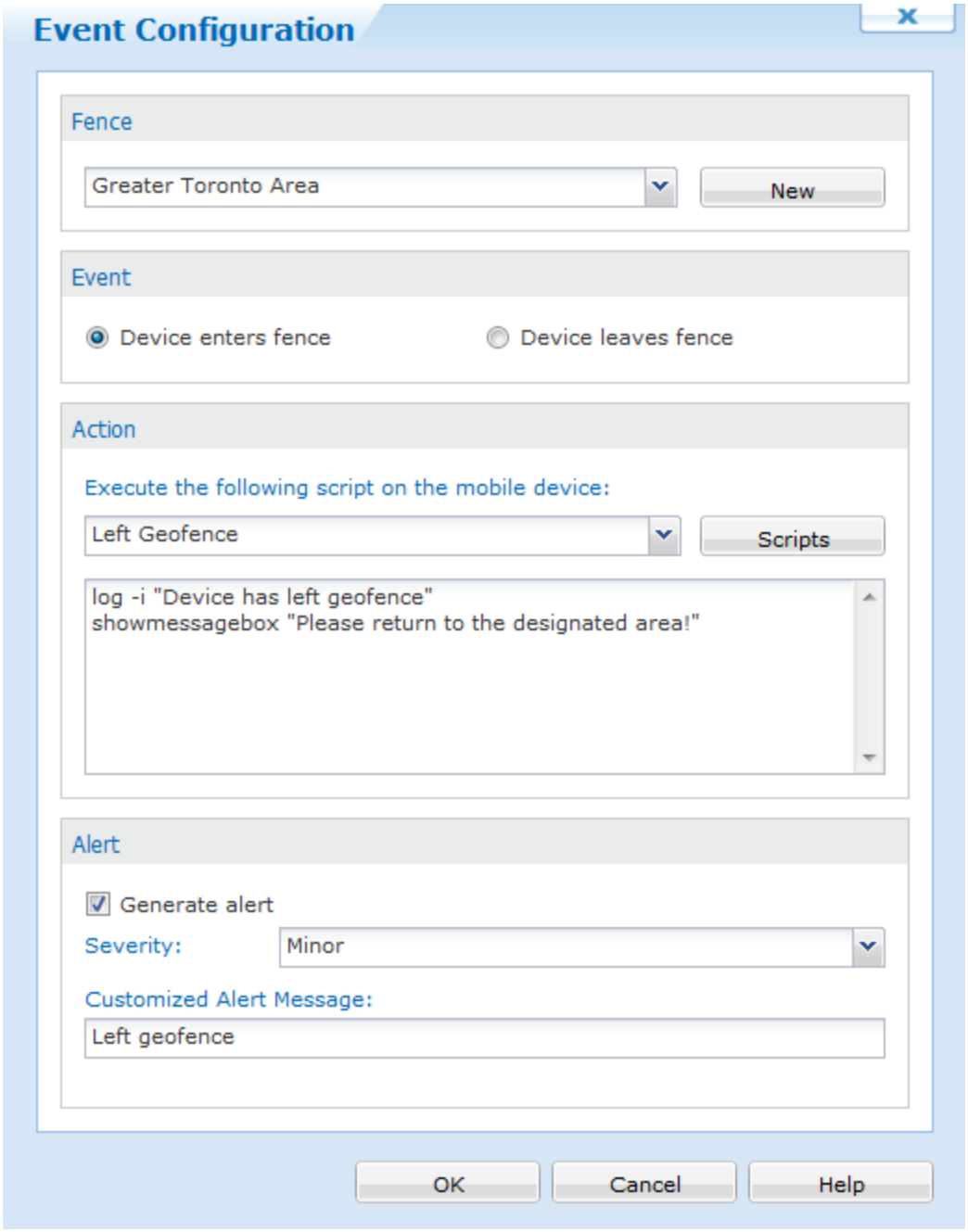
3. Review the summarized information.



Click **Finish** to complete the wizard.

Geofence Event

A Geofence Event is an alert trigger based on a GPS enabled device entering or leaving a Geofenced area defined by you. In order to create a Geofence event, you need to create an Alert Rule with a Type of Geofence Event.



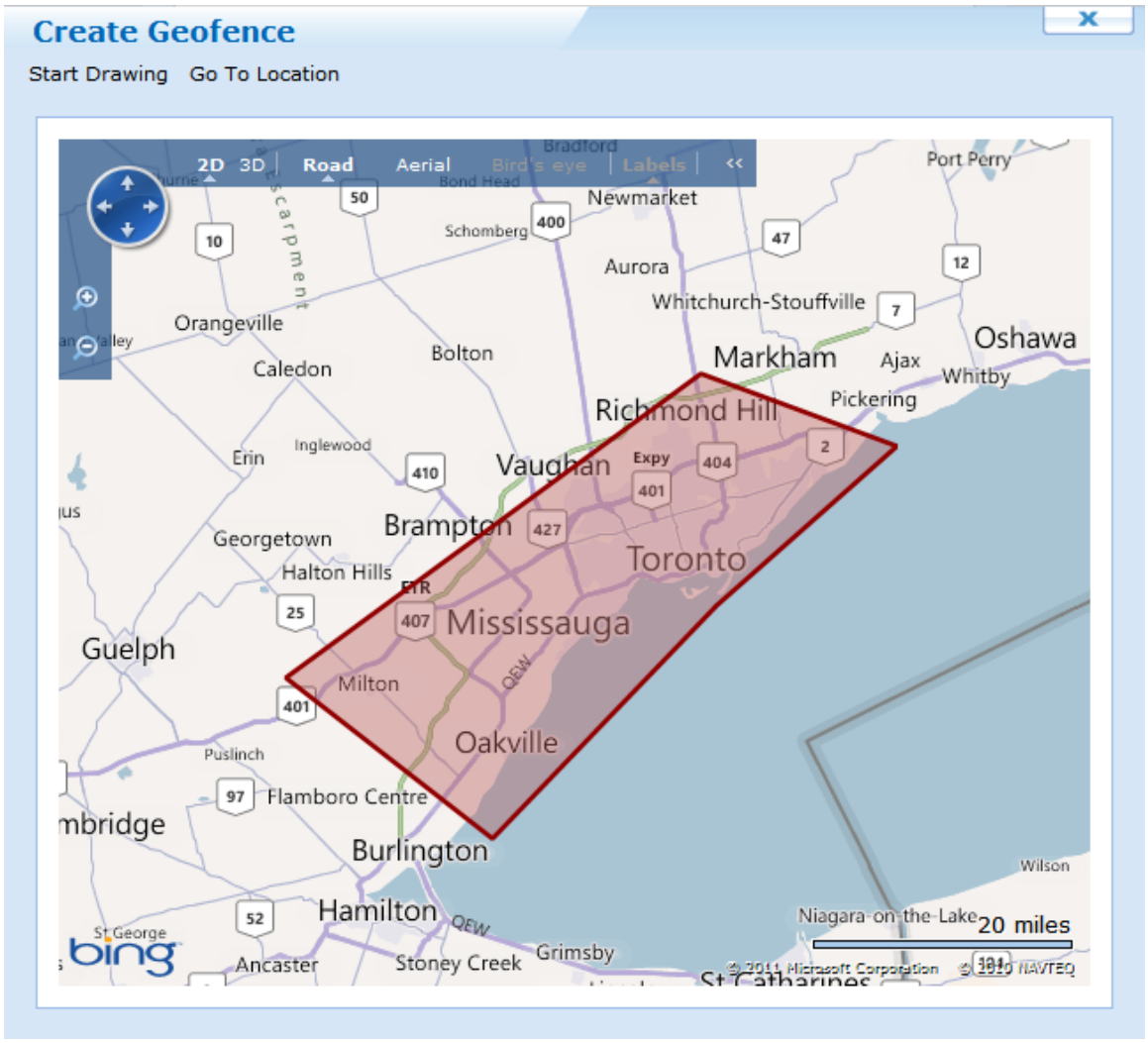
The **Fence** section allows you to create a geofence by clicking on the New button in the dialog box.

The **Event** section allows you to configure whether this event should be triggered on entry or exit of a fence.

The **Action** section allows you to configure what script you want to run on the mobile device when the event is triggered. This is optional, but you have for example the ability to run an Activate Connection, Log Event, Show Message or even wipe the device completely.

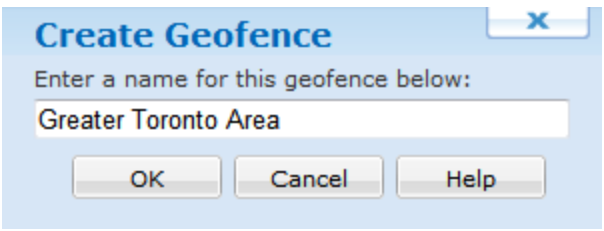
The **Alert** section allows you the option to Generate an alert, configuring its Severity (Minor, Serious and Critical) and add a Customized Alert Message, such as "Entered geofence".

When you click on the **New** button in the **Fence** section, the following Geofence Creation dialog box appears:



The two options available are to Start Drawing and Go to Location.

The **Start Drawing** option allows you to begin drawing on the map below the button. The area drawn on the map will be defined as the Geofence. The defined area must be a complete geometric shape, which means the Start Drawing point will be the same as the End Drawing point. When you have completed a proper geometric shape you be asked to name your geofenced area.



Prior to selecting the Start Drawing button, you have the ability to use the view control buttons in the map in order to move to a desired location, zoom in and out, switch to 3D, Road, Aerial and Bird's eye views among the many options. This allows you ease to create an appropriate view for your geofence.

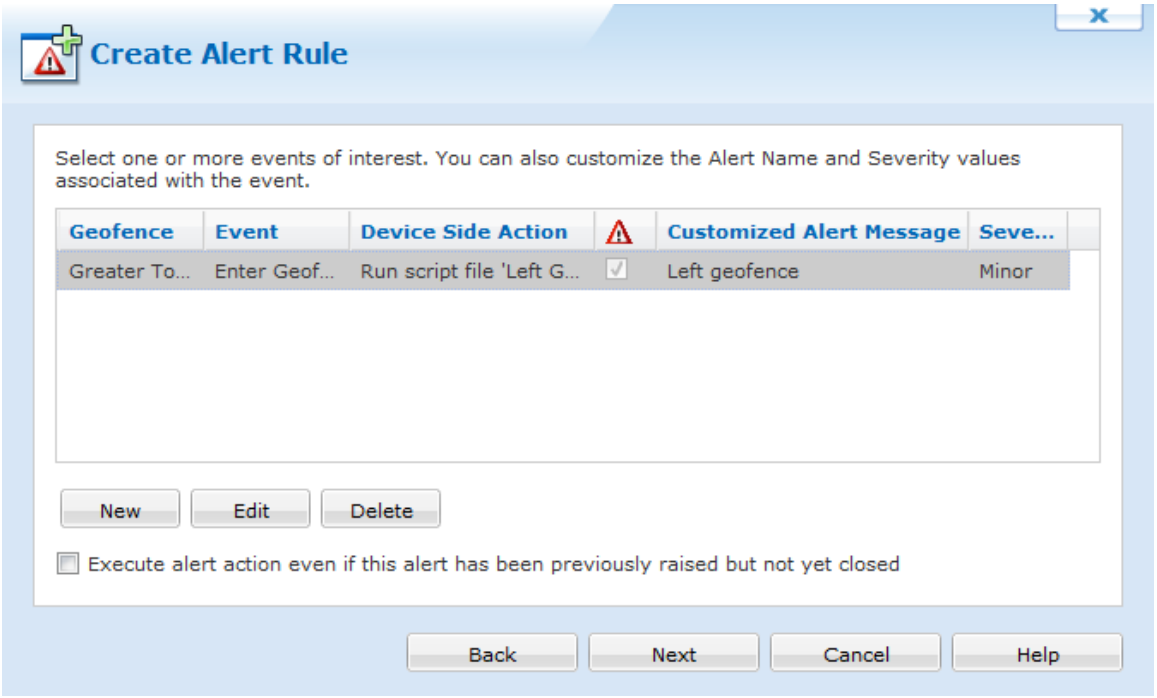
Alternatively to identify the appropriate view of the map, you can click on **Go to Location** which will allow you to specify a street address, location, landmark, or an existing geofence.

EXAMPLE:

- 350 Fifth Avenue, New York City
- Rome
- SFO (San Francisco International Airport)

Once you have the appropriate view displayed, you can click on Start Drawing and you are now able to create a fence. The first click of the mouse is first point of the fence. In order to complete the fence, you must have at least 3 distinct points selected on the map. In order to complete your fence, the last point must end off at the first point so it completes the closure of the fence. Once the last point is selected, a pop-up requesting the name of the geofence is shown. Here you should enter a meaningful name for that specific geofence in case you would like to use it again.

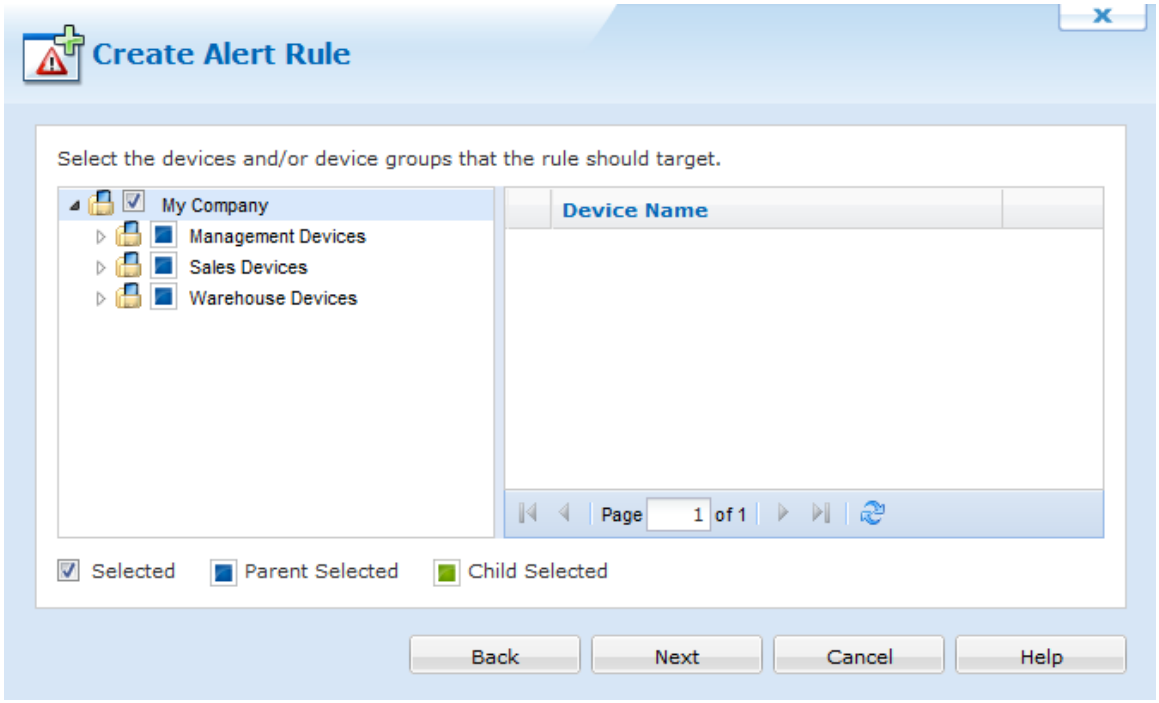
Select Geofence



Once the event is configured it will display as shown in the above diagram. Here you have the ability to create new events, edit existing events or delete events. Also, on this dialog box, there is a checkbox at the bottom allowing you to determine whether or not you want to Execute alert action even if this alert has been previously raised but not yet closed.

Select Devices

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



Select Power Policy

Clicking Next moves you to the Power Policy section as seen below.

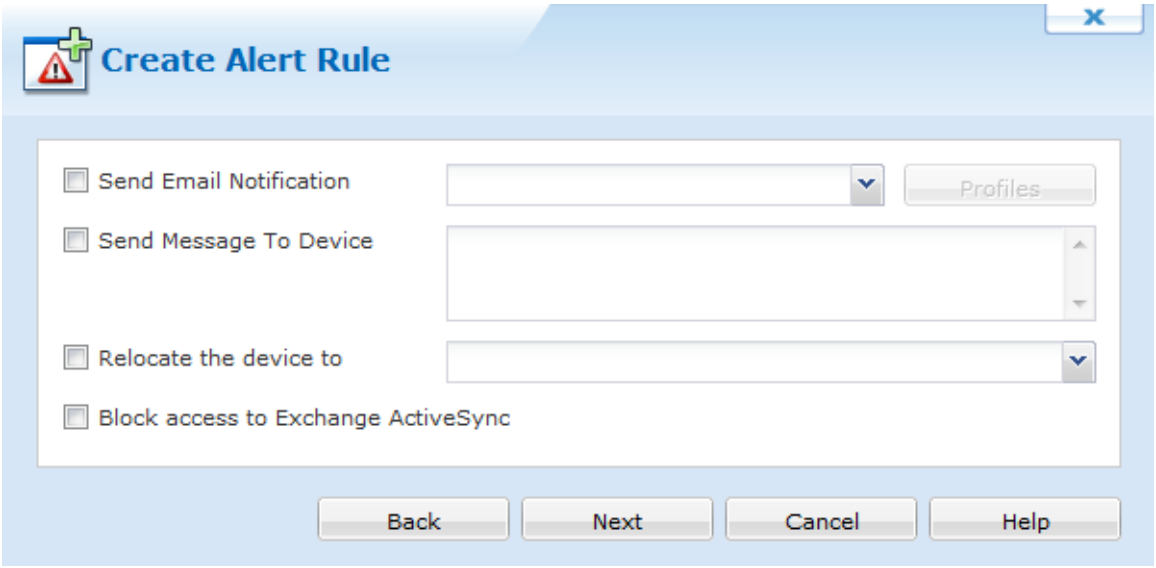
The options available for the Power Policy are Continuous and Periodic.

Continuous indicates the GPS radio is always on and the location will be monitored in real time. It is best to use this option with devices that have an external power source or are vehicle mounted because this option takes up a lot more power.

Periodic will turn on the radio based on a schedule that you define. Based on your business requirements, this can be as responsive as every 2 minutes, or every weekday all the way up to every year. It is best to use this option when you have battery powered devices in order to minimize the amount of power consumed with having this feature on.

Notification Profile Settings

Once the Alert Rule is selected, you must select your Notification Profile.

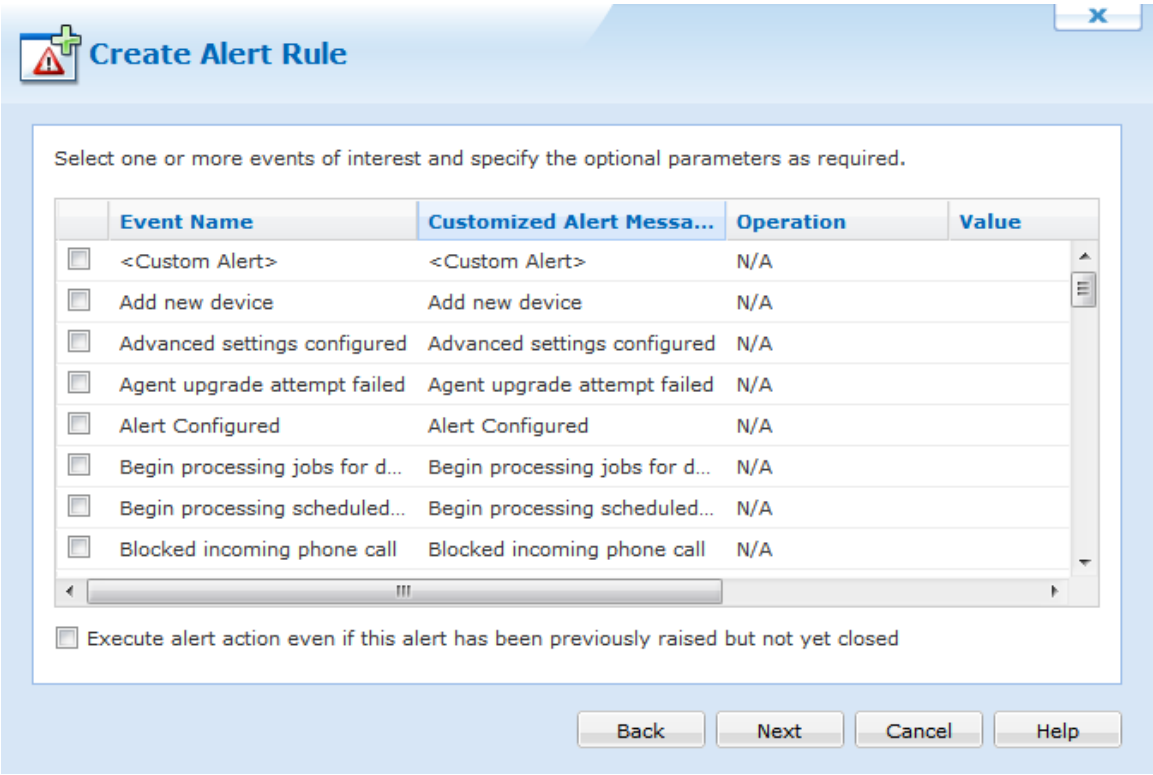


Select an existing notification profile, or click New to create a new Notification Profile. For assistance with notification profiles click here. Once you have selected your notification profile click Next.

Click Next and continue the Alert Rule Wizard here.

Device Event

A Device Event is an alert triggered based on an assortment of device specific conditions. See below for a full list.



Device Event Notification Selection Window

Severity is set to Minor by default and can be altered.

The below table shows all available default Device events:

Log Event	**Alert Message (Customisable)**
<Custom Alert>	<Custom Alert>
Add new device	Add new device
Advanced settings configured	Advanced settings configured
Agent upgrade Attempt failed	Agent upgrade attempt failed
Alert Configured	Alert Configured
Begin processing jobs for device	Begin processing jobs for device
Begin processing scheduled jobs	Begin processing scheduled jobs
Blocked incoming phone call	Blocked outgoing phone call
Change password failure	Change password failure
Change password success	Change password success
Custom Data configured	Custom Data configured
Custom log	Custom log

Log Event	Alert Message (Customisable)
Data Collected	Data Collected
Data Collection configured	Data Collection configured
Dependent packages not installed	Dependent packages not installed
Device connected	Device connected
Device disabled	Device disabled
Device disconnected	Device disconnected
Device Enabled	Device Enabled
Device has not been connected for %VALUE% minutes	Device has not been connected for %VALUE% minutes
Device Manually relocated	Device Manually relocated
Device relocated	Device relocated
Device security configured	Device security configured
Error creating file on device	Error creating file on device
Error message received from device	Error message received from device
Error receiving file	Error receiving file
Error sending file	Error sending file
Error sending message	Error sending message
Error writing to file on device	Error writing to file on device
Exchange ActiveSync configured	Exchange ActiveSync configured
File synchronization failed	File synchronization failed
File synchronization was aborted by pre-sync script	File synchronization was aborted by pre-sync script
File(s) synchronized	File(s) synchronized
File synchronization was aborted by pre-sync script	File synchronization was aborted by pre-sync script
File synchronization failed	File synchronization failed
Geofencing Configured	Geofencing Configured
Inaccurate device date-time detected	Inaccurate device date-time detected
Incompatible platform, processor or OS version	Incompatible platform, processor or OS version
Installation aborted by user	Installation aborted by user
Installation was aborted by install script	Installation was aborted by install script
Insufficient free space on device	Insufficient free space on device
Invalid device software version	Invalid device software version

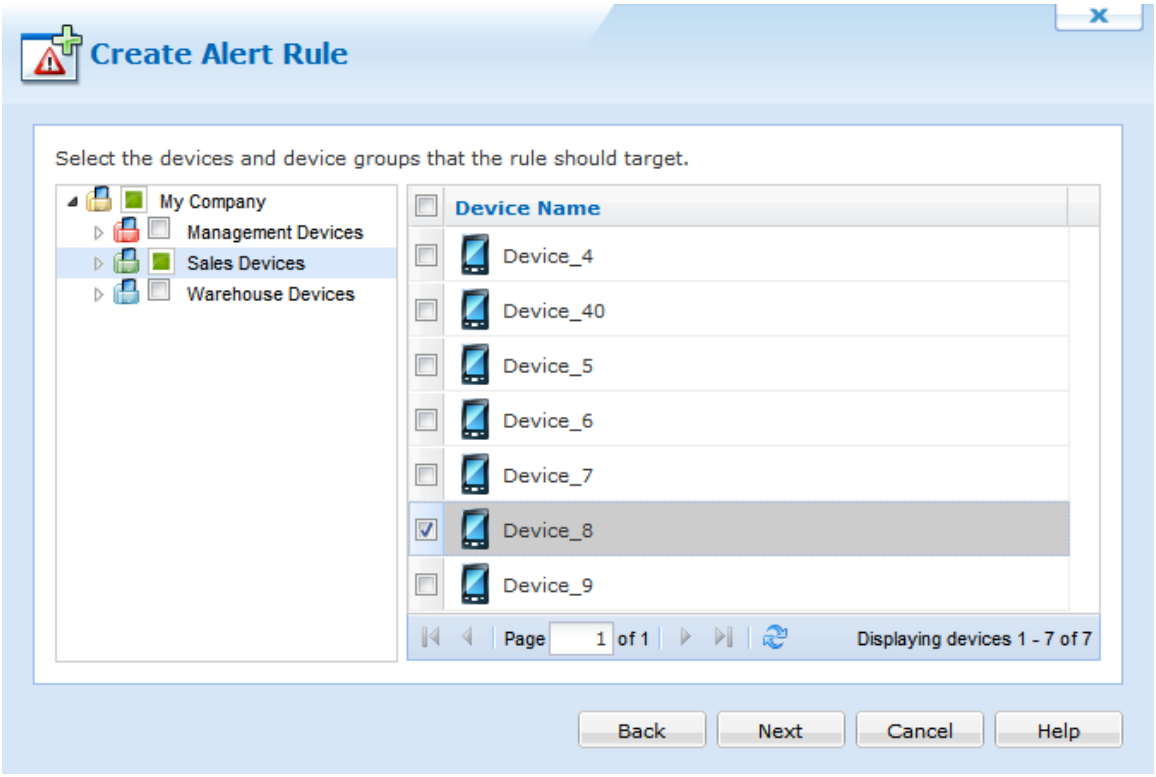
Log Event	Alert Message (Customisable)
Invalid message received from device	Invalid message received from device
Lockdown removed	Lockdown removed
Logon failure	Logon failure
Logon success	Logon success
Multiple packages with the same name in job list	Multiple packages with the same name in job list
No Package ID in installation report	No Package ID in installation report
Package file is corrupted	Package file is corrupted
Package file not found	Package file not found
Package uninstalled	Package uninstalled
Package with higher version number already installed on the device	Package with higher version number already installed on the device
Pending jobs cannot be processed until device user is authenticated	Pending jobs cannot be processed until device user is authenticated
Process Learned	Process Learned
Processed successfully	Processed successfully
Remote Control	Remote Control
Stopped illegal process	Stopped illegal process
Time Sync Configured	Time Sync Configured

The following list of variables are only available within the Customized Alert Message field:

Type	Description
%RULENAME%	The name of the rule
%PACKAGENAME%	The name of the package

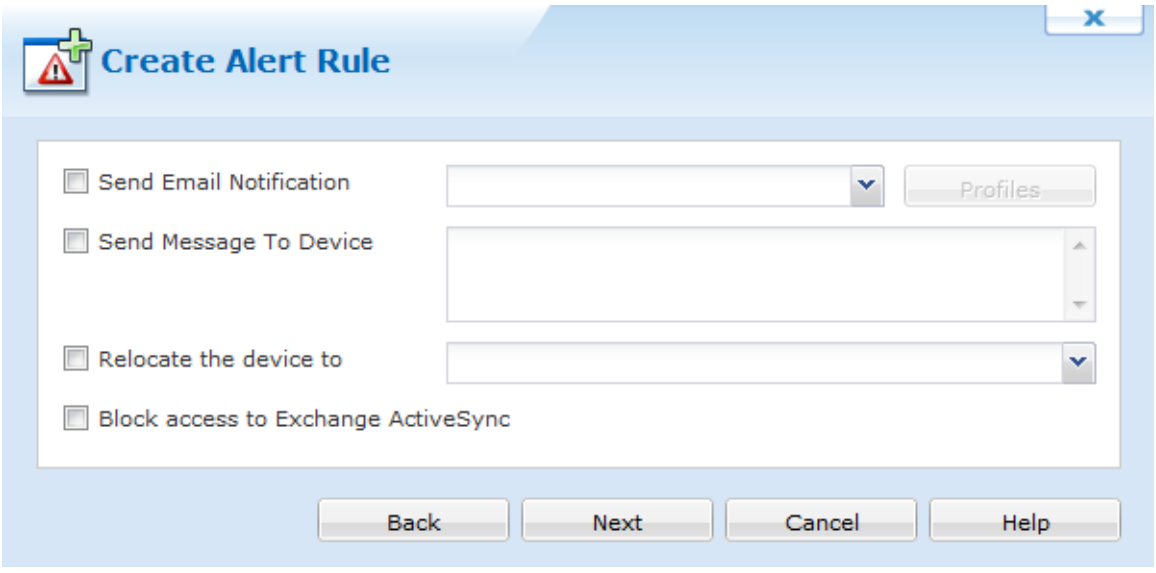
Select devices.

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



Notification Profile Settings

Once the Alert Rule is selected, you must select your Notification Profile.

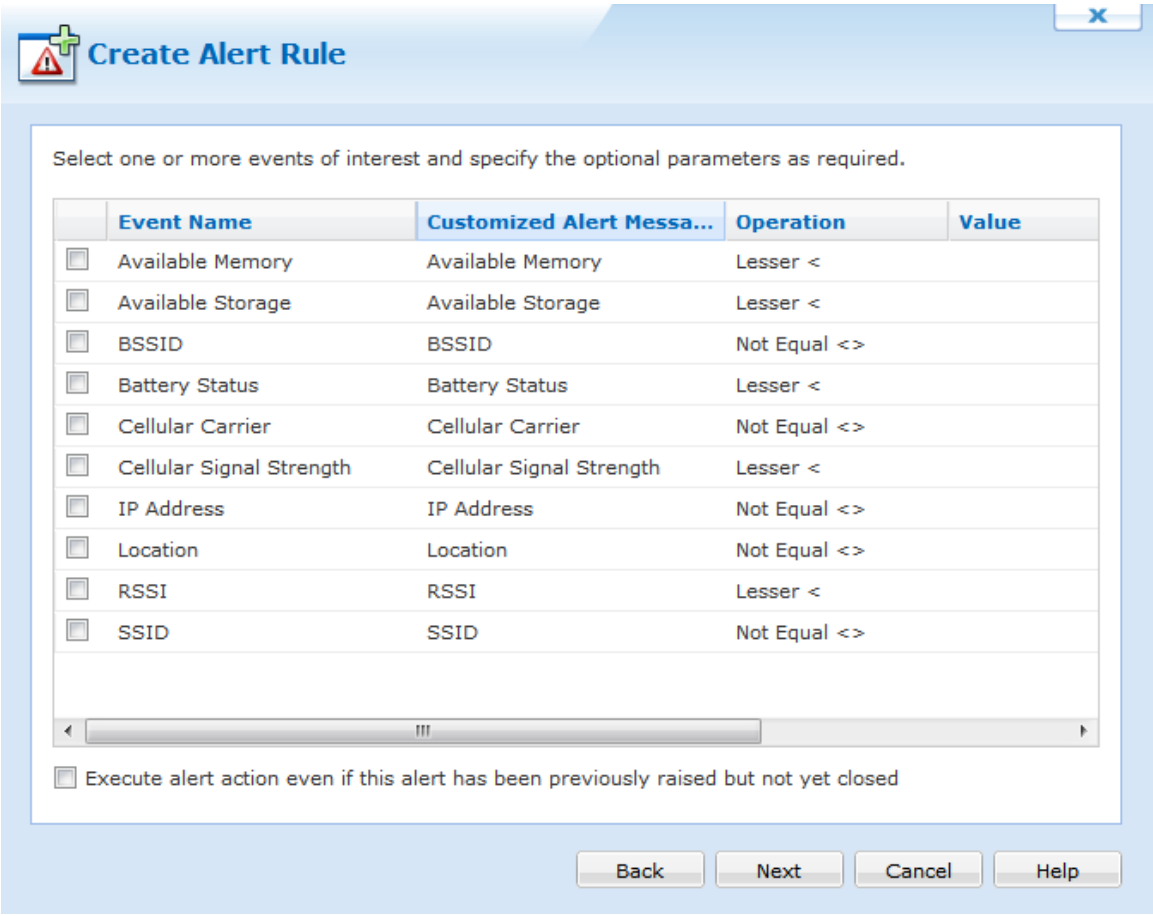


Select an existing notification profile, or click New to create a new Notification Profile. For assistance with notification profiles click here. Once you have selected your notification profile click Next.

Click Next and continue the Alert Rule Wizard here.

Device Status and Custom Data Event

A Device Status and Custom Data Event is an alert triggered based on an assortment of data values that you have set. See below for a full list.



Device Status and Custom Data Event Notification Selection Window

The Operation and Value fields allows to filter out Alerts based on specific values or value ranges. The Operation field specifies at which point an alert will be created for the data value you have specified. Severity is set to Minor by default and can be altered.

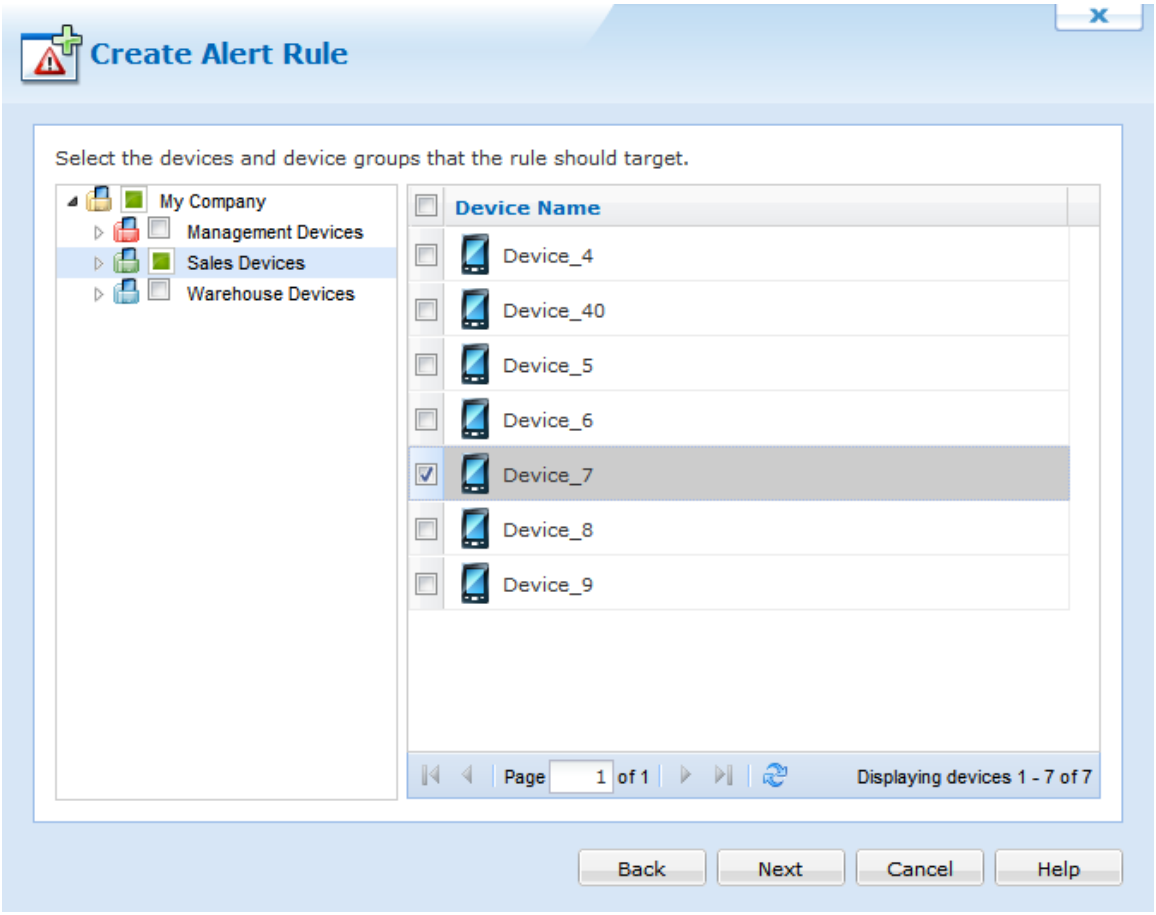
The below table shows all available default Device Status and Custom Data Event events:

Log Event	Alert Message Alert Message (Customisable)
Battery Status	Battery Status
Available Memory	Available Memory
Available Storage	Available Storage
SSID	SSID
Wi-Fi Signal Strength	Wi-Fi Signal Strength

Log Event	Alert Message Alert Message (Customisable)
IP Address	IP Address
Cellular Carrier	Cellular Carrier
Cellular Signal Strength	Cellular Signal Strength

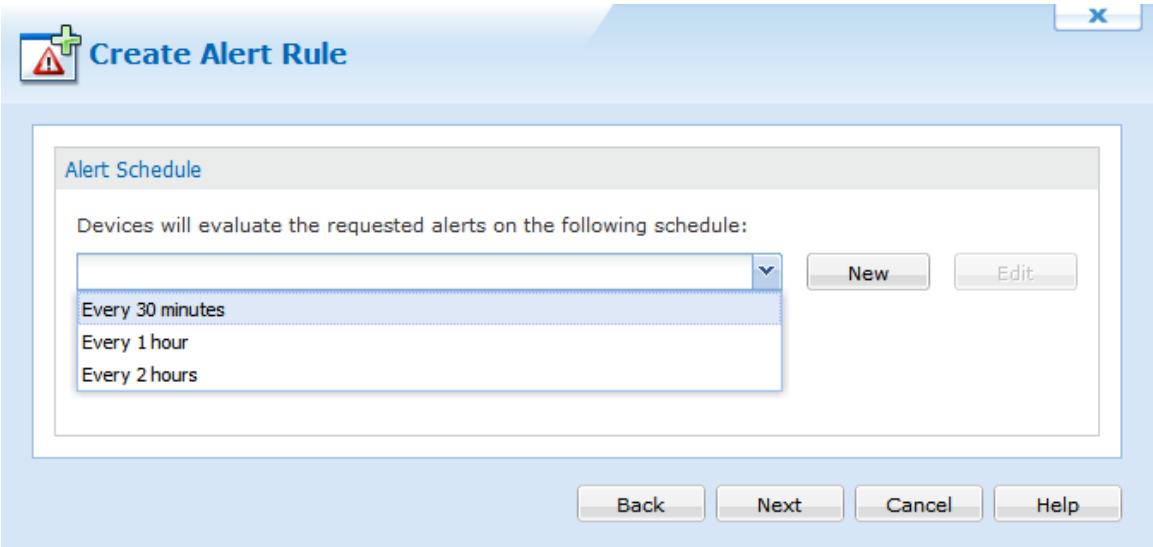
Select devices.

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



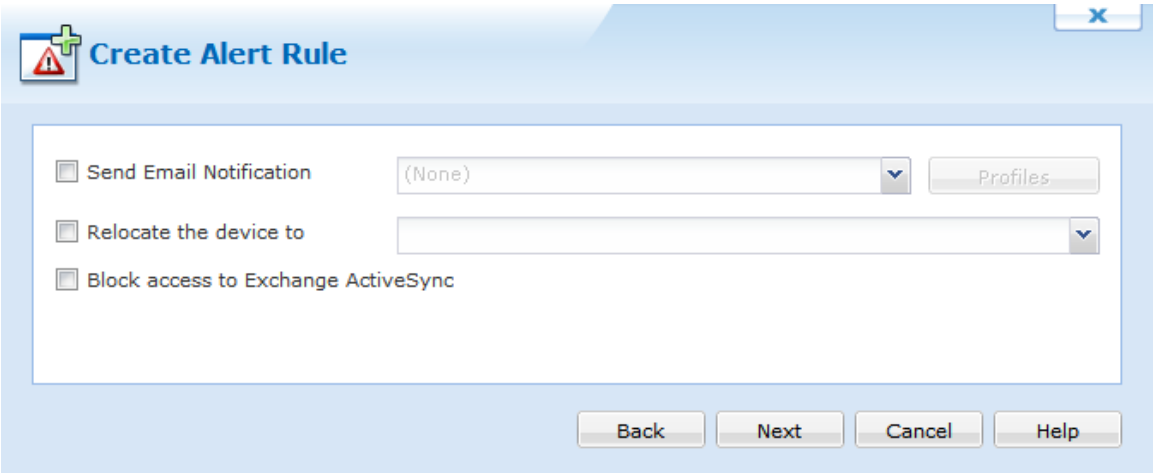
Select Schedule.

Select how frequently the devices should be checked for the requested Alert information. Once you have completed this section, click the **Next** button.



Select Actions.

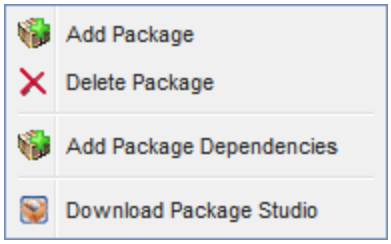
Select an existing notification profile, or click Profile to create a new Notification Profile. For assistance with notification profiles Click Here. Once you have selected your Notification Profile you can select a Device Side Action. This action is a script that will be launched on the device when certain criteria is met. For assistance with the Script Manager Click Here.



After selecting your Profile and Actions, click Next and continue the Alert Rule Wizard here.

Packages Tab

The Packages view (tab) provides a list of the packages that have been imported into the MobiControl system, and the status of their distribution to the devices in the deployment. From this tab you can:



- Upload a Package
- Delete a Package
- Download Package Studio
- Create a Package Dependency

The left panel lists all of the packages that have been imported into the MobiControl system. Package are created using MobiControl Package Studio. Please see the "MobiControl Package Studio" topic on page 413 for more information.

If multiple versions of a package have been imported, each is listed with its own unique version number. The version number is set when creating or editing a package using MobiControl Package Studio.

Adding or Deleting a Package

To add a package to MobiControl, click **Package,** and then click **Add Package.**

To delete a package from MobiControl, select the version number node for the package, click **Package,** and then click **Delete.**

Download Package Studio

Package Studio must be downloaded in order to create packages. The Package Studio is typically installed with the thick client, but if you are using Web only then you can download Package Studio to work with on your desktop.

Package Dependencies

Package dependencies are a way to ensure the correct sequence of installation of packages on a device. To establish a package dependency, click **Package,** and then click **Add Package Dependencies.**

Panels in the Packages Tab

Info Panel

The Info panel provides detailed information about the package that is currently selected in the listing panel. Information includes the meta-data associated with the package that was specified when it was created, for example, processor, platform or OS version, and vendor information. Please see the "Create Package Project" topic on page 415 for a detailed explanation of these fields.

The content displayed in this panel is stored in the MobiControl database. You can select **Refresh** or press F5 on this tab to retrieve updated information from the database.

Devices Panel

The Devices panel lists the devices that have the selected package installed, or marked as pending for installation/uninstallation.

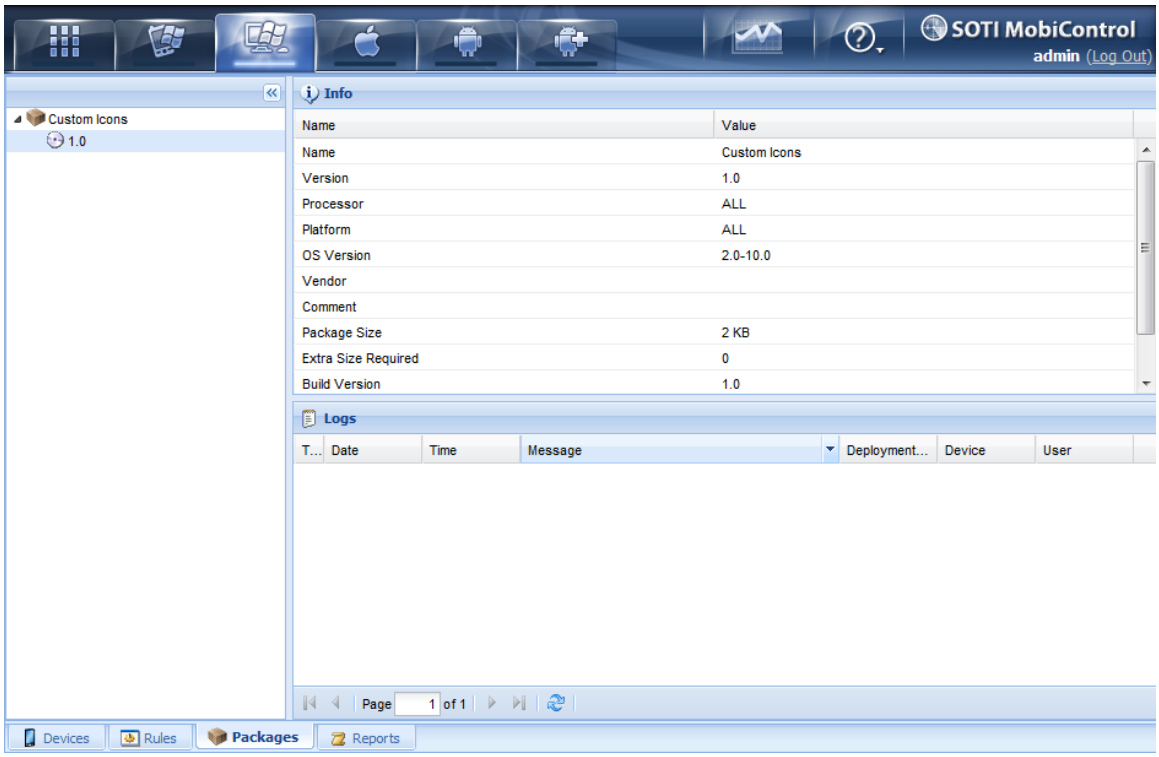
Rules Panel

The Rules panel lists the deployment rules that are configured to deploy the selected package.

Logs Panel

The Logs panel lists events occurring in the MobiControl system. This listing is filtered based on the package that is selected in the package listing.

You have the option to enable or disable logging, as well as adjust the maximum number of logs displayed and frequency with which the Manager should refresh the log panel.



MobiControlPackages Tab Packages view (tab)

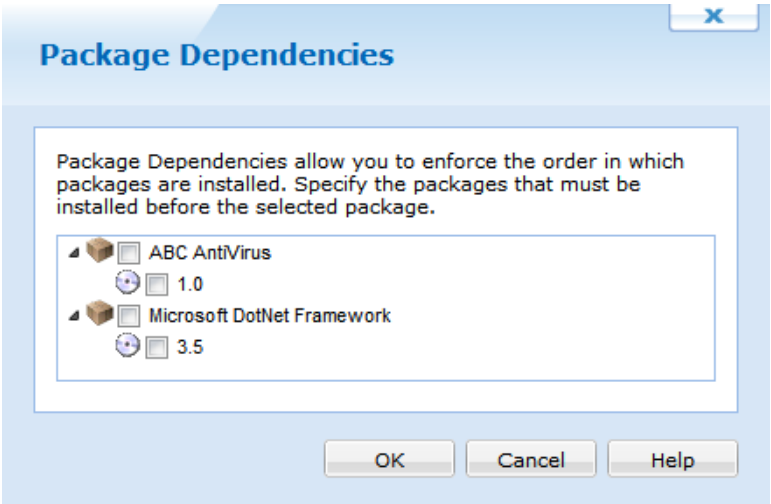
Package Dependencies

Package dependencies provide a mechanism to enforce the order in which packages are installed on a device.

To display the **Package Dependencies** dialog box, right-click on the package and select **Add Package Dependencies** from the pop-up menu. The **Package Dependencies** dialog box lists the configured dependencies.

Adding Package Dependencies

To add a package dependency, select the package(s) and version(s) upon which the target package is dependent.



Package Dependencies dialog box

EXAMPLE:

Packages A and B need to be installed, but it is mandatory that A is installed before B. Configure a dependency for package B: when editing the package dependencies for package B, select package A.

NOTE:

If a package depends on another package that is scheduled to install at a later time, then the Deployment Server will not push the package unless it is also scheduled to install at the same time or later. Please see the "Windows Desktop Package Deployment" topic on page 897 for more information about installation schedules.

Reports Tab

MobiControl includes an advanced reporting engine—Crystal Reports—that gives detailed information about all aspects of system operation. The product includes a set of canned reports that provide information about key areas of system operation. Reports can also be customized as well as new reports can be created and added to the system as needed.

MobiControl Web Console Reports view (tab)

Report Types

The following reports are included with MobiControl:

- A **deployment server activity report** is a detailed report for deployment server activity over a specified time period.
- A **deployment rule report** is a detailed report of deployment rules and all devices.
- A **Battery and Storage Report** is a detailed report of the battery and storage of the selected devices.
- A **Cellular Signal Strength Data Report** is a detailed report of the cellular signal strength of the selected devices.
- A **deployment rule summary report** is about deployment rule exceptions, showing how many devices have executed the rule successfully, are pending, or have encountered an error.
- A **Deployment Server activity report** is a detailed report of Deployment Server activity over a specified time period.
- A **device activity report** provides information about the device activity during a specific time period.
- A **device custom data report** provides information about devices with the custom data values of selected custom data fields.
- A **device note report** provides information about the notes for your devices.
- A **device package report** provides information about packages installed on your device.
- A **device program report** provides information about all the programs installed on your devices.
- A **device relocation rule report** provides information about all the relocation rules for your devices.
- An **out of contact devices report** provides information about devices that have not connected to the system since the specified date.
- A **package deployment report** provides information about package deployment.
- A **Location Collected Data Report** is a detailed report of the location data collected for the devices.
- A **Connectivity Information Report** is a detailed report regarding device's connectivity.
- A **Device Tree Report** provides information about the device tree structure.
- A **Device Tree with Virtual Groups Report** provides information about the device tree structure along with the virtual groups.
- A **Log Information Report** provides information about the device logs.
- A **Phone Number Report** provides information about the phone number of devices.
- A **Alert Summary Report** provides summary of the alerts.
- A **deployment rule report** is a detailed report of deployment rules and all devices.
- A **Geofence Report** provides detailed report based on the Geofence.
- A **Uninstalled Mandatory Applications Report** provides information about the mandatory application not installed on the devices.

Generating a Report

1. In MobiControl Manager, select the Reports view (tab).
2. Select a report in the left pane of the Reports view (tab).
3. Click the **Generate Report** button.
4. For some reports, a window will appear requesting additional parameters (e.g. time period) that may be required.

MobiControl Web Report toolbar view

Saving a Report

1. Generate a report.
2. On the report screen, click the **Export Report** button. (It is the first icon in the toolbar, beside the **Print Report** button.)
3. Select the desired file type. Available file types are:
    - Adobe PDF (`.pdf`)
    - Crystal Reports (`.rpt`)
    - HTML 3.2/4.0 (`.html`)
    - MS Excel 97-2000 (`.xls`) or Data only (`.xls`)
    - MS Word editable RTF (`.rtf`)
    - ODBC
    - Record-style (columns of values with or without spaces) (`.rec`)
    - Report definition (`.txt`)
    - Rich text format (`.rtf`)
    - Comma-separated values (`.csv`)
    - Tab-separated text (`.ttx`)
    - Text (`.txt`)
    - XML (`.xml`).
4. Select the location to which you want to export the report. The options available are:
    - Application
    - Disk file
    - Exchange folder
    - Lotus Domino
    - Lotus Domino Mail
    - MAPI (Messaging Application Programming Interface)

Printing a Report

1. Generate a report.
2. On the report screen, click the **Print Report** button. (It is the second icon in the toolbar, beside the **Export Report** button.)
3. The print menu will pop up. Select the desired printer and the report will be printed there.

Generating Custom Reports

It is possible to create custom report files on any available statistic you desire. The Deployment Server database is a standard SQL database and can be queried by writing a custom query. Also, it is possible to create additional reports that are built into MobiControl. For more details, please contact us.

Other Tools

These other tools are available through the toolbar:

- The **Stop Loading** button stops the report generation process.
- **Refresh** regenerates the report. If parameters were required to generate the original report (e.g. time period), a window will appear requesting the additional parameters.
- The **Search Text** button searches the body of the report for a specified text string.
- The **View Zoom** field allows the user to select view magnification, page width, and whole page views.

MobiControl Tutorial

This is the last step of the MobiControl Tutorial. We hope you feel comfortable with MobiControl!

iOS Devices Tab

The **iOS** tab enables you to access the devices connected to the deployment running an Apple iOS operating system. All functions that can be performed on this OS are:

- Location Services
- Device Security
- Device Configuration
- Adding a Device
- Distributing software to a device
- Data collection functions
- Alerts

There are three views available for iOS within the MobiControl web console. The views can be selected using the tabs at the bottom of the MobiControl Web Console user interface.

- The **Devices view (tab)** allows users to view information about configured devices, for instance packages installed, device ID, and IP address. The Devices view (tab) also allows users to control and configure devices, for example, to remote control a device or to change a device's name. Please see the "iOS Advanced Settings" topic on page 1005 for more information.
- The **Rules view (tab)** allows users to view information about the configured rules. The Rules view (tab) also allows users to configure rules, for instance, create an add devices rule. Please see the "iOS Rules" topic on page 1031 for more information.
- The **Reports view (tab)** provides users with a set of reports containing detailed information about the operation of the system. Provided reports include: deployment rule execution summary report, device configuration rule execution summary report, and device activity report. Please see the "Report Types" topic on page 1110 for more information.

- The **Content Management (tab)** provides a way to upload files to the MobiControl server, and push those files to devices. With the Content Manager, we can also organize files and place categories on them. Users who have a device agent on their device are also able to download files on demand. Please see the "Secure Content Library Tab" topic on page 1456 for more information.

iOS Agent Install Methods

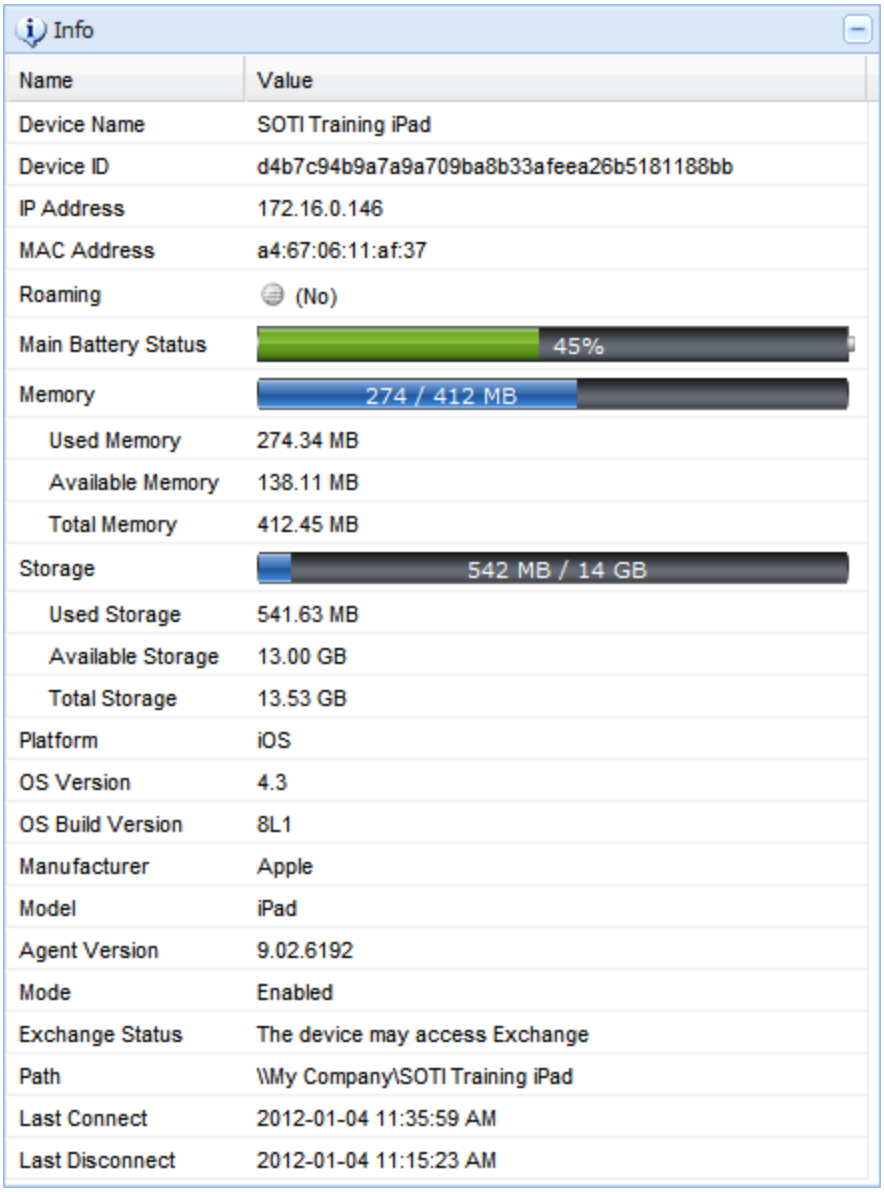
The MobiControl Device Agent is the MobiControl software that is installed onto mobile devices. The Device Agent communicates with MobiControl Deployment Server(s) and carries out the instructions it receives from servers. Device Agents also provide reporting and real-time information to Deployment Servers.

When looking to manage iOS devices, MobiControl has 2 ways to help. First method is Agentless, this method allows administrators to manage all aspects of the device. Second method includes a Device Agent from the App Store, this method allows administrators to have a little more control over the iOS device and gain more stats.

Agentless Installation

When the add devices rule has been created, it will provide you the option to "Publish to Enrollment Service", if you choose not to publish to the Enrollment Service then an "Enrollment URL" will be provided. Simply navigate to the Enrollment URL on the iOS Device(s) you wish to manage, and complete any steps listed. For more information please See "Adding iOS Devices" on page 1034 and See "Enrolling iOS devices" on page 1040

Once enrollment has been completed, you will now see the device on the iOS Devices Tab. Under the Device Info panel, the following information will be collected:



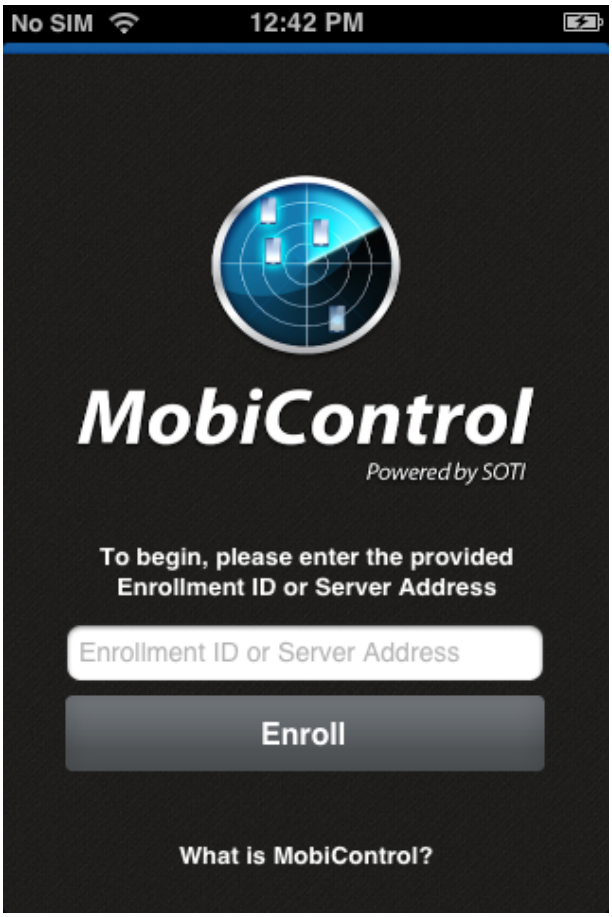
Device Information	Description
Device ID	Device ID
DeviceName	The name given to the device via iTunes.
OSVersion	The version of iOS the device is running.
BuildVersion	The iOS build number (8A260b, for example).
ModelName	Name of the device model, e.g. "iPod Touch".
Model	The device's model number (MC319LL, for example).
ProductName	The model code for the device (iPhone3,1, for example).
SerialNumber	The device's serial number.
DeviceCapacity	Amount of total space on the device

Device Information	Description
AvailableDeviceCapacity	Amount of space available
CellularTechnology	Returns the type of cellular technology (none, GSM, CDMA)
IMEI	IMEI
MEID	MEID
ModemFirmwareVersion	The baseband firmware version.
ICCID	The ICC identifier for the installed SIM card.
BluetoothMAC	Bluetooth MAC address.
WiFiMAC	Wi-Fi MAC address.
CurrentCarrierNetwork	Name of the current carrier network.
SIMCarrierNetwork	Name of the home carrier network. (Note: this query is supported on CDMA in spite of its name.)
CarrierSettingsVersion	Version of the currently-installed carrier settings file.
PhoneNumber	Raw phone number without punctuation, including country code.
DataRoamingEnabled	The current setting of the Data Roaming setting.
isRoaming	Returns whether the device is currently roaming.
SubscriberMCC	Home Mobile Country Code (numeric string).
SubscriberMNC	Home Mobile Network Code (numeric string).
CurrentMCC	Current Mobile Country Code (numeric string).
CurrentMNC	Current Mobile Network Code (numeric string).
HardwareEncryptionCaps	Bitfield. Describes the underlying hardware encryption capabilities of the device. Values are described in Table 8 (page 23).
PasscodePresent	Set to true if the device is protected by a passcode.
PasscodeIsCompliant	Set to true if the user's passcode is compliant with all requirements on the device, including Exchange and other accounts.
PasscodeIsCompliantWithProfiles	Set to true if the user's passcode is compliant with requirements from profiles.

Additional information is available when the Device Agent is installed, please see below for more information.

Device Agent Installation

The Device Agent is only available from the App Store by searching for MobiControl. Once the Device Agent is installed, it will require an Enrollment ID which is provided when creating an add devices rule. Once the device has completed all the Enrollment steps required, additional options will be available. For more information on the Enrollment process please See "Enrolling iOS devices" on page 1040



Device Menu

Device Information	Description
AvailableMemory	Available RAM
TotalMemory	Total RAM
Battery Status	Total % of battery available
IP Address	Devices IP Address used to connect to MobiControl
Security Status	Detects "Jailbroken" devices

iOS Device Agent

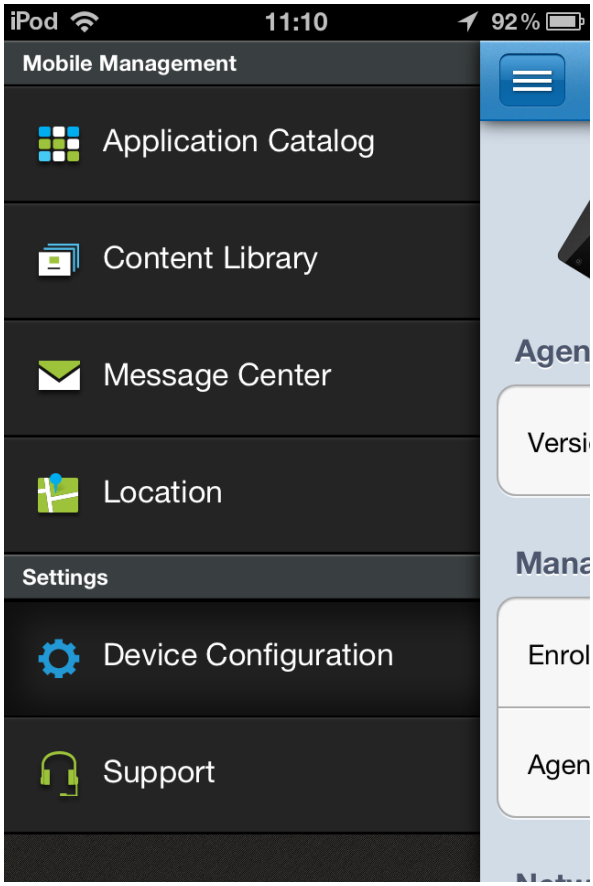
NOTE:

iOS devices must have version 4.3 or higher to be used with MobiControl

Opening the Device Agent will allow us to gain access to specific components of MobiControl. For the iOS Device Agent these components will be:

- Application Catalog
- Content Library
- Message Center
- Location
- Device Configuration
- Support

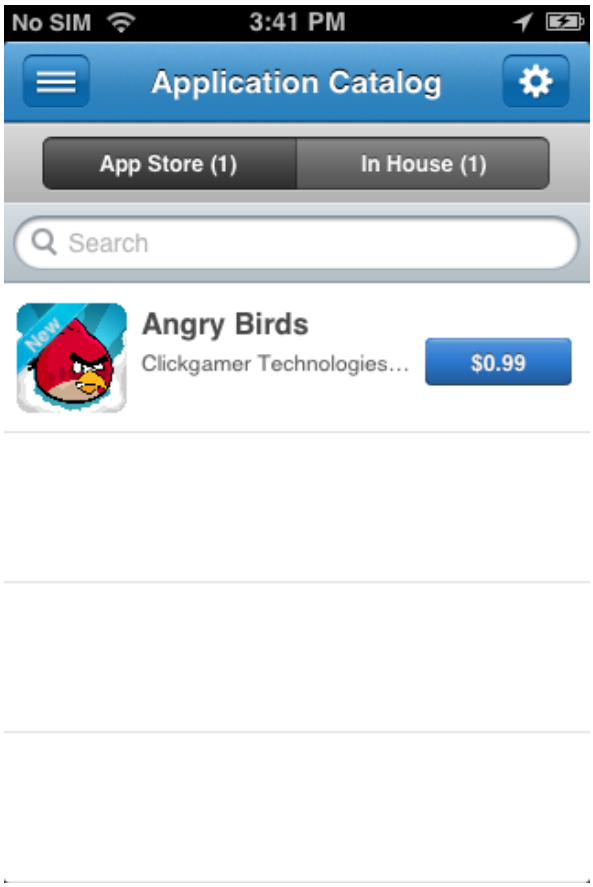
Tapping the menu button will show all these components on the left hand side.



Device Menu

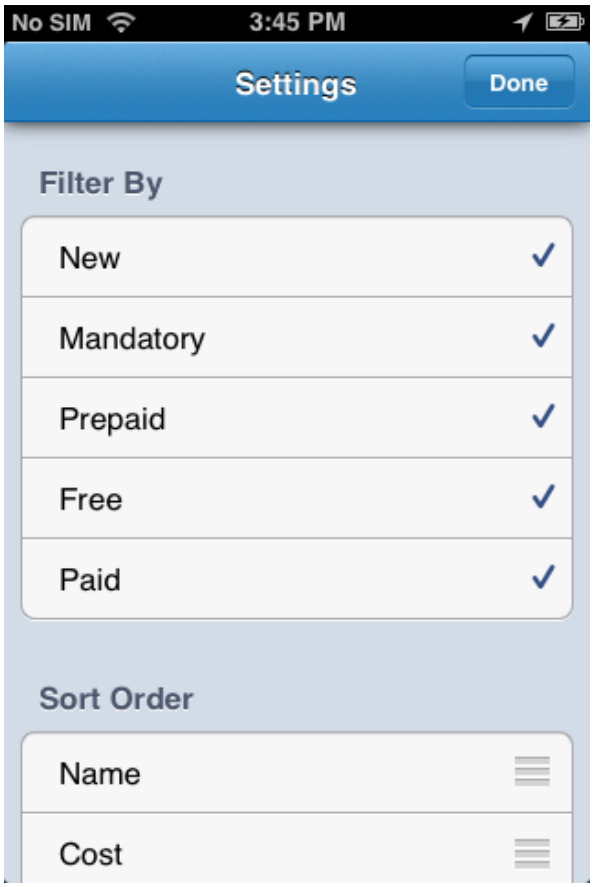
Application Catalog

The application catalog menu will show the available applications, (App Store and Enterprise), that the device is able to download. Please see the "iOS Application Catalog" topic on page 1050 for more information.



Application Catalog

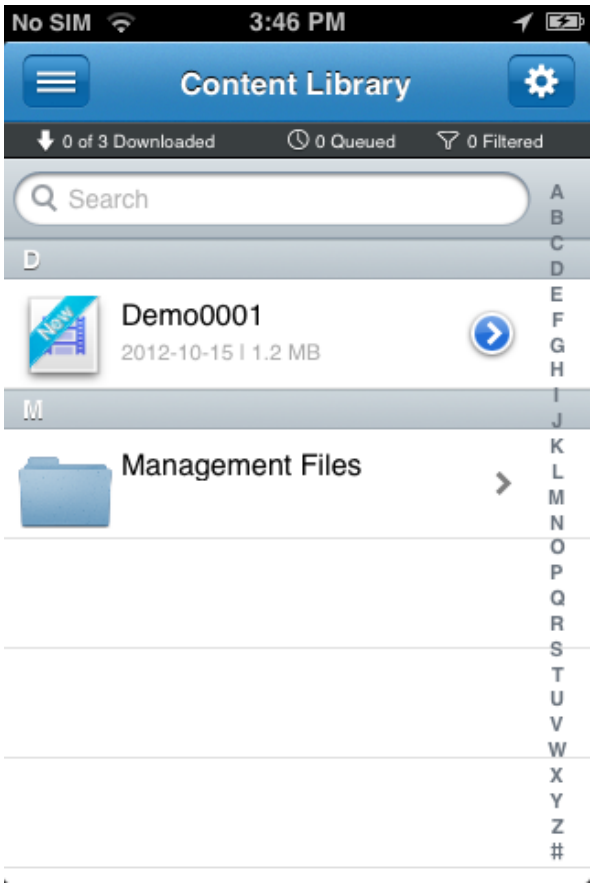
Tapping the settings icon on the top right hand corner brings out more options available to us with the application catalog. Most of these options will relate to sorting and filtering.



Application Catalog settings

Content Library

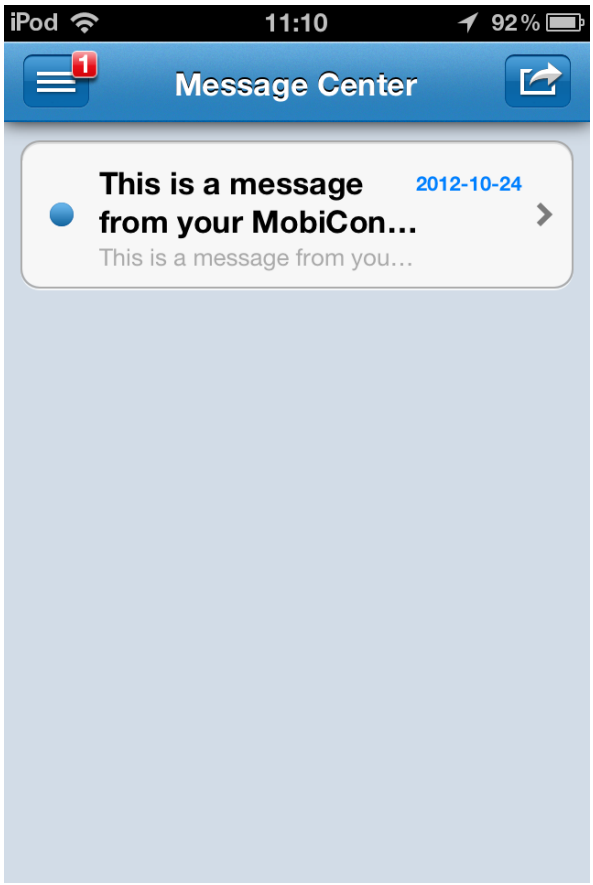
The content library tab will show all files that are available for download from MobiControl. Please see the "Secure Content Library Tab" topic on page 1456 for more information.



Content Library

Message Center

The message center will store all messages that were sent from MobiControl administrators. Users can tap each message to see the whole message.

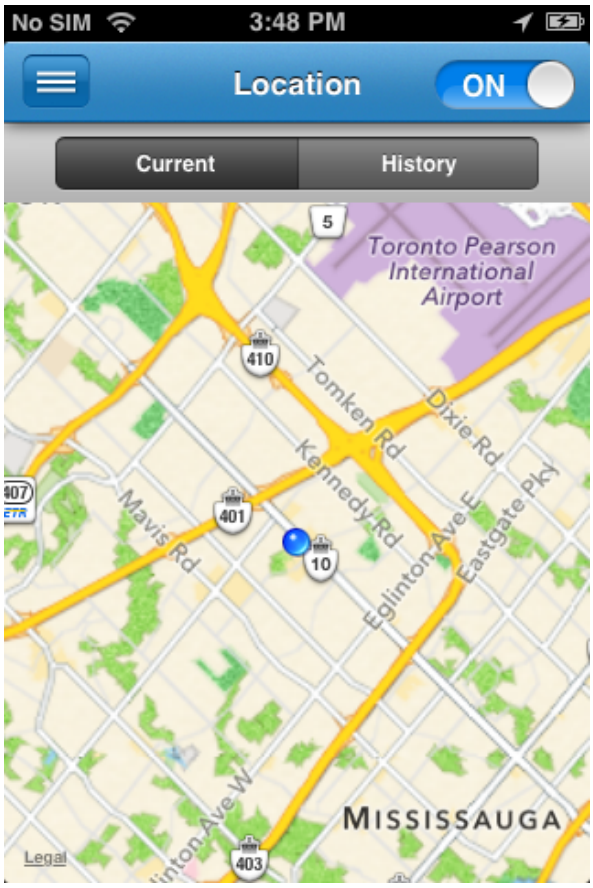


Message Center

Location

The location menu shows where the device is currently located.

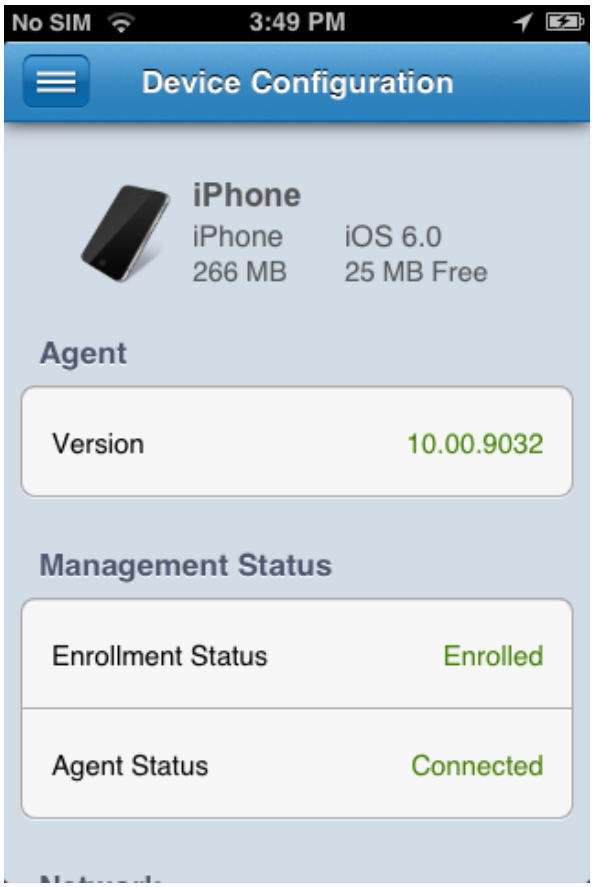
When the location switch is on, MobiControl will continuously track the device and show this in the history tab.



Location

Device Configuration

The device configuration menu shows all available information for the device. This includes the model type, iOS version, enrollment status and other bits of information.



Device Configuration

Support

The support menu will show the items that were configured from the MobiControl web console. When a user taps either the phone or email items, it will open the respective application to complete the action. For example, tapping the phone item will open up the phone application. Please see the "iOS Support Contacts Info" topic on page 1011 for more information.

Support

iOS Devices Tab

The Devices view (tab) is the main view into the status of the devices in the MobiControl system.

Device Tree

The device tree provides a structured view of the devices in the system. The group structure is easily defined by the user by creating new groups and dragging and dropping devices between groups.

Commonly-reported device information can be easily referenced in the device tree window by right-clicking in any open space in the device tree window and selecting the information that you would like to see displayed.

Devices are added to the system by defining an add device rule and creating a MobiControl Device Agent that is installed on the device. Please see the "Adding iOS Devices" topic on page 1034 for a detailed explanation of how to add devices to MobiControl.

Info Panel

The Info panel provides detailed status information about the group or device that is selected in the device tree. When a group is selected, the displayed information includes the number of subgroups and how many unique, online, offline, or disabled devices are in the group. For devices, the displayed information includes device ID, IP address, battery and memory status.

The content displayed in this panel is stored in the MobiControl database. This information is refreshed when a device establishes a new connection to the MobiControl Deployment Server, and when you click **Refresh** or press F5 on this tab.

Logs Panel

The Logs panel provides a listing of the events occurring in the MobiControl system. This listing is filtered based on the group or device that is selected in the device tree. If only one device is selected, only the events related to that device are displayed. If a group is selected, events for the group and all the devices that belong to that group are displayed.

You have the option to show or hide logging, adjust the maximum number of logs displayed, and the frequency with which the Manager should refresh the log view.

Update Schedule Panel

The Update Schedule panel lists the dates and times when the device is programmed to query the MobiControl system to check for updates. By default, a device will also check for updates whenever it connects to the MobiControl system. Please see the "iOS Device Update Schedule" topic on page 1012 for more information.

Programs Panel

The Programs panel lists the applications that are installed on the device that is selected in the device tree.

Rules Assigned Panel

The Rules Assigned panel lists the deployment and file sync rules assigned to the group or device that is selected in the device tree. Rules are inherited from parent groups; a rule will apply to a device if it belongs to group to which the rule has been assigned.

The assignment of rules to groups provides a flexible and convenient means for easily configuring devices. For example, once you have set up your rules for software or data distribution, you can automatically provision your devices by simply adding them to the appropriate group within the device tree. Please see the "iOS Rules" topic on page 1031 for information on creating deployment rules and file sync rules.

Notes Panel

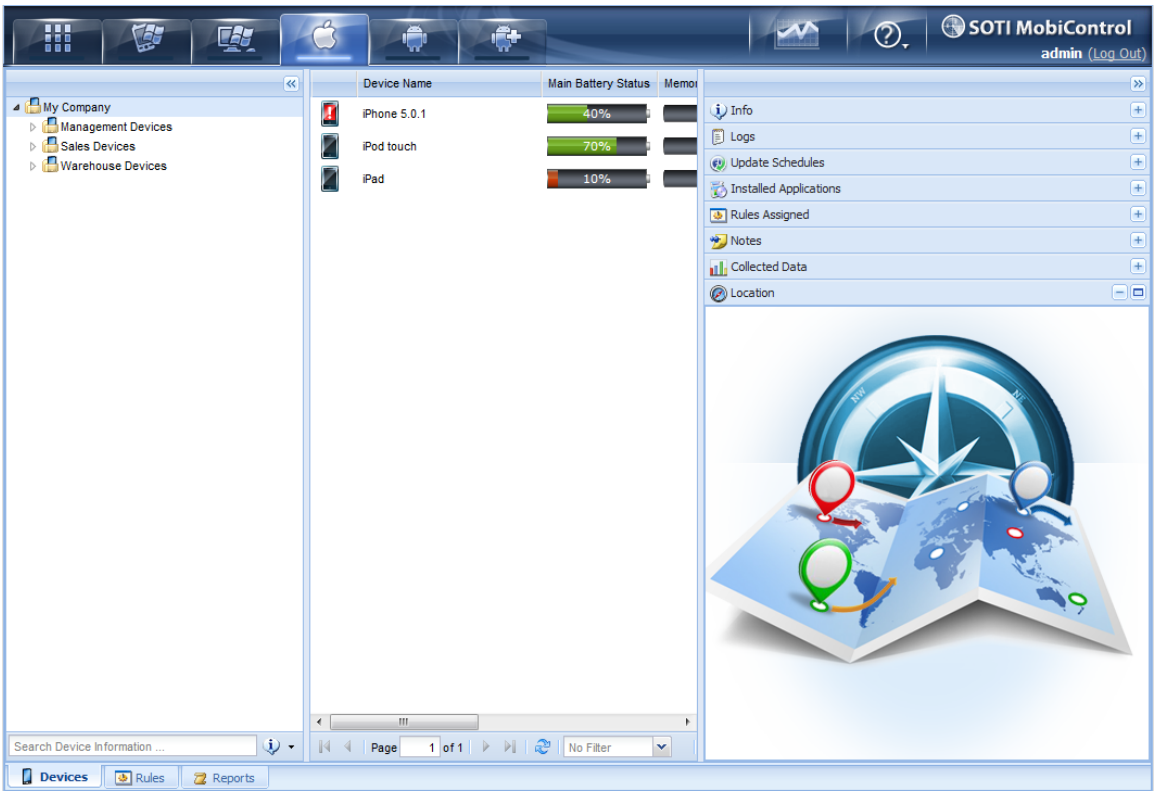
The Notes panel lists the notes that are associated with the selected device. If a group is selected in the device tree, all the notes for the devices that belong to the group are listed. Notes are a convenient way to maintain information about the device such as trouble tickets. Please see the "Device Notes" topic on page 1384 for information on creating device notes.

Collected Data Panel

The Data Collection Panel allows you to view the collected historical data for a set of devices. By creating a Data Collection Rule you will be able to specify which items to collect data from, how often to collect them, and when to upload the collected data to the server. Please see the Creating Data Collection Rules page for information on creating Data Collection.

Location Panel

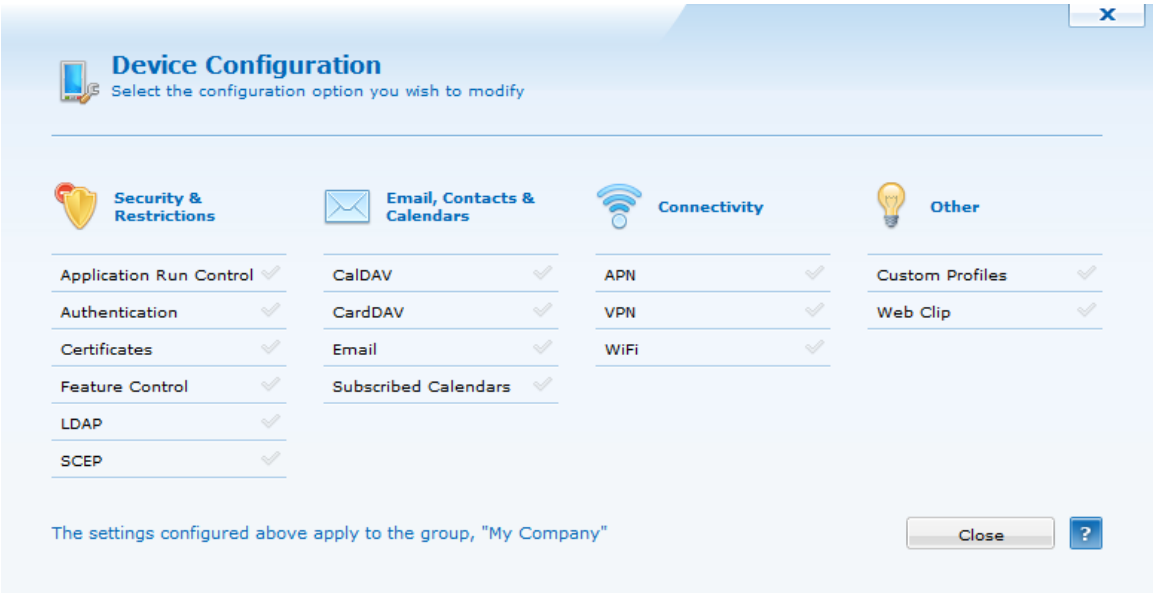
The Location Panel gives the ability to locate, track and gather information on the movement of your GPS enabled devices, no matter where they are in the world which is powered by Microsoft's Bing maps technology. Whether you need to confirm the current location of a particular field-worker, track the progress of an important shipment or collect historical information on the movement of a group of devices or vehicles in order to analyze performance, MobiControl's Location Services can help. Please see the Location Services page for more information.



MobiControl Devices Tab Devices view (tab)

iOS Device Configuration

MobiControl offers several device security options ranging from password authentication, application control, contact setup, to different connectivity settings.



MobiControl Device Configuration dialog box

MobiControl's security provides powerful features for securing devices and mobile data, while maximizing usability and making security implementation easy, efficient and cost-effective. Salient features of MobiControl's security include:

- Over-the-Air (OTA) security policy distribution
- Policies can be assigned at the individual device, group or global level
- Security managed for both online (connected) and offline (disconnected) devices

To access MobiControl's Security Center, select the device or group of devices for which you want to configure security and then click **Device,** then click **Device Configuration.**

Click each heading below to read a brief summary under each section:

Security & Restrictions

Email, Contacts & Calendars

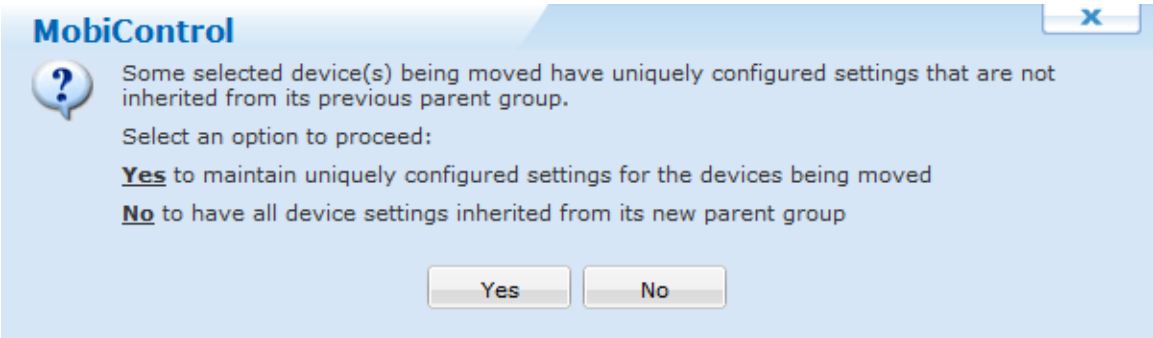
Connectivity

Other

Configuration Override Settings

Override settings allows you to create unique configuration settings at the current level which you have selected. This will override the settings that the device or group was previously inheriting from the parent group.

If the configuration settings are different at any sublevel (be it device or subgroup) then a confirmation prompt will allow you to choose whether the current setting(s) should be applied to all sub devices and groups or only the level that inherit configurations from this group.



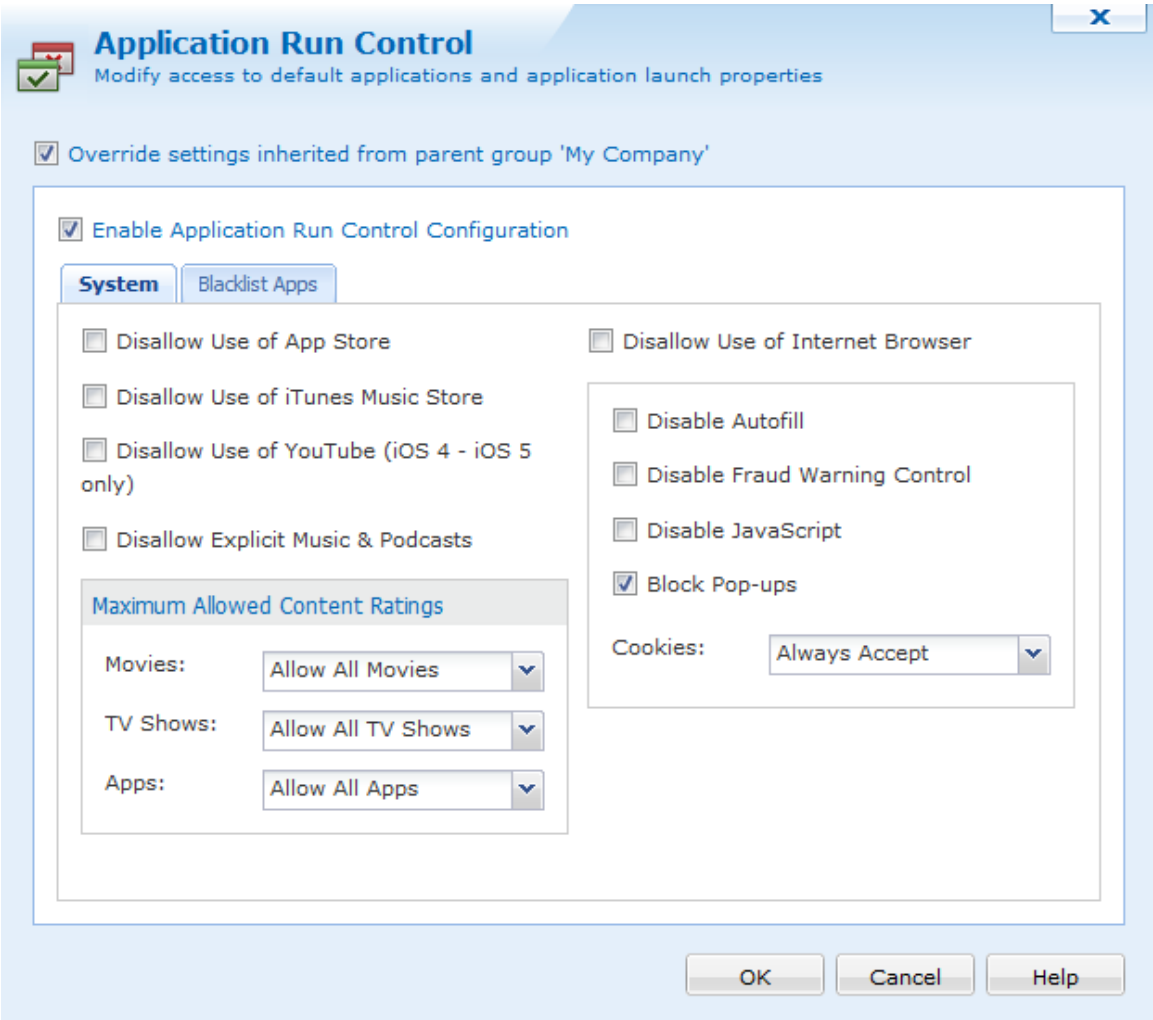
iOS Application Run Control

The easy availability of applications—games, consumer-oriented utilities and third party tools—for mobile devices results in end users installing and running unauthorized personal programs and recreational software on devices meant for business use. In addition to contributing to memory and battery life overhead, this situation also contributes to productivity losses. The installation of unauthorized and unapproved non-business applications contributes to a significantly higher volume of support calls, increasing the IT help desk's support burden. Most critically, it is imperative for security-conscious users to control and restrict the unauthorized installation of personal applications to ensure compliance with strict mobile data protection requirements.

MobiControl's application run control features reduce the risk of leakage of sensitive data and complement the existing network security model by preventing the introduction of malware and viruses into the network through the mobile devices. Additionally, it also allows memory management on the mobile devices to free up resources taken up by unnecessary processes, and allowing for better device performance. MobiControl integrates tightly with the operating system to prevent restricted applications from running entirely on the mobile device, making it much more efficient than competing white list and black list solutions which use CPU and battery-consuming processes to monitor for and destroy restricted applications.

To enable application run control for a device or group of devices, select **Application Run Control Policy** from the MobiControl Security Center. (Please see the "iOS Device Configuration" topic on page 962.)

Application Run Control System Configuration



Application Run Control dialog box System Tab

The following table will describe the features provided on the System Tab.

Feature	Description
Disallow use of App Store	Removes the **App Store** icon from the device preventing the user from installing additional applications. **IMPORTANT:** All applications, including both App Store and Enterprise applications will remain on the device and be available for the user to use.
Disallow use of iTunes Music Store	Prevents the user from purchasing music from the iTunes Music Store App.
Disallow use	Prevents the user from viewing YouTube content via the YouTube App. The user will

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>of YouTube</td><td>still be able to access www.YouTube.com unless Internet access is filtered. Only functional with iOS 4 and 5.</td></tr>
<tr><td>Maximum allowed content ratings</td><td>This setting sets the maximum rating of a Movie, TV Show or App allowed to be used on the device

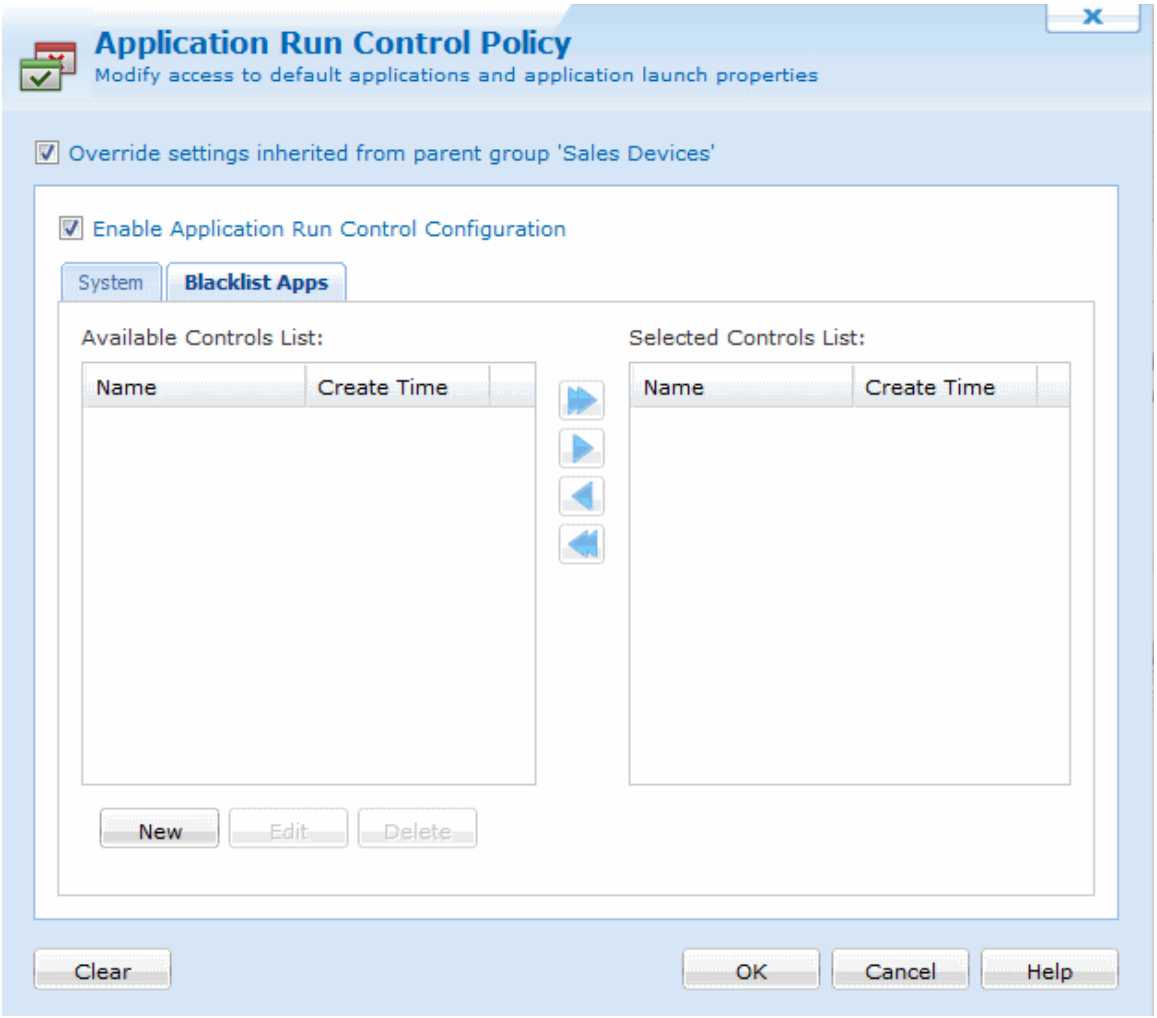
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Movies</td><td>Sets the maximum rating for movies to:
Don't Allow Movies
G
PG
PG-13
R
NC-17
Allow All Movies</td></tr>
<tr><td>TV Shows</td><td>Sets the maximum rating for TV shows to:
Don't Allow TV Shows
TV-Y
TV-Y7
TV-G
TV-PG
TV-14
TV-MA
Allow All TV Shows</td></tr>
<tr><td>Apps</td><td>Sets the maximum rating for apps to:
Don't Allow Apps
IMPORTANT:
All App Store applications will be removed from the device. The user will still be able to view the App Store's content, however, they will not be able to download or install any applications from it. All Enterprise Apps will still be available for the user to use.
4+
9+
12+
TV-PG
17+
Allow All Apps</td></tr>
</table>
</td></tr>
</table>

Feature	Description
Disallow use of Internet Browser	Prevents the user from browsing the Internet.
Disable autofill	Prevents the user from using browser autofill.
Disable fraud warning control	Prevents the user from changing the fraud warning settings.
Disable JavaScript	Prevents the user from running JavaScript applications.
Cookies	Sets the cookie settings to: • Always accept • From visited sites only • Never accept

NOTES:

- When logged in as Admin on the mobile device, application control enforcement is suspended.
- Certain processes and applications are critical and necessary for stable device operation and normal execution of the MobiControl Device Agent. These processes are automatically protected through a built-in "permanent white list" and cannot be put on a black list. Applications that are included in a lockdown program menu are automatically on a white list, and cannot be put on a black list.

Application Run Control Blacklist Applications



Application Run Control dialog box Blacklist Tab

Control List Creation

Configuration of application run control begins with the creation of an application control list. An application control list is simply a listing of the names of the Bundle Identifiers that correlate to the application you may wish to disallow on the mobile device. For example, `pword.exe` corresponds to XXXXXXX.

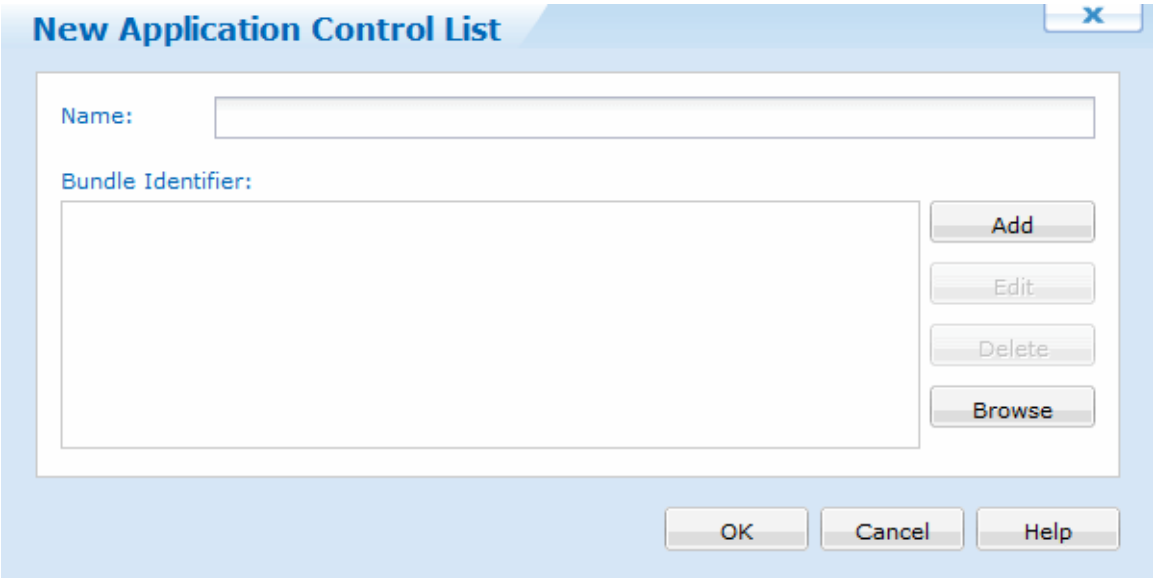
Manual Mode

Manual list creation is provided for the device administrator who already knows exactly which Bundle Identifiers are to be put on the black list. This advanced feature is only recommended if you are aware of the names of the Bundle Identifiers that need to be allowed for correct device operation, and those that you wish to restrict.

You can manually create a new application control list by clicking the **New** button in the **Application Run Control** dialog box, and then choosing the **Manually Create a New Control List** option in the **Select Control List Creation Method** dialog box. The **New Application Control List** dialog pops up, allowing you to specify the application that you want to add to the list, and the platform for which this entry

would be valid. This allows you to restrict applications on a device running a specific operating system (e.g. Windows Mobile 5), if you have a mix of devices with different operating systems in the same group.

Once created, the list may be applied to one or more devices or groups.



Creating a black list in manual mode

Modifying or Deleting a Control List

An application control list can be edited whether it is currently in use or not, but its type (white list or black list) cannot be changed once created.

An application control list can only be deleted if it is currently not selected for any devices or device groups. A control list that is listed in the **Selected** field is considered in-use, even if the application run control is disabled for the given group or device.

NOTE:

If you edit an application control list that is shared among device groups that are not subgroups of the group you are configuring, the changes will not be propagated to the other devices. The modified control list will only affect devices belonging to the group being configured or its subgroups.

Application Run Control Event Notification

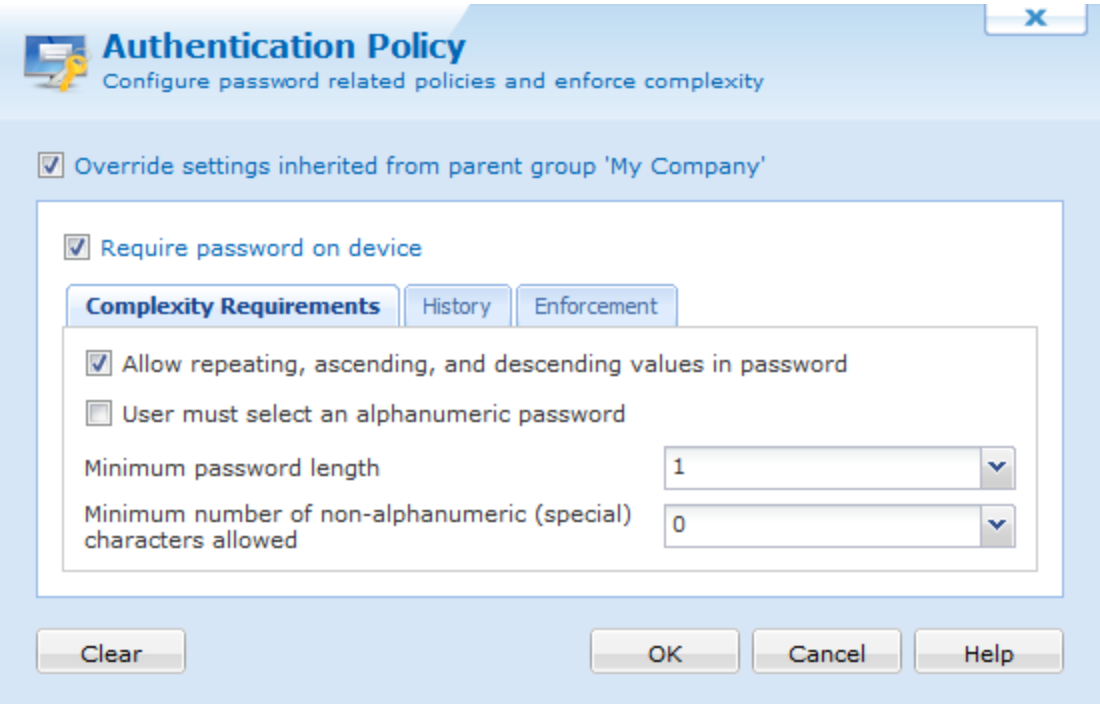
Every time MobiControl's application run control feature detects an application that is not allowed to run by the security policy in effect, it will notify the server.

The **Notify Server on Application Termination** option will generate a log event on the server and display it in the Event Logs for that particular device when an attempt is made to run a blocked operation. Device logs can be viewed in the MobiControl Manager by highlighting the device or the group of devices and enabling the **Logs** tab. This allows the administrators using MobiControl Manager to track any attempts by the end users to run or install unauthorized applications and ensures a higher level of monitoring.

iOS Authentication

The Authentication Policy option in the **MobiControl Security Center** dialog box allows administrators to set up device-side, password-based user authentication.

To enable Authentication Security for a device or group of devices, select **Authentication Policy** from the MobiControl Security Center. (Please see the "iOS Device Configuration" topic on page 962.)



Device Authentication Configuration dialog box

Field Name	Description
Require Password	If no user authentication is set. Any user can access the mobile device without any authentication
Allow repeating, ascending, and descending values	Allows the user to create a password that contains repeating, ascending, and descending values, such as 1234, or 1111
User must select an alphanumeric password	Requires the user to have numbers and letters in their password.
Minimum password length	Requires the user to have a minimum password length
Minimum number of special characters	Requires the user to have number of special characters in their password

Device Authentication Configuration dialog box

Field Name	Description
Maximum Password Age	Requires the user to change their password after the specified amount of time
Number of Unique passwords	Specifies how many passwords must be unique before the same password can be used again

Device Authentication Configuration dialog box

Field Name	Description
Auto Lock	Specifies how long before the device will lock after inactivity
Password Lock	Specifies how long the device can be locked for before requiring the user to re-enter their password
Maximum # of failed attempts	Specifies how many time an incorrect password can be entered before the device is wiped

iOS Certificates

With MobiControl's certificate policy, we are able to install certificates on devices on behalf of authenticated users or devices.

To get here, right click a device/device group, and select Device Configuration. Once the Device Configuration window appears, click **Certificates**.

Here, we are able to upload certificates, or generate new ones based on Templates.

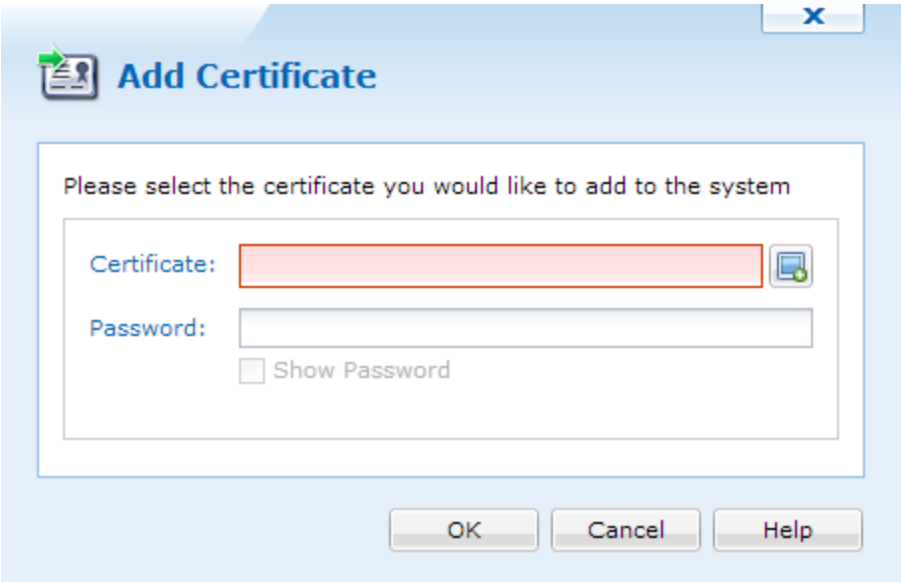
NOTE:

To set up certificate templates, Certificate Authorities must be set up. Please see the Certificate Authorities page for more information.

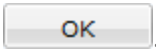
Certificates

Device Configuration - Certificates

When the Certificates window is open, we can upload new certificates by clicking New.



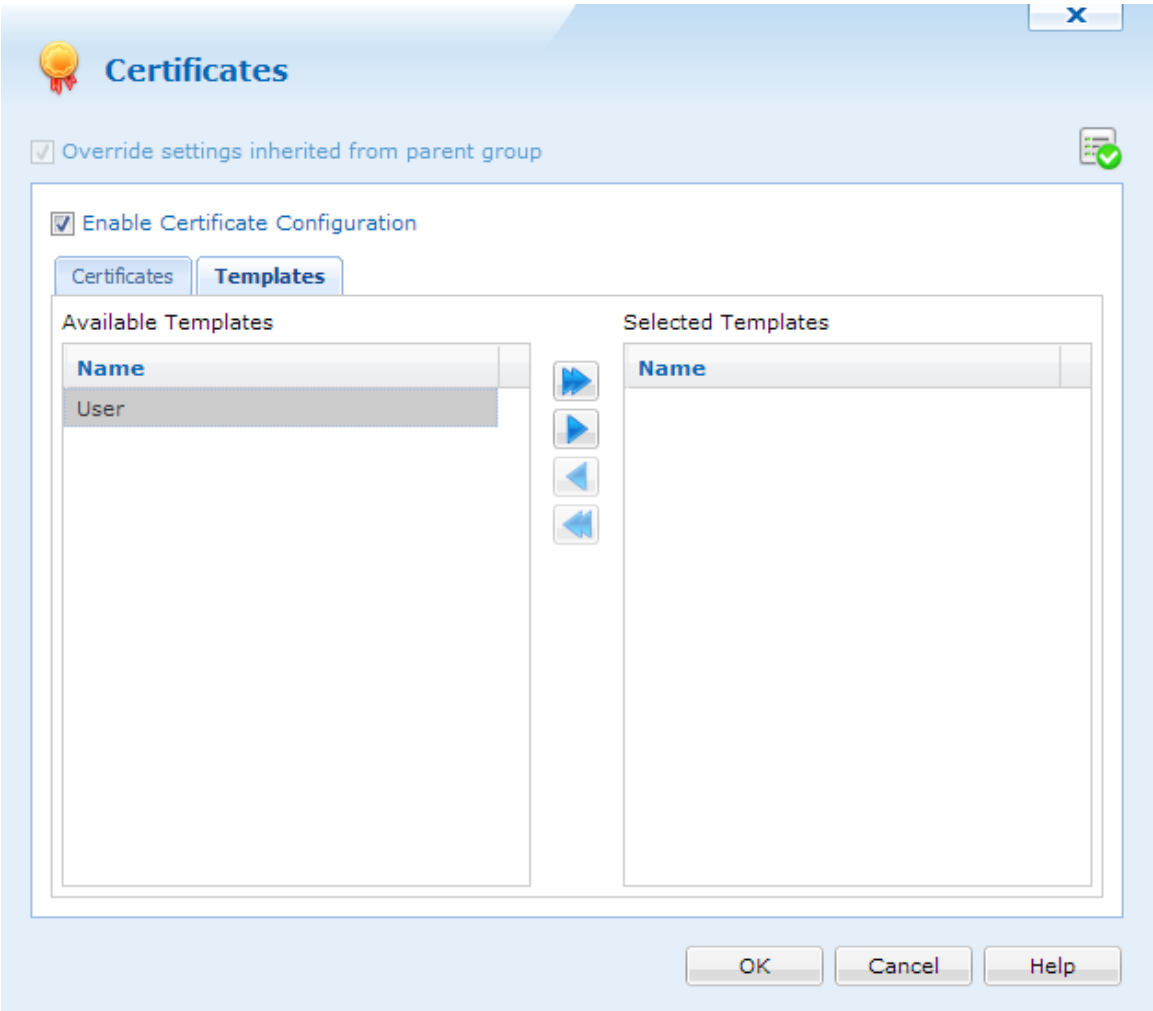
Adding new certificates

Click  to select a certificate. When uploaded, type the password associated with it, and click  .

When the certificate is added, we can select it and click any of the right arrows to move it to the *Select Certificates* panel. This will now install the certificate on the device or device group it is configured for.

Templates

Templates allows MobiControl to request a certificate on behalf of a user or device, and install it. This allows for dynamic certificates.



Selecting Certificate Templates

Certificate Templates are based off the templates configured in Certificate Authorities. Please see the Certificate Authorities page for more information about certificate templates.

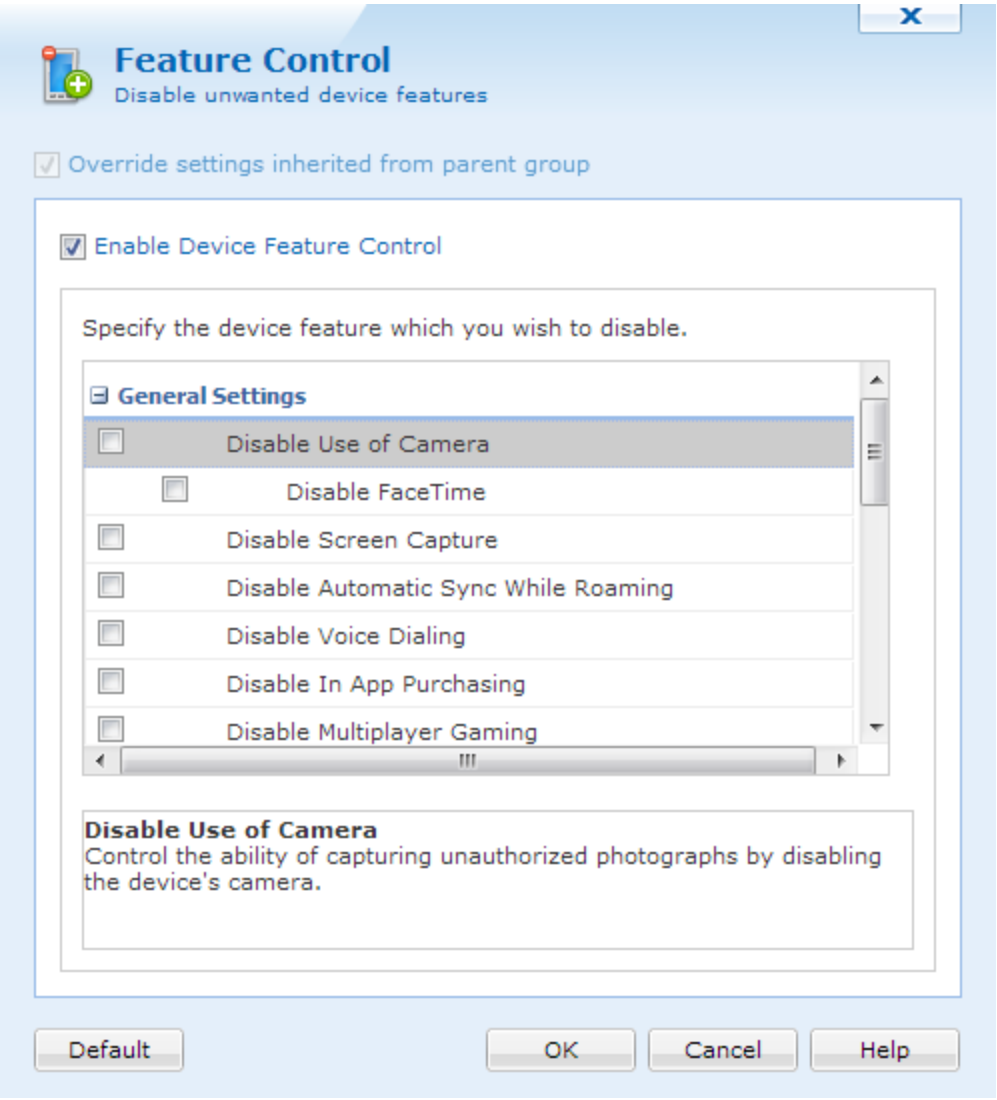
When templates are configured, we can select one or many, and move it to the **Selected Template**s panel.

After all certificates have been selected, clicking OK, will close the window and apply the settings.

iOS Feature Control

For security-conscious organizations and environments where privacy and information security concerns require controlling the unauthorized transfer of mobile data out of the mobile devices, MobiControl provides various on-device feature controls including the capability to block various device communications, similar to firewall functionality. MobiControl's device features control policy allows IT administrators to selectively disable device features. Applying the policy at the individual or group level

allows custom profiles for different users and locations in an organization. The ability to disable or enable Bluetooth and infrared ports allows controlling whether end users can beam business cards, applications or documents to one another.



Device Feature Control Policy dialog box

To enable device feature control for a device or group of devices, select **Device Feature Control Policy** from the MobiControl Security Center. (Please see the "iOS Device Configuration" topic on page 962.)

The following features can be enabled or disabled using the device feature control policy:

Option	Description
Disable use of Camera	Control the ability of capturing unauthorized photographs by disabling the device's camera.
Disable FaceTime	Prevents the user from utilizing FaceTime.
Disable screen capture	Control the ability of applications to capture the device screen.
Disable automatic sync while roaming	Control the ability to sync data (i.e. email) while in foreign coverage areas and prevent related expenses by disabling roaming syncing.
Disable voice dialing	Prevents the user from using the voice dialing feature.
Disable In App Purchasing	Prevents the user from purchasing additional features of an application or an additional app from within an app.
Disable multiplayer gaming	Prevents the user from engaging in multiplayer gaming.
Force encrypted backups to iTunes	Forces backups to iTunes to be encrypted, this is always selected.

iOS 5 and 6 only options

Option	Description
Force user to enter iTunes password for each transaction	Forces the user to enter their iTunes password for each iTunes transaction.
Automatically reject untrusted HTTPS certificates	Automatically reject untrusted HTTPS certificates.
Disable iCloud device backup	Prevents the user from backing up the device with iCloud.
Disable iCloud document syncing	Prevents the user from automatically syncing documents to iCloud.
Disable iCloud key-values syncing	Prevents the user from automatically syncing key-values to iCloud.
Disable Photo Stream	Prevents the users from using the photo streaming function.
Disable voice roaming	Disables voice calls while the device is roaming.
Disable voice roaming setting	Prevents the user from changing the setting for voice calls while roaming.

Option	Description
Disable data roaming	Disables data while the device is roaming.
Disable data roaming setting	Prevents the user from changing the setting for data while roaming.
Enforce data roaming setting	Forces the data roaming setting to enabled.
Disable Siri	Prevents the user from using Siri.
Disable diagnostic submission	Prevents the user from submitting diagnostic information.

iOS SCEP

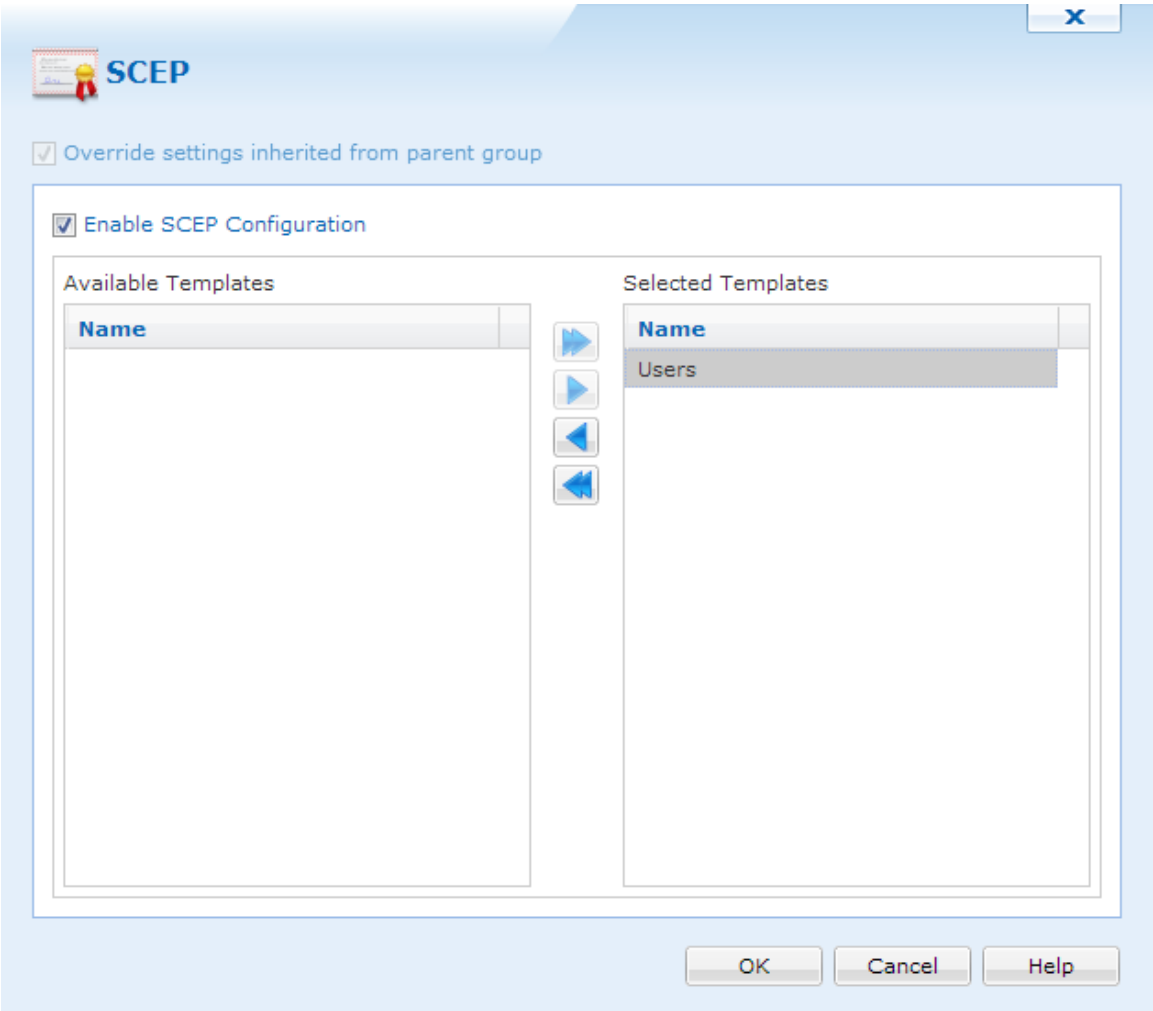
MobiControl's SCEP policy, configures iOS devices to reach a SCEP server and request a certificate.

To get here, right click a device/device group, and select Device Configuration. Once the Device Configuration window appears, click **SCEP**.

NOTE:

To set up certificate templates, Certificate Authorities must be set up. Please see the Certificate Authorities page for more information.

Templates allows the same configuration to be sent down to iOS devices. This ensures that each certificate received by the device is dynamic.



Selecting SCEP Templates

Templates are based off the templates configured in Certificate Authorities. Please see the Certificate Authorities page for more information about certificate templates.

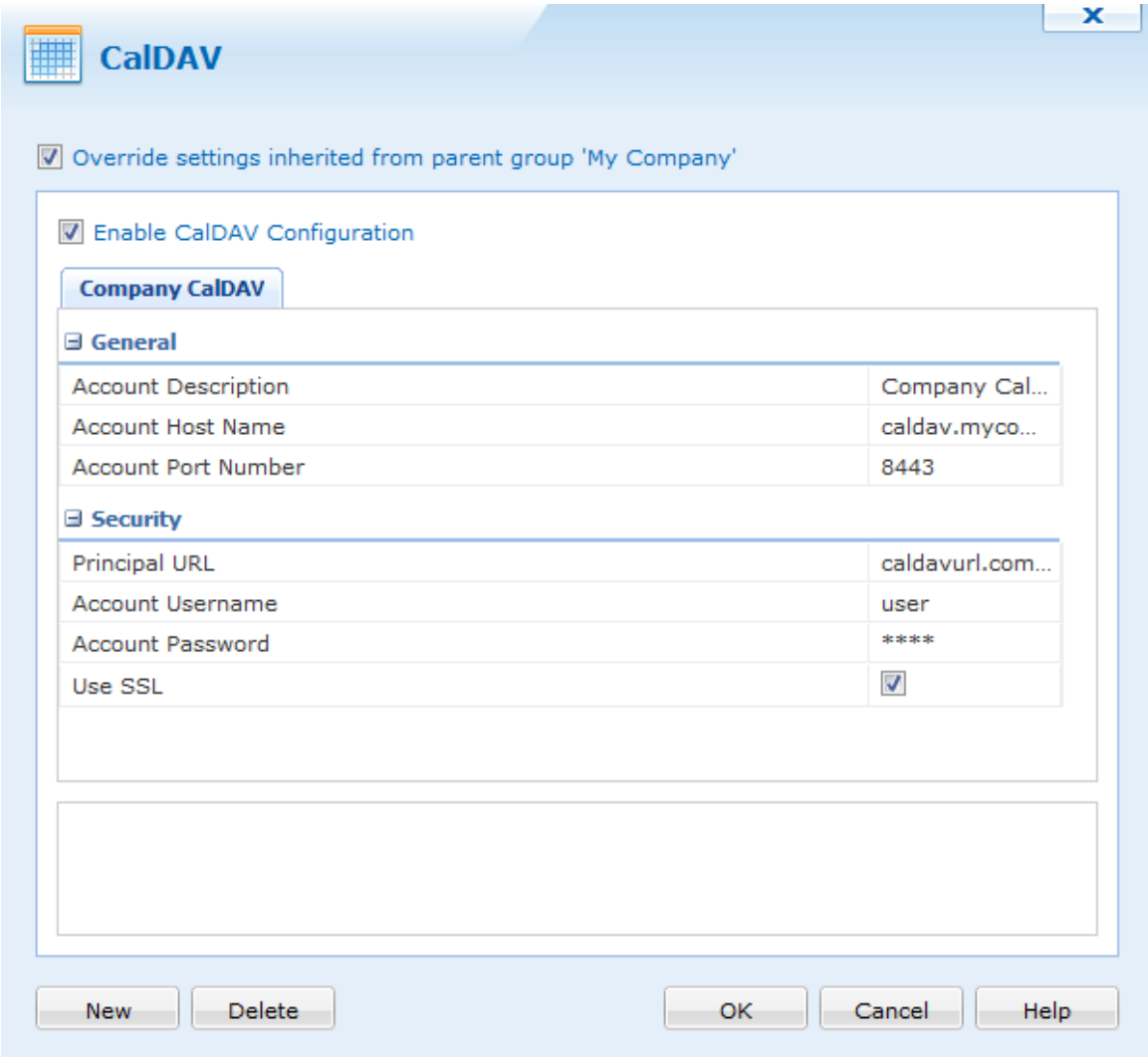
When templates are configured, we can select one or many, and move it to the **Selected Template**s panel.

After all templates have been selected, clicking OK, will close the window and apply the settings.

iOS CalDAV configuration

Setting up the CalDAV configuration allows devices to download specified company calendars. Once configured, information from these calendars will be placed on the iOS calendar app.

To access the CalDAV configuration right click any iOS device or group, then click **Device Configuration**. Once the Device Configuration panel opens, click **CardDAV**.



iOS CalDAV configuration

General Settings

Below is an explanation for each field under the general settings:

Field Name	Description
Account Description	The display name for this configuration
Account Host Name	The CalDAV account host name
Account Port Number	The CalDAV account port number

Security

Below is an explanation for each field under the general settings:

Field Name	Description
Principal URL	The URL for the CalDAV account

Field Name	Description
Account Username	The username for the CalDAV account
Account Password	The password for the CalDAV account
Use SSL	If selected, this enables SSL communication with the CalDAV server

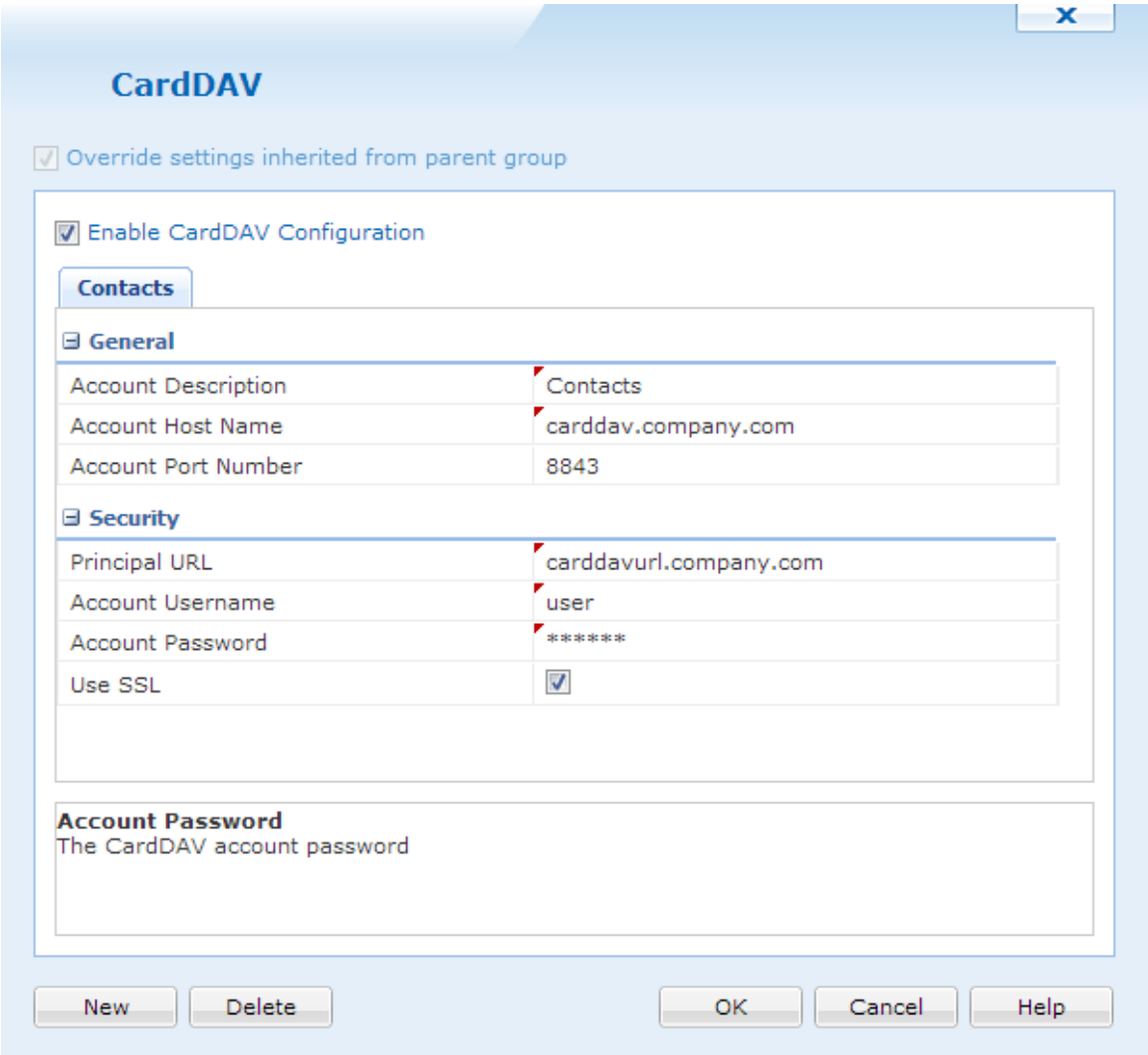
If more than one CalDAV configuration is needed, just click New. If one isn't needed any more click Delete.

When all configurations are complete, click OK to save and close the window.

iOS CardDAV

Setting up the CardDAV configuration allows devices to download specified company contacts. Once configured, information from these directories will be placed on the iOS contacts app.

To enable the CardDAV Policy for a device or group of devices, right click a device or group, and select **Device Configuration**, from there, click **CardDAV**.



CardDAV dialog box

General Settings

Below is an explanation for each field under the general settings:

Field Name	Description
Account Description	The display name for this configuration
Account Host Name	The CardDAV account host name
Account Port Number	The CardDAV account port number

Security

Below is an explanation for each field under the general settings:

Field Name	Description
Principal URL	The URL for the CardDAV account

Field Name	Description
Account Username	The username for the CardDAV account
Account Password	The password for the CardDAV account
Use SSL	If selected, this enables SSL communication with the CardDAV server

If more than one CardDAV configuration is needed, just click New. If one isn't needed any more click Delete.

When all configurations are complete, click OK to save and close the window.

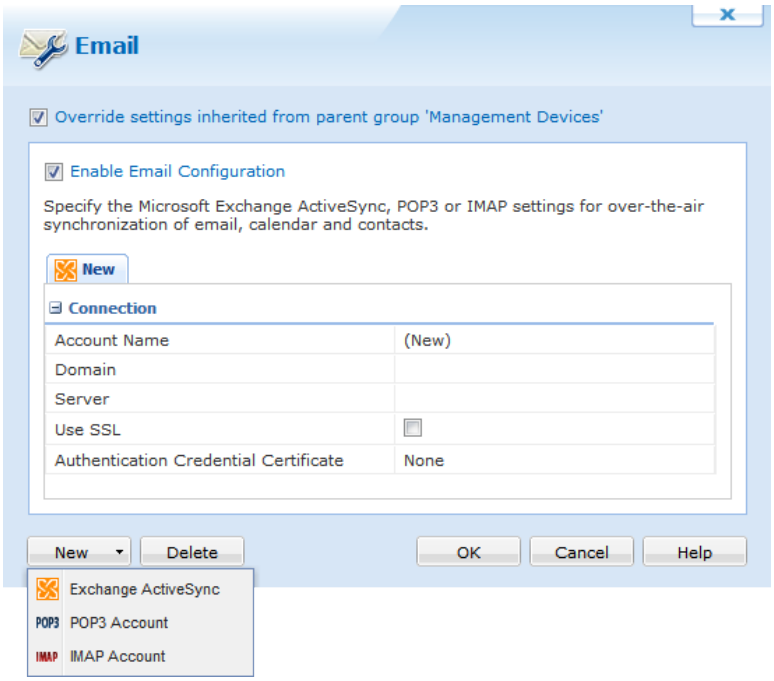
iOS Email Configuration

With MobiControl, you can now completely configure Email settings for your Apple iOS device.

To arrive at this configuration menu, select the device or the group, right-click, select **Configure Device(s)**, and click **Email Configuration**.

When clicking on **New** you can configure the following types of Email accounts:

- Microsoft Exchange
- POP Email
- IMAP Email

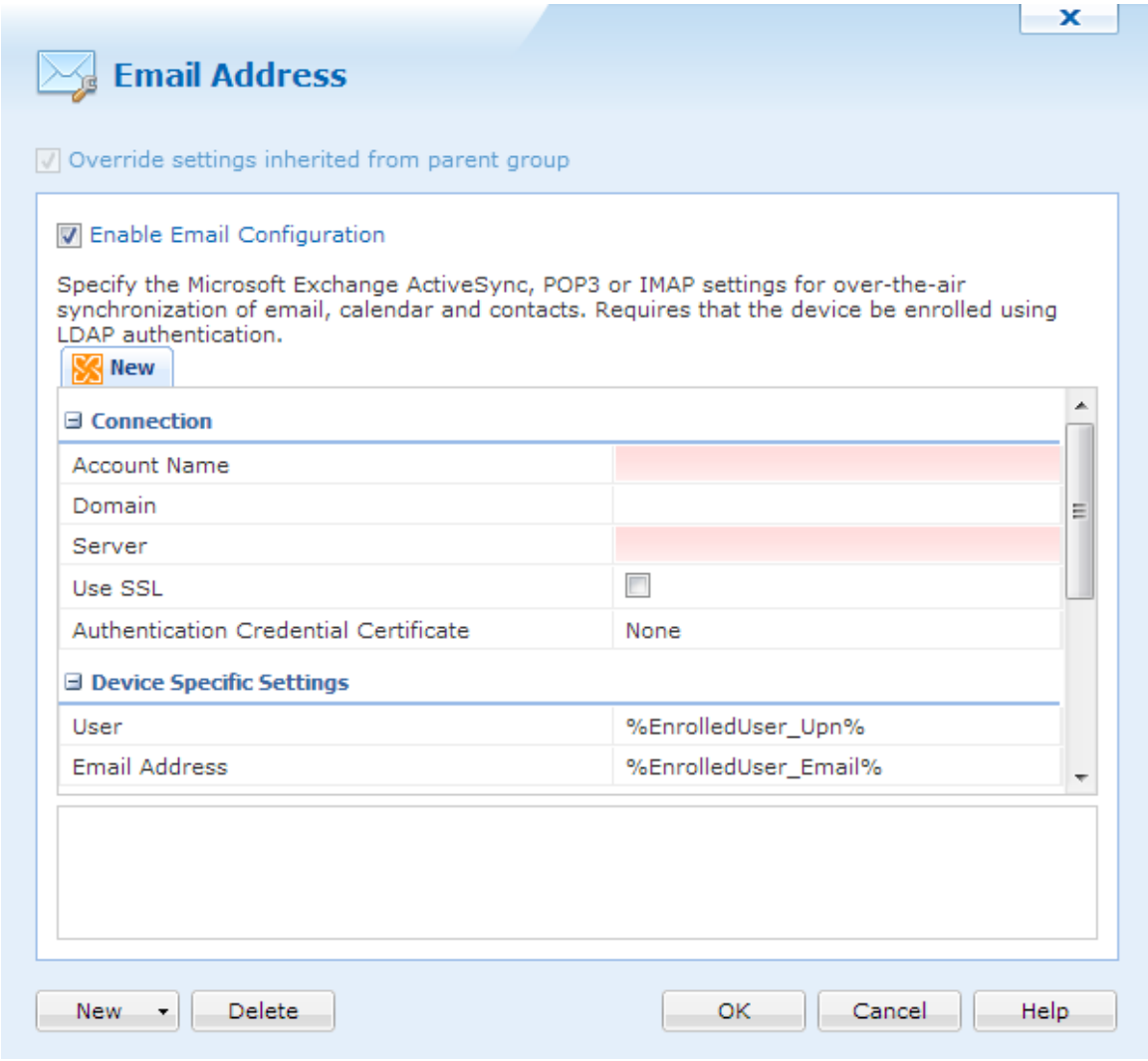


NOTE:

Multiple Email accounts can be provisioned from this same screen simply by pressing the **New** button and selecting the account type.

iOS Microsoft Exchange Email Configuration

With MobiControl, you can configure Microsoft Exchange Email settings for your Apple iOS device. To arrive at this configuration menu, select the device or the group, right-click, select **Configure Device(s)**, and click **Email Configuration**.



Connection Options

Option	Description
Account Name	Enter the account name of your organization.
Domain	Enter the domain name of your organization.
Server	Enter the server address of your organization.
Use SSL	This option allows the end user to select whether or not SSL is used for communication with the Exchange server.

Option	Description
Authentication Credential Certificate	Select an Authentication Credential Certificate from the list of authentication certificates installed on the device.
User	Enter the user name associated with your exchange account.
Password	Enter the account password here.
Re-type Password	Re-type the account password here to verify accuracy.
Email	Enter the Email address associated with your exchange account.
Sync the past	Select how far back to synchronize past Emails. The following options are available: • One Day • Three Days • One Week • Two Weeks • One Month • 3 months • 6 months • Unlimited

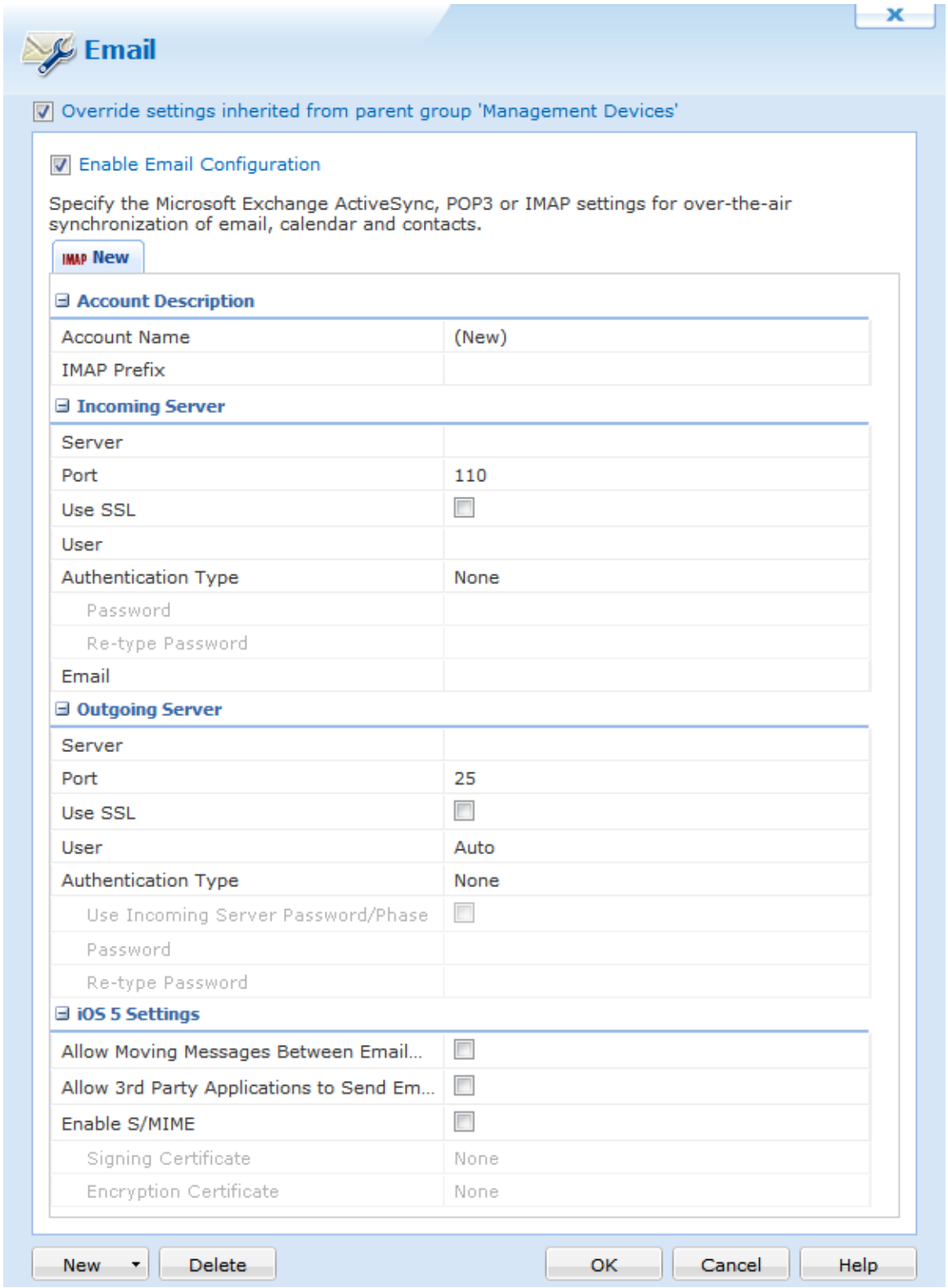
iOS 5 and 6 only options

Option	Description
Allow Moving Messages Between Email Accounts	Permits the users to move Email messages between the different configured Email accounts on the device.
Allow 3rd Party Applications to Send Email	Permits 3rd party applications on the device to use this Email account for sending Email.
Enable S/MIME	Allows you to utilize the following S/MIME cryptographic security services for Emails accounts: • authentication • message integrity • non-repudiation of origin (using digital signatures) • privacy and data security (using encryption) S/MIME specifies the MIME type application/pkcs7-mime (smime-type "enveloped-data") for data enveloping (encrypting) where the whole (prepared) MIME entity to be enveloped is encrypted and packed into an object which subsequently is inserted into

Option	Description
	an application/pkcs7-mime MIME entity.
Signing Certificate	Select the existing S/MIME Signing Certificate from the certificate library on the device.
Encryption Certificate	Select the existing S/MIME Encryption Certificate from the certificate library on the device.

iOS Device IMAP Email Configuration

With MobiControl, you can now configure IMAP Email settings for your Apple iOS device. To arrive at this configuration menu, select the device or the group, right-click, select **Configure Device(s)**, and click **Email Configuration**.


Email
Override settings inherited from parent group 'Management Devices'
Enable Email Configuration
Specify the Microsoft Exchange ActiveSync, POP3 or IMAP settings for over-the-air synchronization of email, calendar and contacts.
IMAP New
Account Description
Account Name
(New)
IMAP Prefix
Incoming Server
Server
Port
110
Use SSL
User
Authentication Type
None
Password
Re-type Password
Email
Outgoing Server
Server
Port
25
Use SSL
User
Auto
Authentication Type
None
Use Incoming Server Password/Phase
Password
Re-type Password
iOS 5 Settings
Allow Moving Messages Between Email...
Allow 3rd Party Applications to Send Em...
Enable S/MIME
Signing Certificate
None
Encryption Certificate
None
New
Delete
OK
Cancel
Help

Incoming Server Settings

Option	Description
Account Name	Enter the account name of your organization.
IMAP Prefix	Specify the incoming IMAP Server prefix.
Server	Enter your IMAP server address.
Port	Enter the incoming (IMAP) mail port for the account. 110 is the default port for POP3
Use SSL	This option allows the end user to select whether or not SSL is used for communication with the Email server.
User	Enter the user name associated with your Email account.
Authentication Type	Select the type of authentication to be used for this account. Options are: • None • Password • MD5 Challenge-Response • NTLM • HTTP MD5 Digest
Password	Enter the account password here.
Re-type Password	Re-type the account password here to verify accuracy.
Email	Enter the Email address associated with your Email account.

Outgoing Server Settings

Option	Description
Server	Enter your SMTP server address.
Port	Enter the incoming (SMTP) mail port for the account. 25 is the default port for SMTP (Outgoing mail)
Use SSL	This option allows the end user to select whether or not SSL is used for communication with the Email server.
User	Enter the user name associated with your Email account. **Auto** and **Use Incoming Server Password/Phrase** is selected by default. This option will use the information provided in the **Incoming Server** settings automatically for outgoing Email. Once the checkmark is removed you can then specify a different account or passphrase for outgoing Email.
Authentication Type	Select the type of authentication to be used for this account. Options are: • None • Password • MD5 Challenge-Response • NTLM

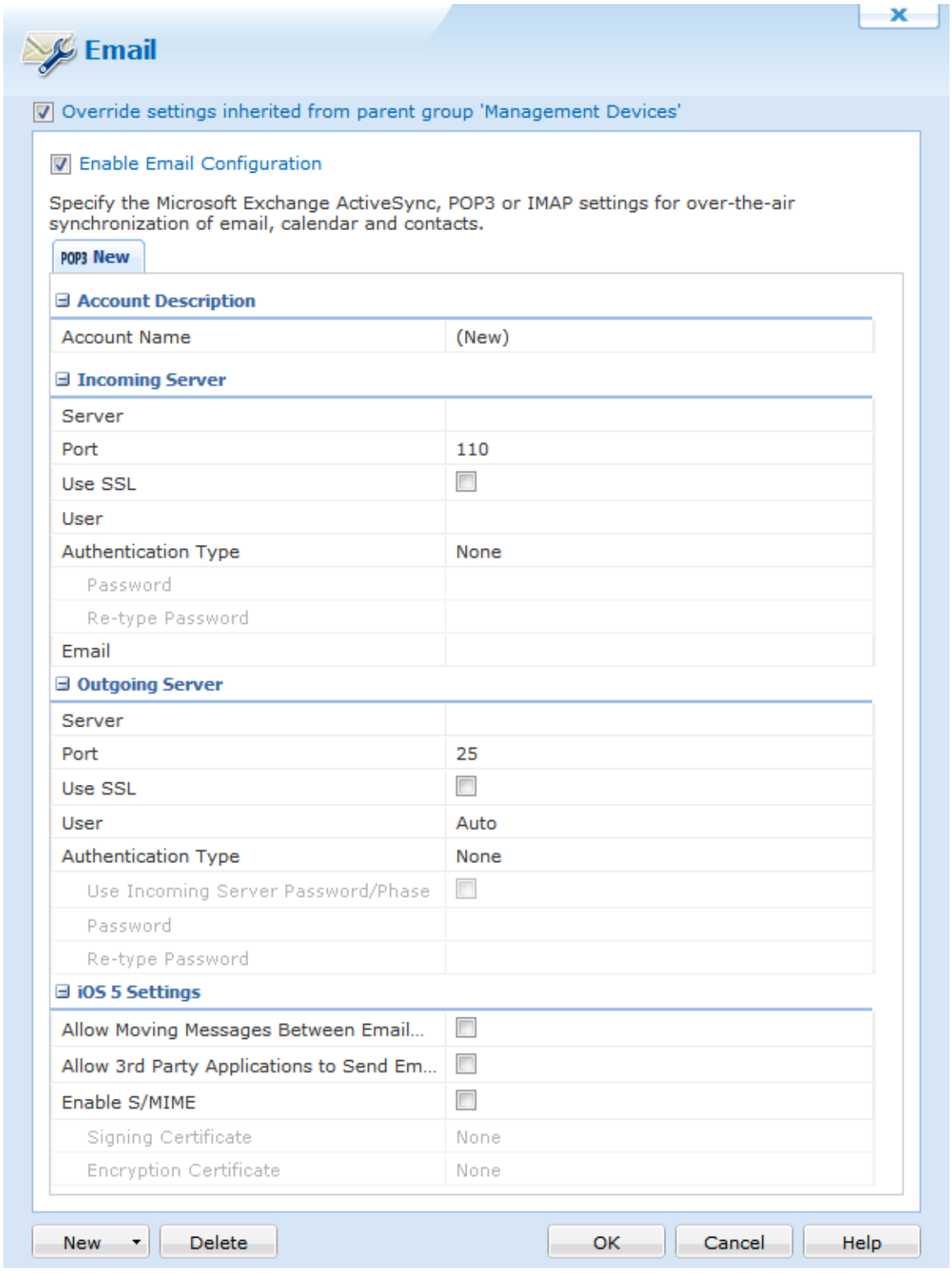
Option	Description
	• HTTP MD5 Digest
Password	Enter the account password here.
Re-type Password	Re-type the account password here to verify accuracy.
Email	Enter the Email address associated with your Email account.

iOS 5 and 6 only options

Option	Description
Allow Moving Messages Between Email Accounts	Permits the users to move Email messages between the different configured Email accounts on the device.
Allow 3rd Party Applications to Send Email	Permits 3rd party applications on the device to use this Email account for sending Email.
Enable S/MIME	Allows you to utilize the following S/MIME cryptographic security services for Emails accounts: • authentication • message integrity • non-repudiation of origin (using digital signatures) • privacy and data security (using encryption) S/MIME specifies the MIME type application/pkcs7-mime (smime-type "enveloped-data") for data enveloping (encrypting) where the whole (prepared) MIME entity to be enveloped is encrypted and packed into an object which subsequently is inserted into an application/pkcs7-mime MIME entity.
Signing Certificate	Select the existing S/MIME Signing Certificate from the certificate library on the device.
Encryption Certificate	Select the existing S/MIME Encryption Certificate from the certificate library on the device.

iOS Device POP Email Configuration

With MobiControl, you can now configure POP3 Email settings for your Apple iOS device. To arrive at this configuration menu, select the device or the group, right-click, select **Configure Device(s)**, and click **Email Configuration**.


Email
Override settings inherited from parent group 'Management Devices'
Enable Email Configuration
Specify the Microsoft Exchange ActiveSync, POP3 or IMAP settings for over-the-air synchronization of email, calendar and contacts.
POP3 New
Account Description
Account Name
(New)
Incoming Server
Server
Port
110
Use SSL
User
Authentication Type
None
Password
Re-type Password
Email
Outgoing Server
Server
Port
25
Use SSL
User
Auto
Authentication Type
None
Use Incoming Server Password/Phase
Password
Re-type Password
iOS 5 Settings
Allow Moving Messages Between Email...
Allow 3rd Party Applications to Send Em...
Enable S/MIME
Signing Certificate
None
Encryption Certificate
None
New
Delete
OK
Cancel
Help

Incoming Server Settings

Option	Description
Account Name	Enter the account name of your organization.
Server	Enter your POP3 server address.
Port	Enter the incoming (POP3) mail port for the account. 110 is the default port for POP3
Use SSL	This option allows the end user to select whether or not SSL is used for communication with the Email server.
User	Enter the user name associated with your Email account.
Authentication Type	Select the type of authentication to be used for this account. Options are: • None • Password • MD5 Challenge-Response • NTLM • HTTP MD5 Digest
Password	Enter the account password here.
Re-type Password	Re-type the account password here to verify accuracy.
Email	Enter the Email address associated with your Email account.

Outgoing Server Settings

Option	Description
Server	Enter your SMTP server address.
Port	Enter the incoming (SMTP) mail port for the account. 25 is the default port for SMTP (Outgoing mail)
Use SSL	This option allows the end user to select whether or not SSL is used for communication with the Email server.
User	Enter the user name associated with your Email account. **Auto** and **Use Incoming Server Password/Phrase** is selected by default. This option will use the information provided in the **Incoming Server** settings automatically for outgoing Email. Once the checkmark is removed you can then specify a different account or passphrase for outgoing Email.
Authentication Type	Select the type of authentication to be used for this account. Options are: • None • Password • MD5 Challenge-Response • NTLM • HTTP MD5 Digest

Option	Description
Password	Enter the account password here.
Re-type Password	Re-type the account password here to verify accuracy.
Email	Enter the Email address associated with your Email account.

iOS 5 and 6 only options

Option	Description
Allow Moving Messages Between Email Accounts	Permits the users to move Email messages between the different configured Email accounts on the device.
Allow 3rd Party Applications to Send Email	Permits 3rd party applications on the device to use this Email account for sending Email.
Enable S/MIME	Allows you to utilize the following S/MIME cryptographic security services for Emails accounts: • authentication • message integrity • non-repudiation of origin (using digital signatures) • privacy and data security (using encryption) S/MIME specifies the MIME type application/pkcs7-mime (smime-type "enveloped-data") for data enveloping (encrypting) where the whole (prepared) MIME entity to be enveloped is encrypted and packed into an object which subsequently is inserted into an application/pkcs7-mime MIME entity.
Signing Certificate	Select the existing S/MIME Signing Certificate from the certificate library on the device.
Encryption Certificate	Select the existing S/MIME Encryption Certificate from the certificate library on the device.

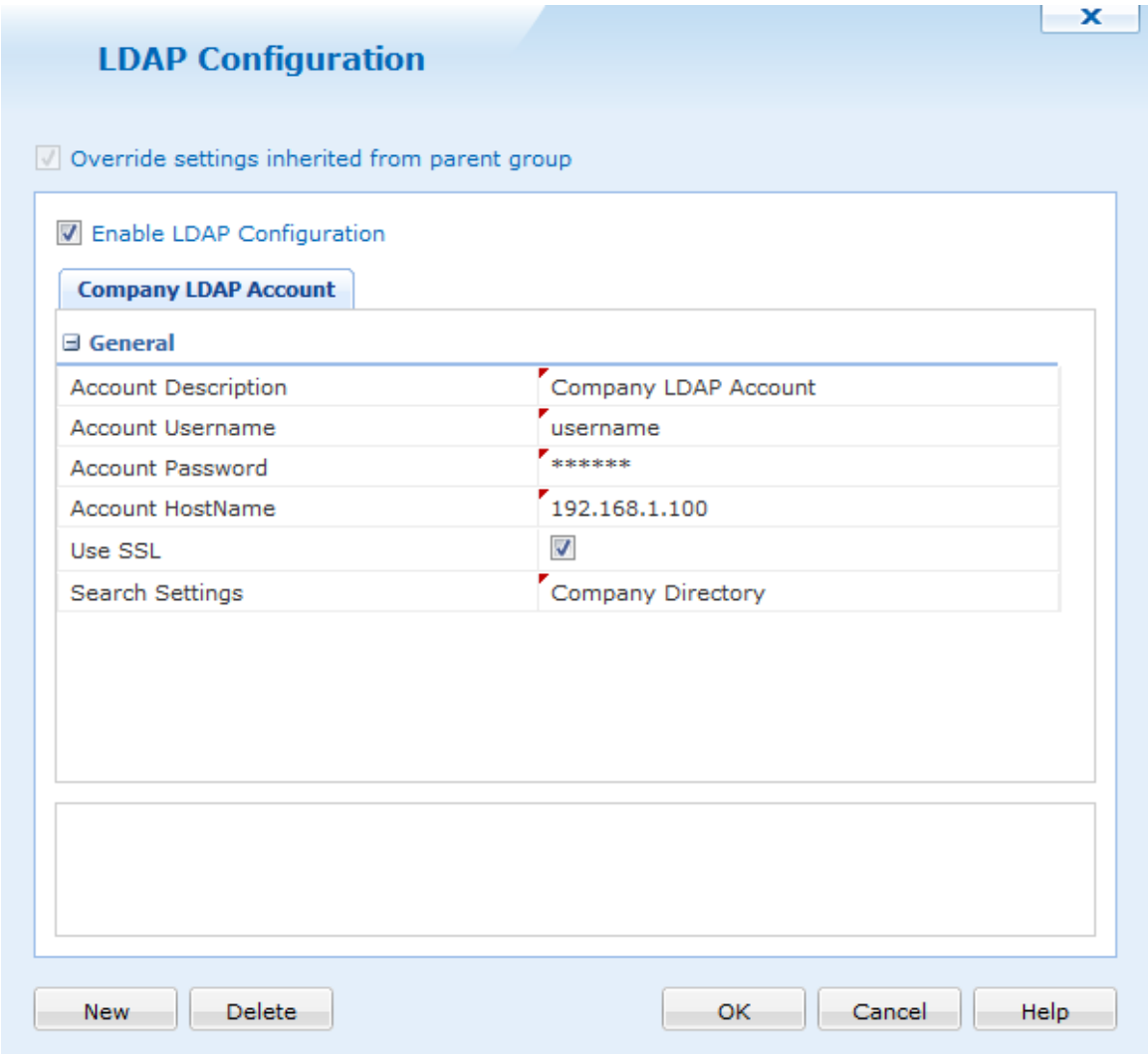
iOS LDAP Configuration

Setting up the LDAP configuration allows devices to download the company contacts currently configured in LDAP. Once configured, information from LDAP will be placed on the contacts app.

NOTE:

This does not set up LDAP authentication so that users can unlock devices; it only gives a list of contacts in the company directory.

To access the LDAP configuration right click any iOS device or group, then click **Device Configuration**. Once the Device Configuration panel opens, click **LDAP**.



iOS LDAP configuration

Below, we will go over each field included in the LDAP configuration:

Field Name	Description
Account Description	The name of this LDAP configuration
Account Username	The account name used to query LDAP
Account Password	The password for the account used for querying LDAP
Account HostName	The location of the LDAP server
Use SSL	If enabled, SSL will be used for all communications

Field Name	Description
Search Settings	Search settings allows us to search specific directories in LDAP. Clicking the text field box opens up a pop up. Clicking search settings below expands a greater explanation of this feature.

Search Settings

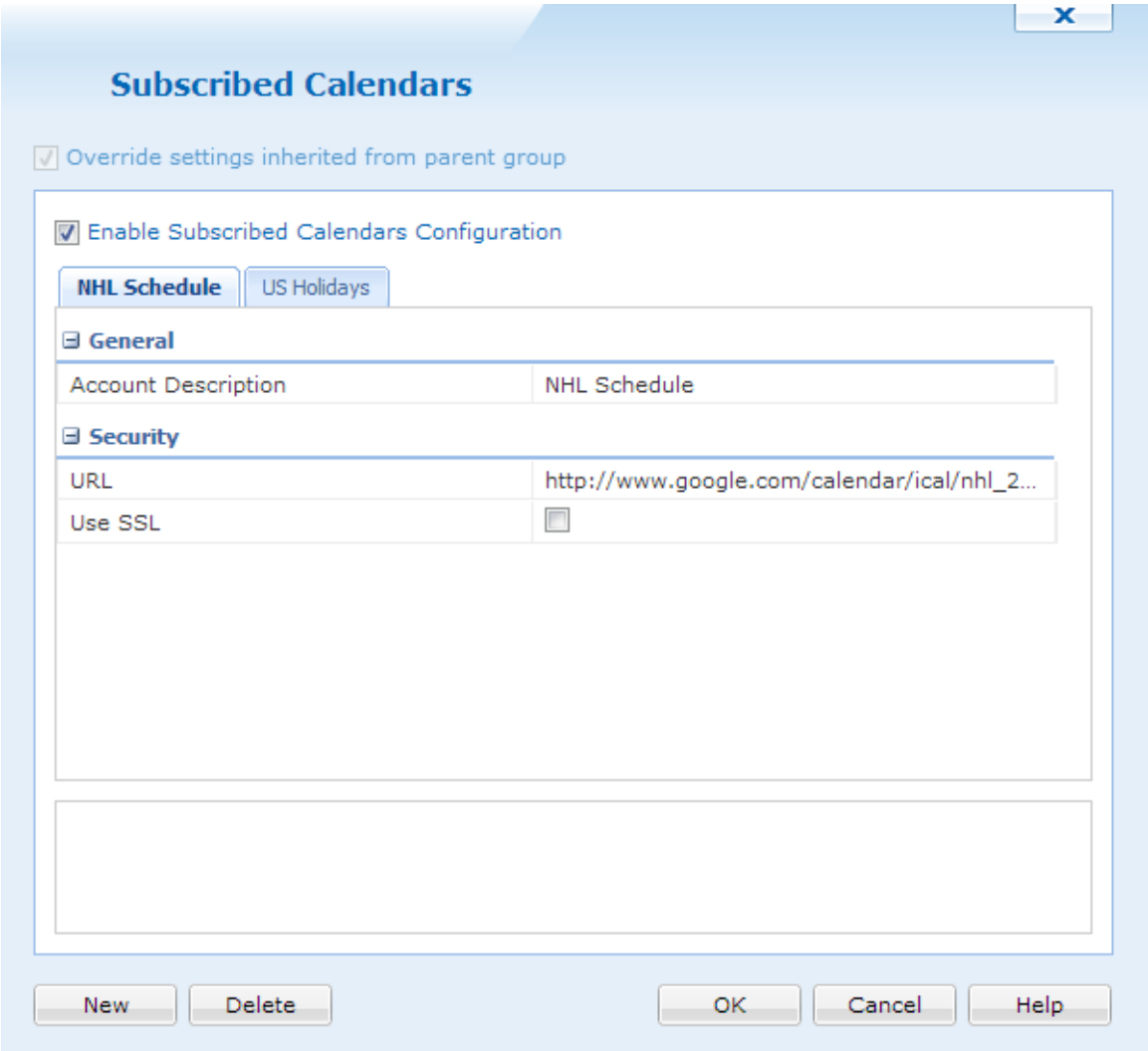
If more than one LDAP configuration is needed, just click New. If one isn't needed any more click Delete.

When all configurations are complete, click OK to save and close the window.

iOS Subscribed Calendars

MobiControl can configure the subscribed calendar section for iOS devices. Subscribed calendars add calendar entries to the device's calender app. These entries cannot be edited and can only be viewed.

To enable Subscribed Calendars for a device or group of devices, right click a device or group, and select **Device Configuration**, from there, click **Subscribed Calendars**.



Subscribed Calendars dialog box

If more than one Subscribed Calendar is needed to be configured, selecting New will create an additional entry.

Field Name	Description
Account Description	The name of the subscribed calendar.
URL	The URL for the calendar.
Hidden Network	If SSL is needed for a calendar, select this option.

EXAMPLE:

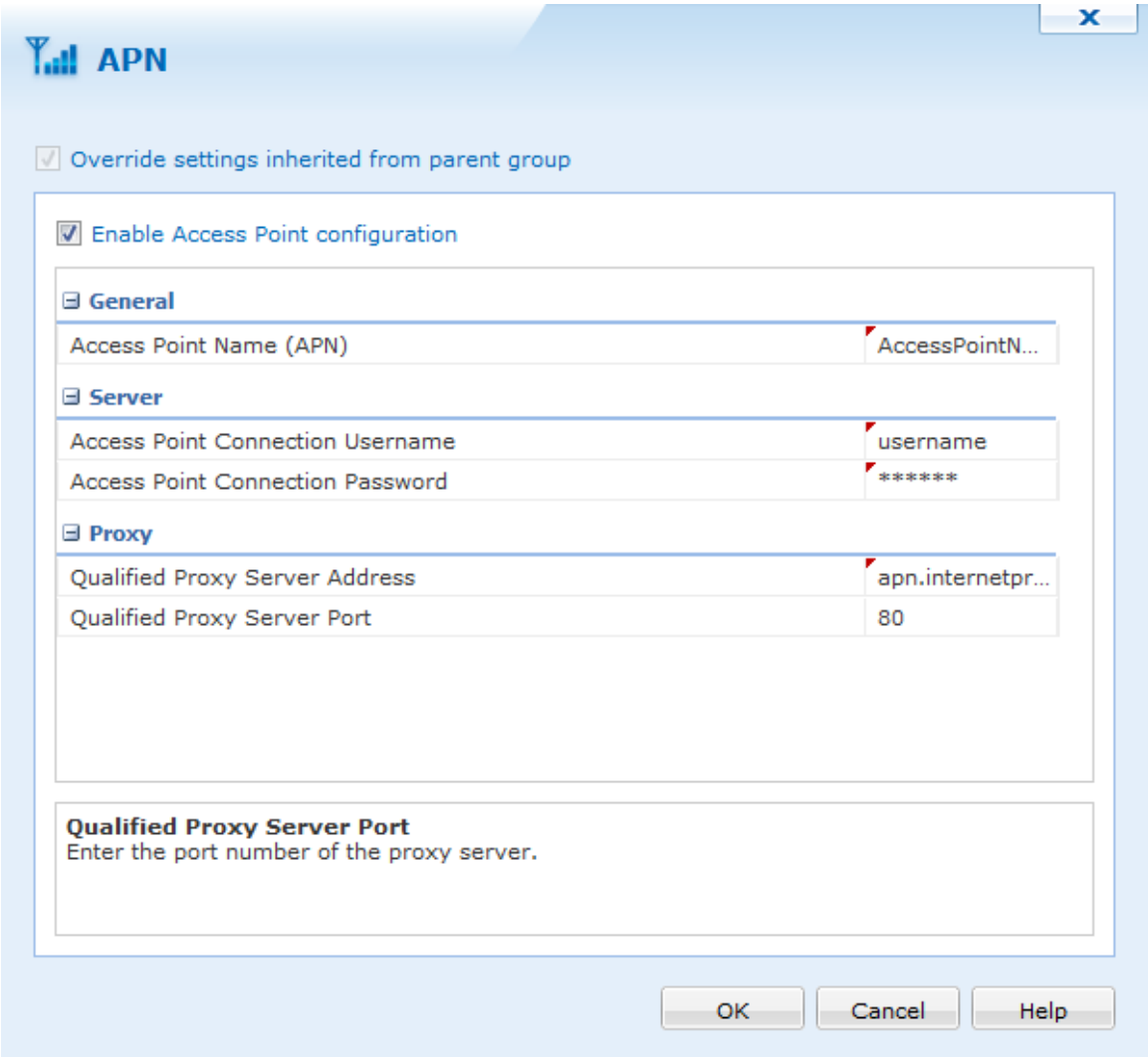
Google offers a wide range of subscribed calendars. For example, if you would like to add US holidays to all iOS devices, use this URL: http://www.google.com/calendar/ical/en.usa%23holiday%40group.v.calendar.google.com/public/basic.ics

If a Subscribed Calendar is not needed anymore, just select Delete. After all configurations are done, click OK.

iOS APN Configuration

If a cellular company has given specific APN connection settings to allow devices to connect to the Internet, MobiControl allows us to centrally manage these settings through a special configuration.

To access this configuration, right click a device (or group) and click **Device Configuration**. When the Device Configuration panel appears, click **APN** under Connectivity.



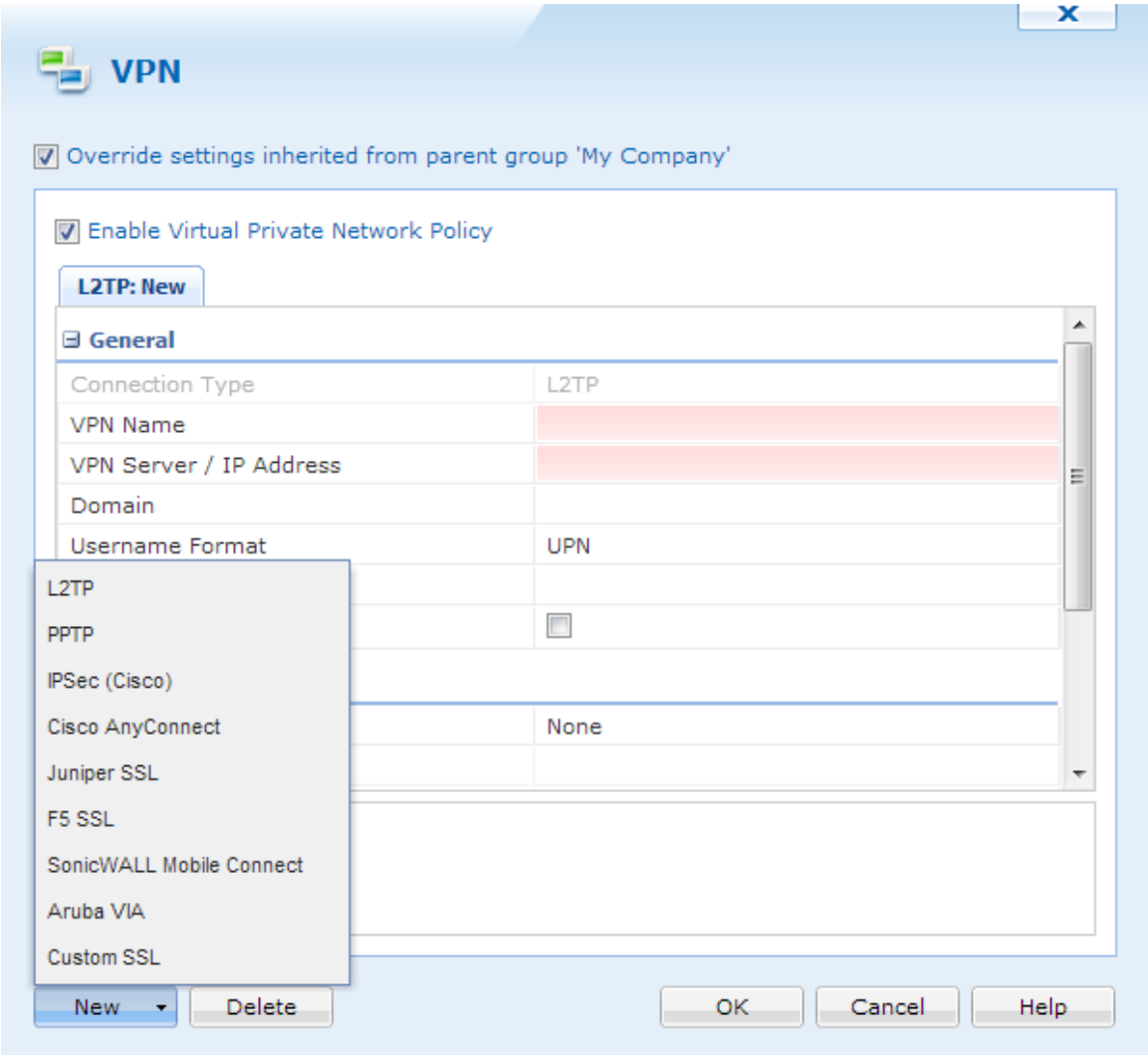
Configure APN dialog box

Item	Description
Access Point Name	Enter the SSID if the Wireless network the device connects to
APN Connection Username	Select the Network Security type used by the Wireless Access Point
APN Connection Password	Enter the Password required in order to connect to the Wireless Network
Qualified Proxy Server Address	Enter the Server Address for the APN connection
Qualified Proxy Server port	Enter the Server port for the APN connection

iOS Connection Security

MobiControl's iOS VPN Configuration allows us to set up the VPN settings for devices. We are able to set up VPN for L2TP, PPTP, IPSec, Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connection, Aruba VIA, or a Custom SSL connection.

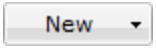
To access the VPN configuration page, right click a group or device and select **Device Configuration**. When the Device Configuration dialog appears, click **VPN**



iOS VPN dialog box

IMPORTANT:

VPN settings are only available for devices with iOS 5 or higher.

To create a new VPN connection click 

and select the desired connection type.

Below we will go through each of the configurations for iOS VPN Configuration. Click the titles to reveal the information:

- **L2TP**
- **PPTP**
- **IPSec (Cisco)**
- **Cisco AnyConnect**
- **Juniper SSL**
- **F5 SSL**
- **SonicWALL Mobile Connect**
- **Aruba VIA**
- **Custom SSL**

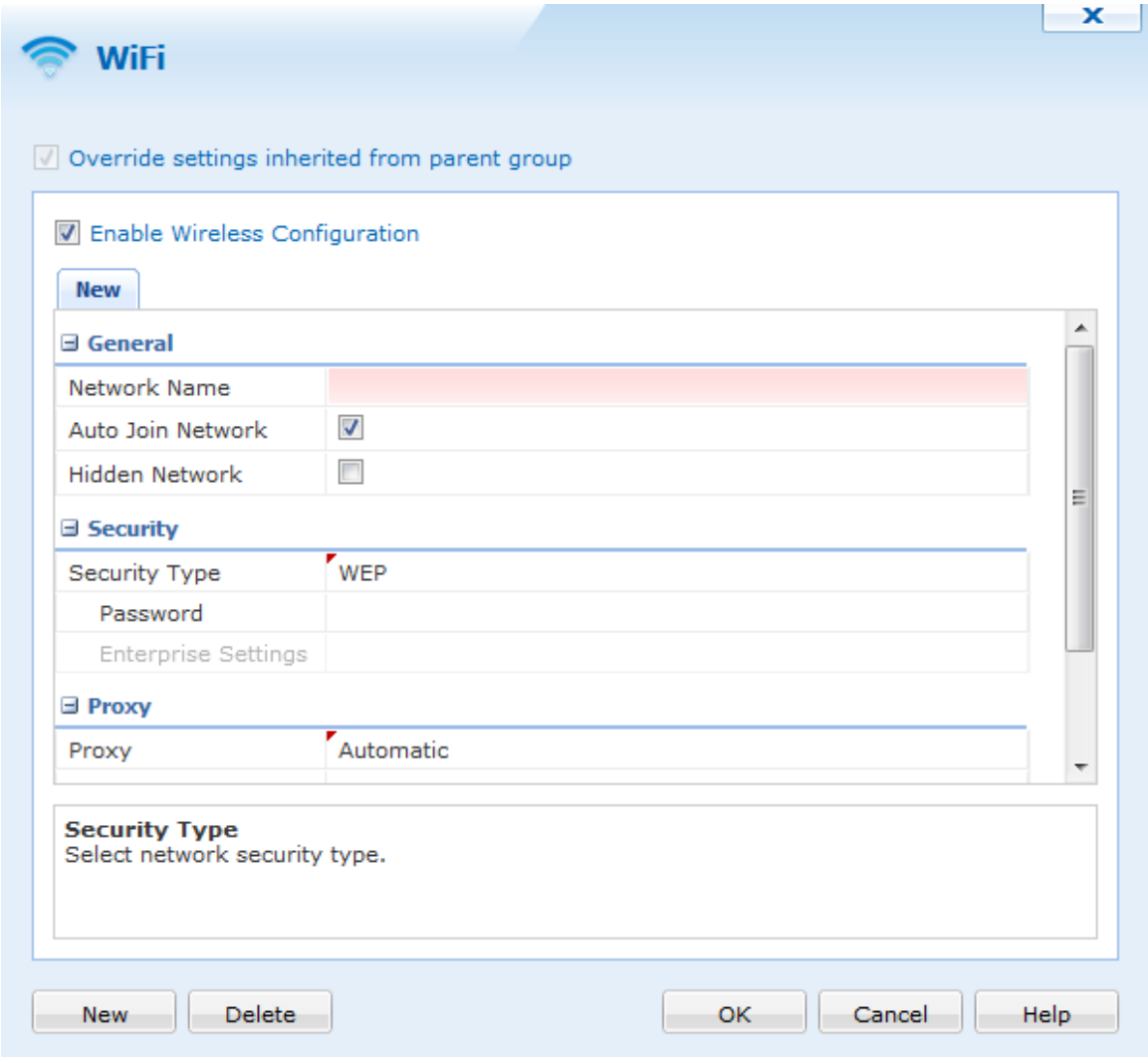
If a VPN connection is not needed any more, click Delete.

After all settings have been configured, click OK to save and close.

 iOS WiFi

---

With MobiControl's WiFi policy, we are able to configure the WiFi connection on iOS devices.
This offers a way to safely and quickly configure the wireless connection on one or hundreds of devices.
To enable the Wireless Policy for a device or group of devices, right click a device or group, and select **Device Configuration**, from there, click **WiFi**.



WiFi Policy dialog box

If more than one network is needed to be configured, selecting New will create an additional profile.

Field Name	Description
Network Name	The name of the network which the device should connect to. Also is the name of the Wireless Policy.
Auto Join Network	Selecting this will enable the device to auto connect to this network.
Hidden Network	Select whether the network is hidden or not.
Security Type	The security protocol currently being used on the network. We can select WEP, WPA/WPA2, Any (Personal), WEP Enterprise, WPA/WPA2 Enterprise, Any (Enterprise) or None.
Password	The password to connect to the network.
Enterprise Settings	If 802.1x Enterprise is selected as the security type, clicking the text box will bring up the Enterprise settings page. See below for more information on the Enterprise settings panel.
Proxy	MobiControl offers proxies to be automatically configured, or to manually configure them. If automatic is selected, then enter a URL in the URL field. If manual is set, then we must enter data in the Proxy Server, Username, and Password fields.
URL	If automatic is et as the proxy setting, enter the URL of the proxy here.
Proxy Server	If manual is selected, enter the name of the proxy server here.
Username	If manual is selected, enter the username for authentication here.
Password	If manual is selected, enter the password here.

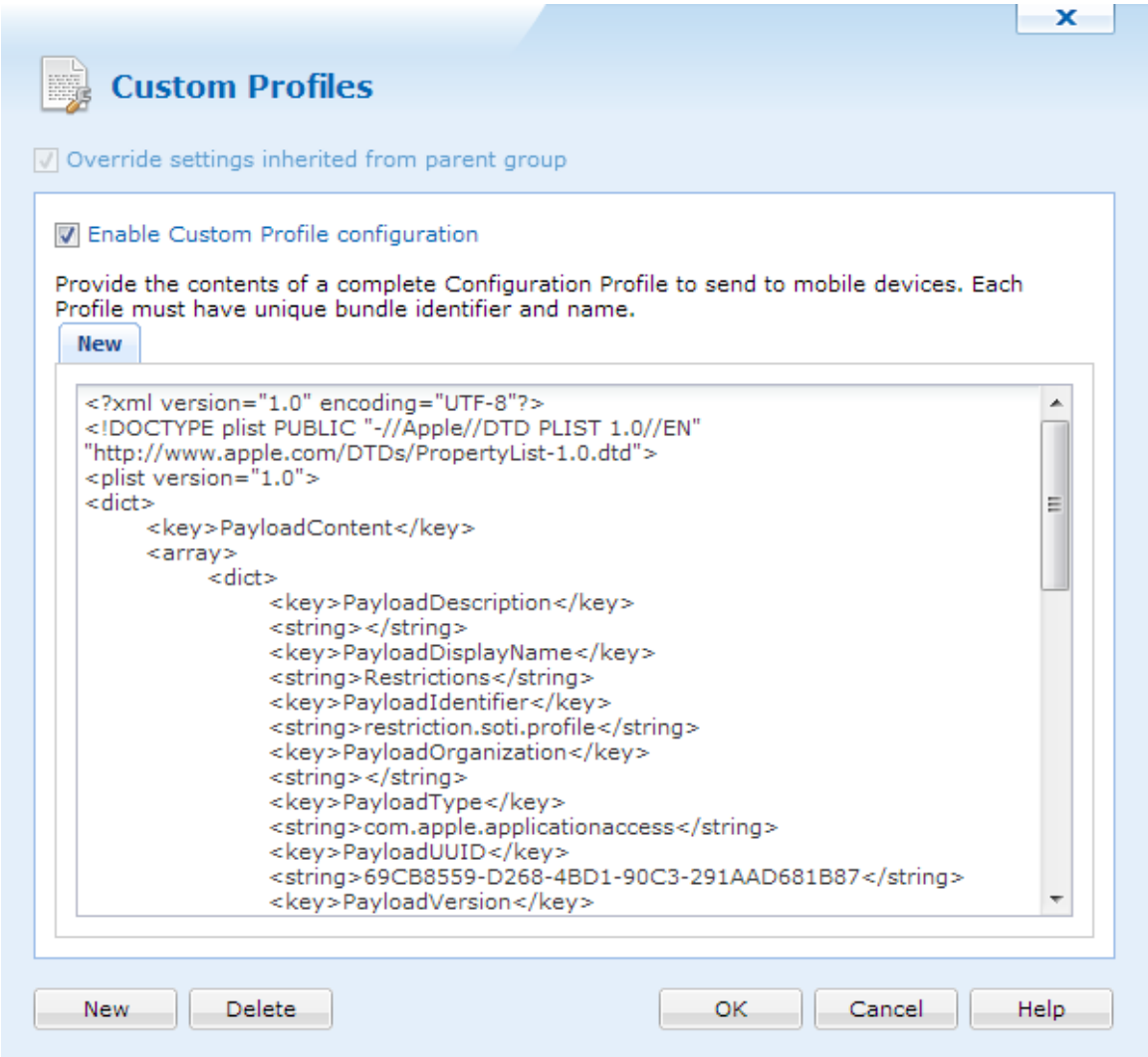
Enterprise Settings

If a wireless configuration is not needed anymore, just select Delete. After all configurations are done, click OK.

iOS Custom Profiles

Custom Profiles allows us to configure features of iOS devices through the use of XML files. If a newer version of iOS has new MDM features that are not yet implemented with MobiControl, we can create a custom profile that uses that feature and send it to devices.

To enable Custom Profiles for a device or group of devices, right click a device or group, and select **Device Configuration**, from there, click **Custom Profiles**.



Custom Profiles dialog box

If more than one Custom Profile is needed, clicking New will create an additional profile.

If a Custom Profile is not needed anymore, just select Delete. After all configurations are done, click OK.

NOTE:

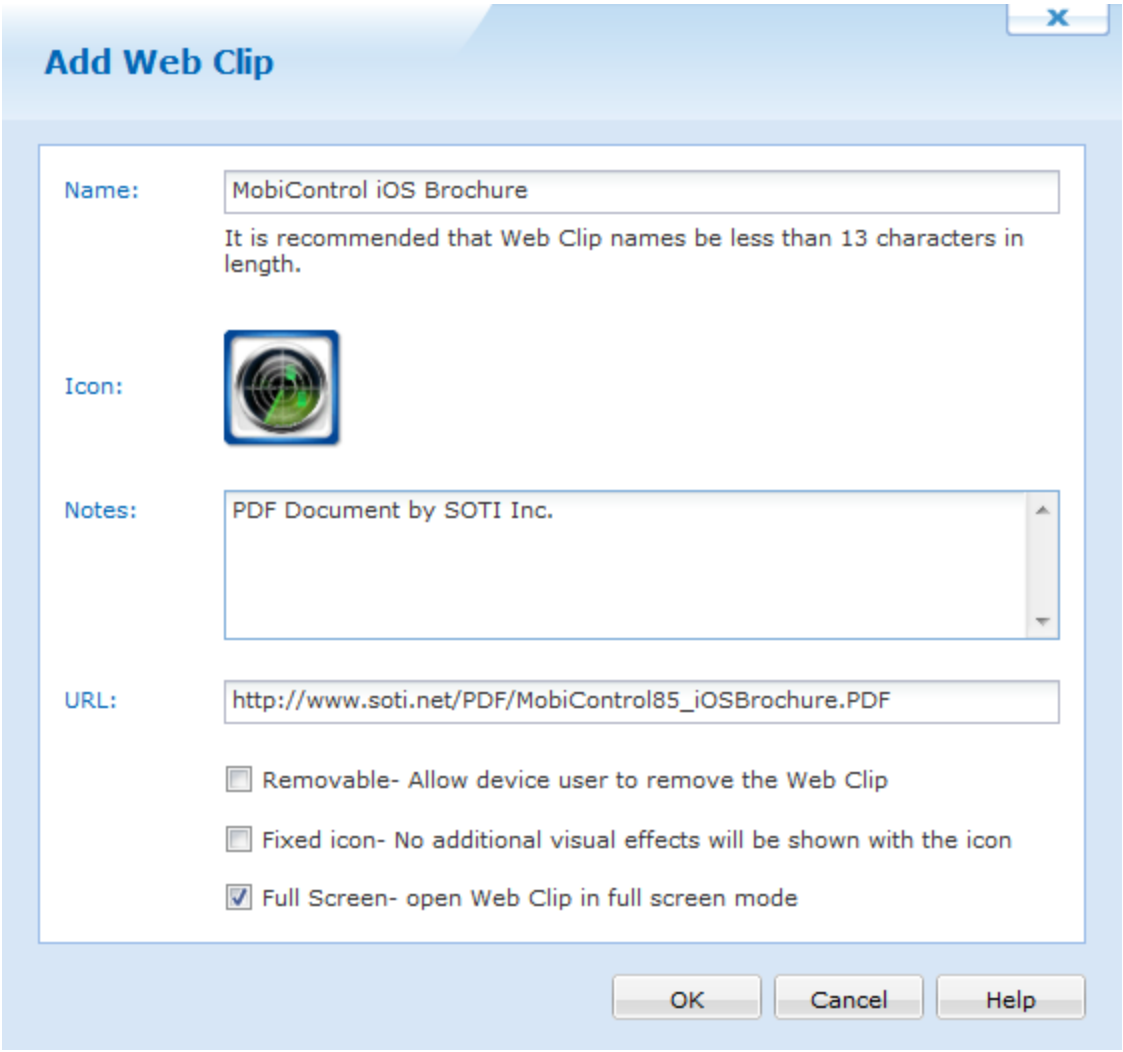
For assistance with custom profiles, please email us at support@soti.net or by phone at (905) 624-9828.

Web Clip

Web Clips are essentially shortcuts to URL's. Files and websites are often the target URL's.

The Web Clips are stored on the device, and points directly to the source. For example, a PDF hosted on a company website. A Web Clip would point to the source address.

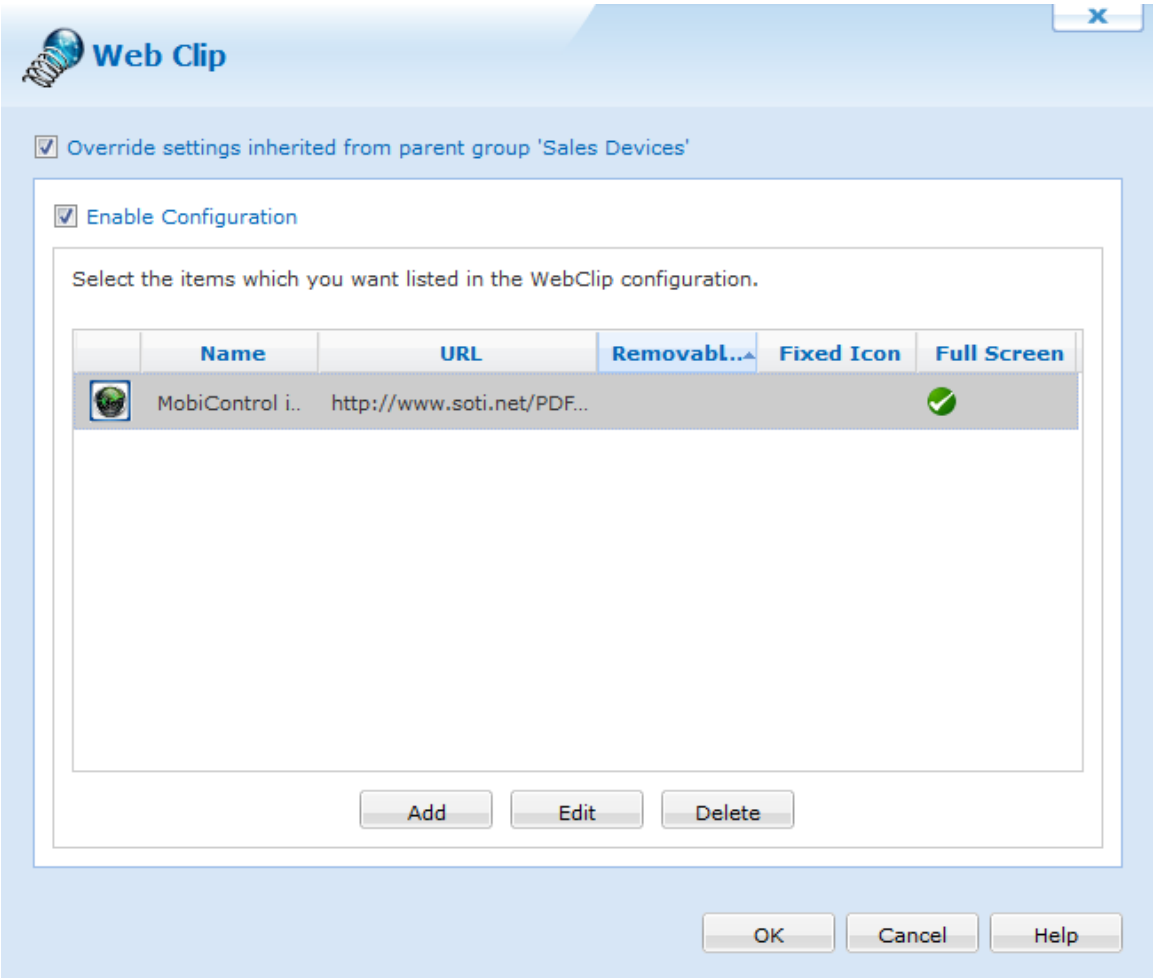
To add a new Web Clip, right click on the iOS device in the Web Console and select Configure>Web Clip.



Adding a new Web Clip

Item	Description
Name	Name for the Web Clip as it will appear on the device
Icon	Icon for the Web Clip as it will appear on the device
Notes	Description of the Web Clip
URL	URL path to the Web Clip
Removable	Allows the device user to remove the Web Clip
Fixed Icon	No additional visual effects will be shown with the icon
Full Screen	Open Web Clip in full screen mode

To Manage Web Clips that have been created already, simply right click on a device or group of devices that have a web clip setup already.



Web Clip Dialog

Advanced Settings for iOS Devices

There are five main aspects to iOS Advanced Settings. Each of these settings can be configured for a single device or applied at the device group level thereby configuring a set of devices. When the devices are moved from one device group to another in the device tree, the settings for the new device group are applied automatically to the devices.

Custom Attributes

Custom Attributes allows us to create custom information that appears on the information panel on the right hand side of the web console. Please see the "Custom Attributes" topic on page 1343 for more information.

Deployment Server Priority

This option allows you to specify the Deployment Server preferences for the devices. When a device is configured with more than one Deployment Server, it will try to connect to highest priority one first and if this server is not accessible, then it will try to connect to the next server available. Please see the "iOS Deployment Server Priority" topic on page 1009.

Remote View Settings

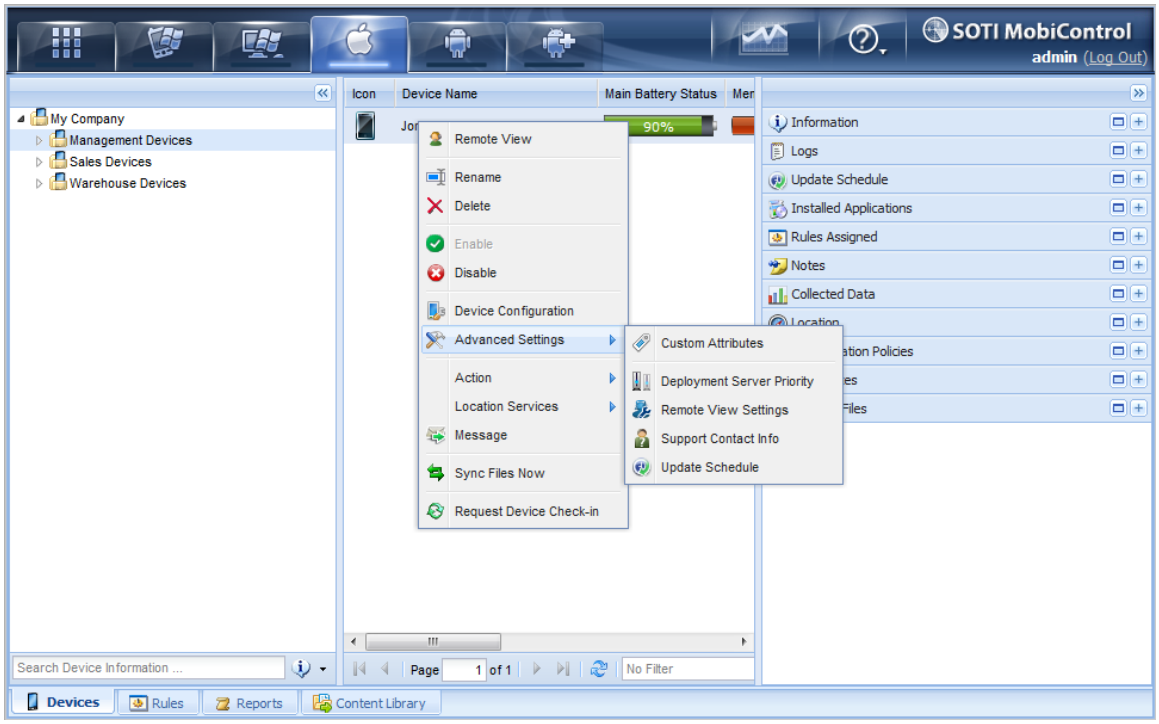
Select a device skin to display in the MobiControl Remote, and choose the connection profile to use when remote controlling the device. This allows for customized remote control settings, optimised for different types of connections, for instance, high-speed Wi-Fi or low-speed cellular connections). Please see the "iOS Remote Control Settings" topic on page 1010.

Support Contacts Info

If users call support for their mobile device needs, configuring this option allows them to find the contact information reliably. Since this information is set centrally all information is updated once it's changed. Please see the "iOS Support Contacts Info" topic on page 1011 for more information.

Device Update Schedule

Adjust the interval at which the mobile devices contact the Deployment Server for new updates, configuration changes and packages. Please see the "iOS Device Update Schedule" topic on page 1012.



Device Configuration Menu options

Custom Attributes

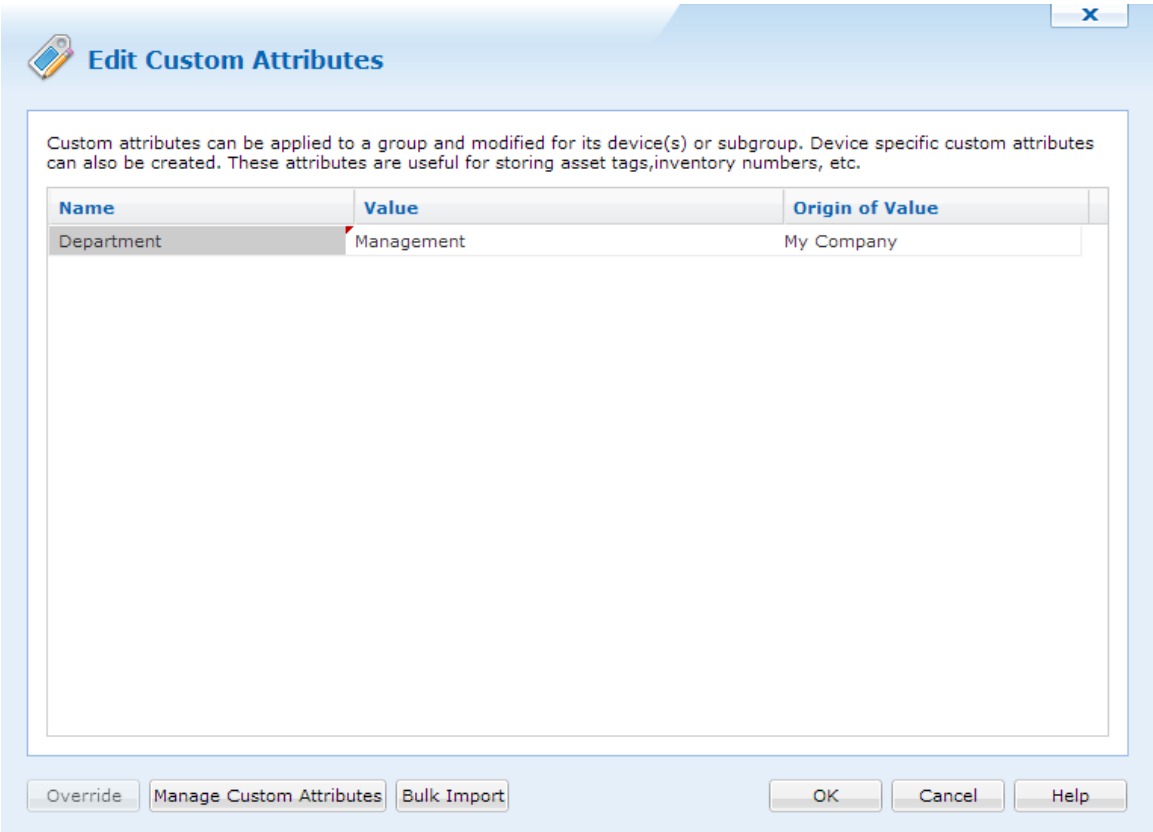
Custom Attributes allows us to create attributes to show in the information panel with our own data. This offers custom organization and labelling. For example, we can create a department attribute and put a different department for each device or device group.

Custom Attributes can also be propagated to devices so that they can be used in other applications and information.

NOTE:

Custom Attributes are available for all device types.

To set up Custom Attributes, right click a device or device group, go to Advance and click **Custom Attributes**.



Custom Attributes panel

The Custom Attributes panel has 3 columns: name, value and origin of value.

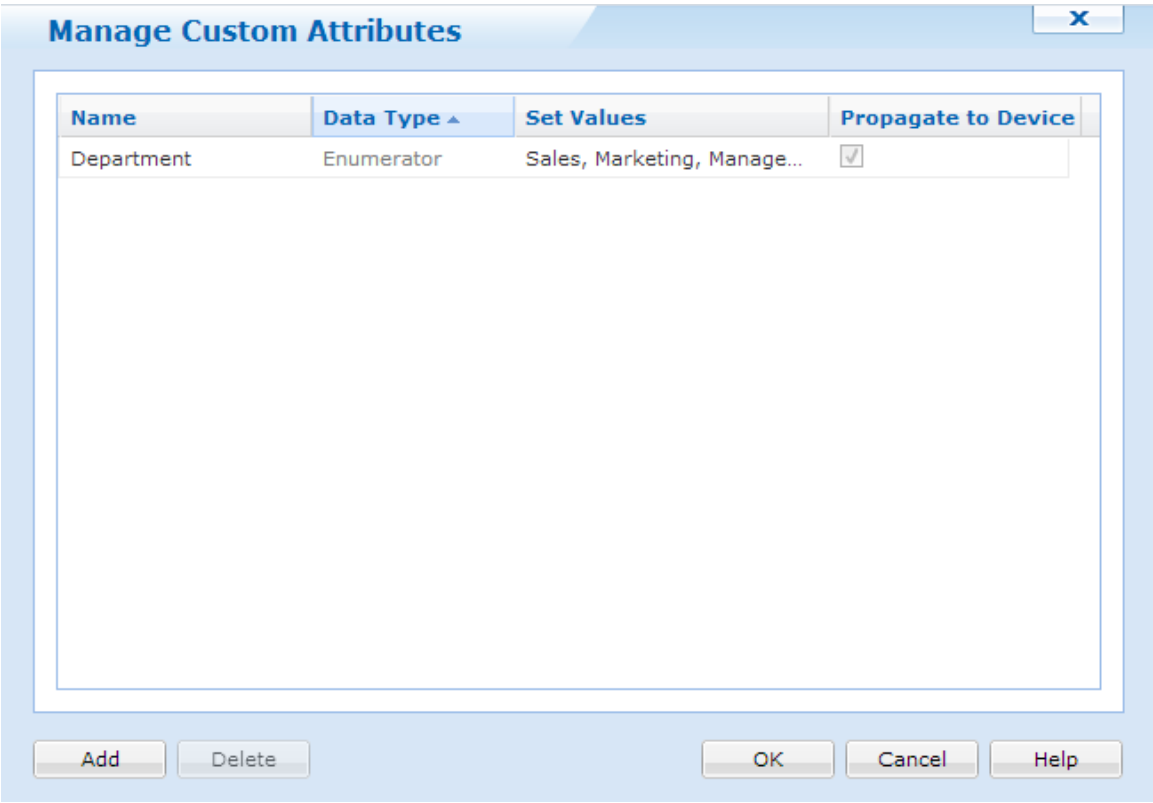
The name column shows the name of the Custom Attribute that will be shown in the info panel. Value contains the actual attribute for this field. Origin of value shows us where this field came from. For example, if Custom Attributes were set at the root level of the device tree, the origin of value will show the root level device group.

Clicking **Override** will change the origin of value to that where the device resides. This is useful if attributes change for each device. The Override button will change to **Remote Override** if we want to inherit the value from a parent group.

To create new attributes, click **Manage Custom Attributes**.

Manage Custom Attributes

When Manage Custom Attributes is clicked we a new dialog box appears. Here we will be able to create the Custom Attributes.



Manage Custom Attributes

Click  to add a new attribute.

When Add is clicked, a new row will appear. Clicking the field under name will allow us to name this attribute.

Data Types

There are 5 available data types to have for Custom Attributes:

- Text
- Numeric
- Date
- Boolean
- Enumerator

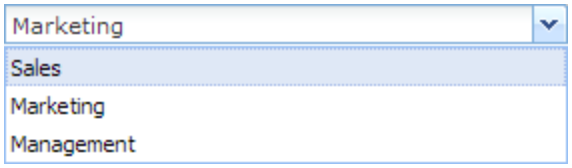
Text will allow us to create values with **letters and numbers**.

Numeric will allow us to create values with **only numbers**.

Date will allow us to set dates.

Boolean will create a checkbox for **yes or no / true or false**.

If we select enumerator, this allows us to create a drop down list when we set the attribute. To create the list, click the field in **Set Values** column. Here we can type the items we want in the drop down list. **Each value must be separated with a comma (,)**. For example, if we want to create a department attribute, we can have Sales, Marketing, Management. When we set this attribute, we will be presented with the drop down.



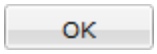
Enumerator Example

Propagate to Device

Checking this off will have MobiControl create the Custom Attributes in the pdb.ini file on the device. Applications can then read this file and pull the Custom Attribute value.

Bulk Import

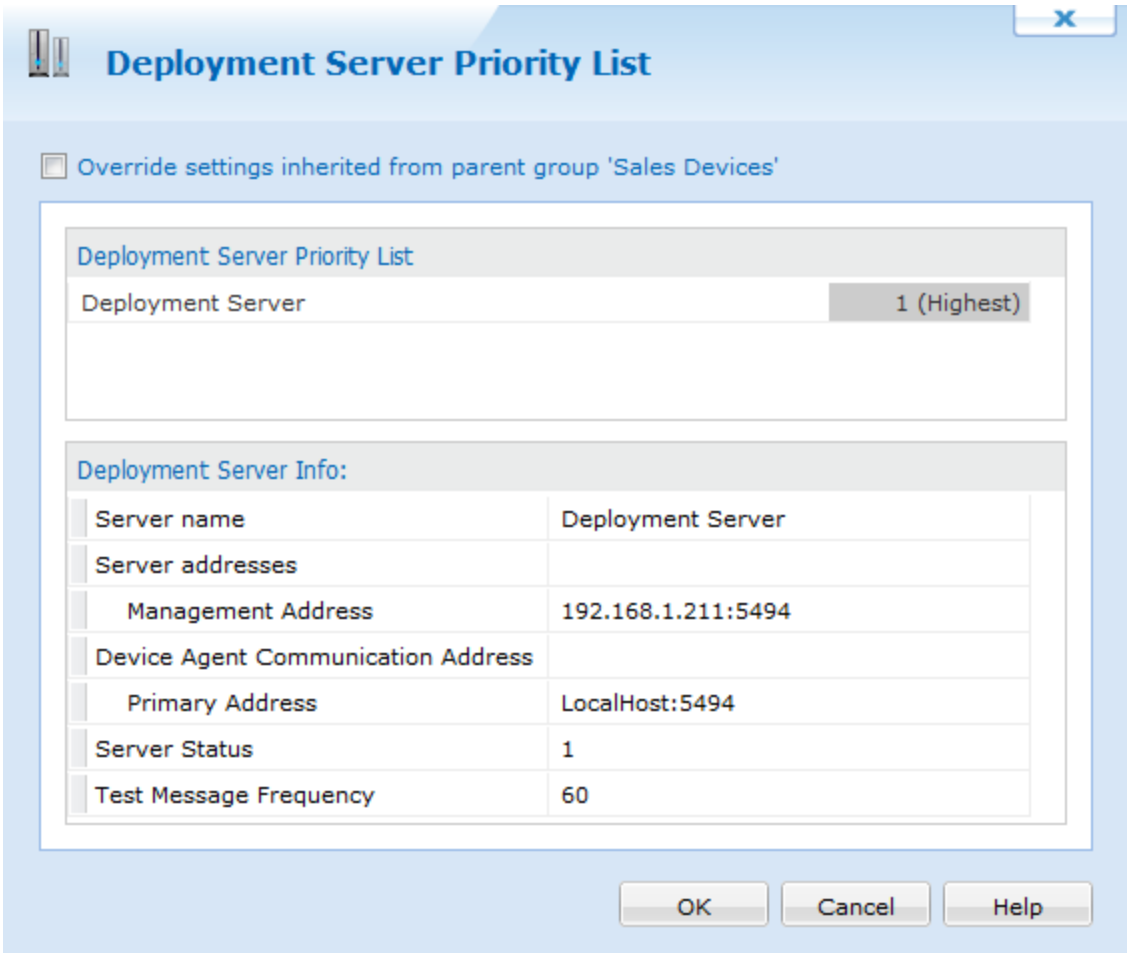
If there is a large amount of Custom Attributes to be inserted, we can do a bulk import so that everything is added at once.

Once everything is set, click 

to save and close the Custom Attributes.

iOS Deployment Server Priority

The **Deployment Server Priority List** dialog box allows you to specify the Deployment Server preferences for the devices. Priority one is the highest and five is the lowest. When a device is configured with more than one Deployment Server, it will try to connect to highest priority one first. If this server is not accessible, then it will try to connect to the next server available.



Deployment Server Priority List dialog box

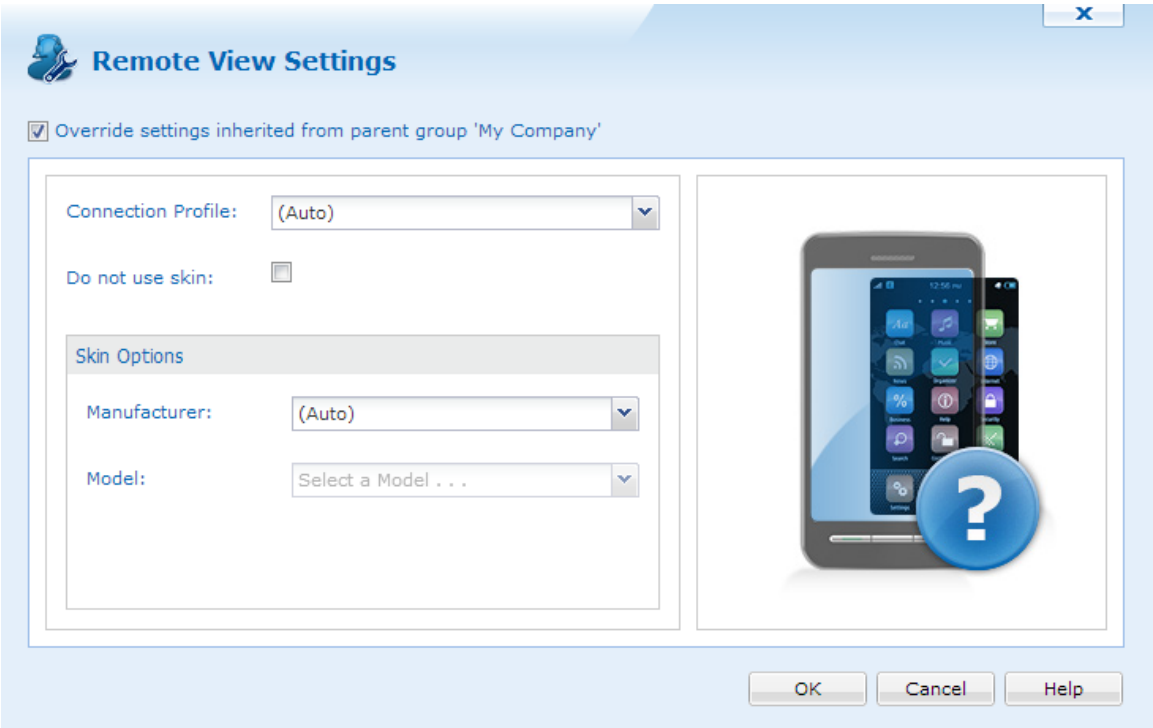
Multiple servers may be assigned the same priority level to establish a pool of Deployment Servers to balance the load of a large number of devices.

If you select "Not used," the selected devices will not connect to that Deployment Server.

Deployment Server priority is only applicable when you have installed multiple Deployment Servers using the same site name.

iOS Remote View Settings

In the **Remote Control Settings** dialog box, it's possible to select a device skins and connection profiles. A skin is an image of the body of your mobile device, which mimics the physical device on your desktop screen. Displaying your device in a skin gives you access to most of the physical buttons of the device. It can be useful in training or presentations. Skins are automatically configured based on the device type.



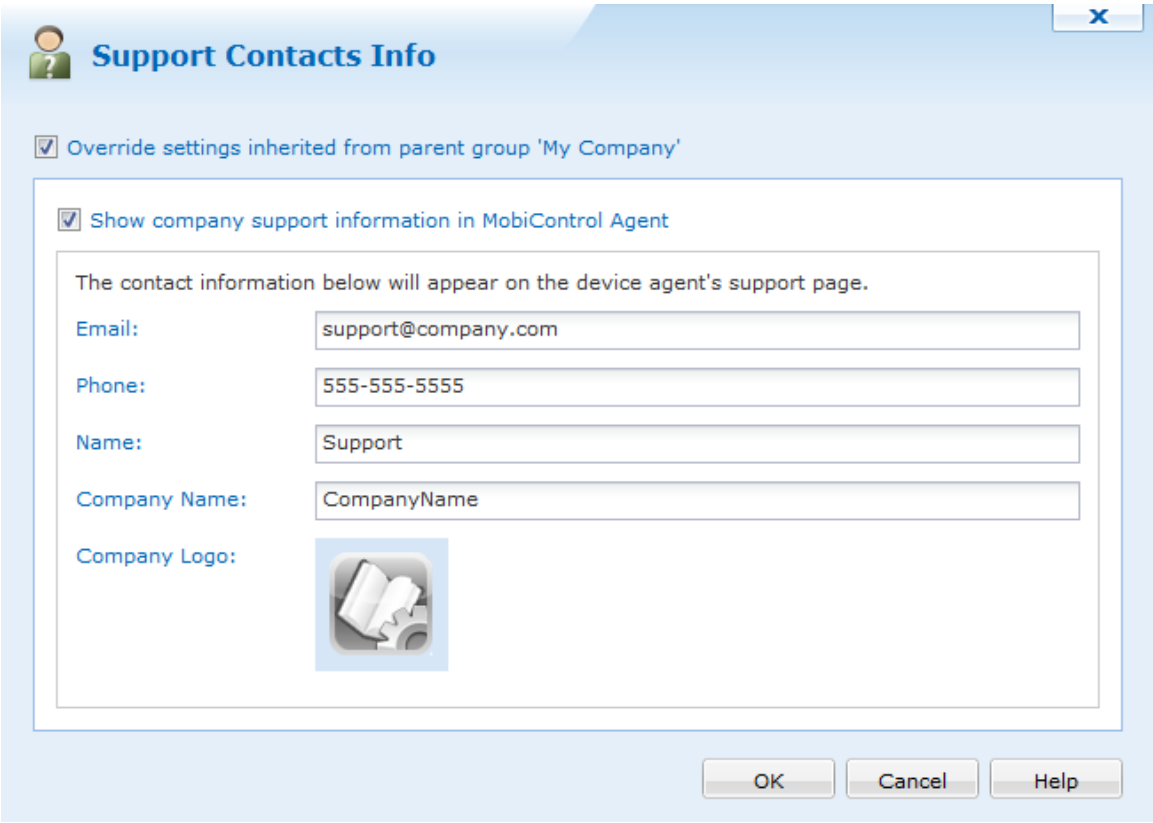
Remote Control Settings dialog box

The following table describes fields in the **Remote Control Settings** dialog box.

Field Name	Description
Connection Profile	Allows you to select the appropriate connection profile that you wish to use for your remote session. Auto is the default option and will use the inherited option.
Do not Use Skin	Checking this off will remove the skin from the device when remote controlling it.
Manufacturer	Select the manufacturer and model of your device to have its skin be displayed in a remote control session. At this time Apple is the only Manufacturer of iOS devices.
Model	The model of the device is determined by the Manufacturer. Select the model of the device from the list.

iOS Support Contacts Info

The Support Contacts Info panel allows us to set contact information when a user opens up the MobiControl agent on their device. Information that we are able to configure are Email, Phone, Name, Company name and a company logo.



Support Contacts Info dialog box

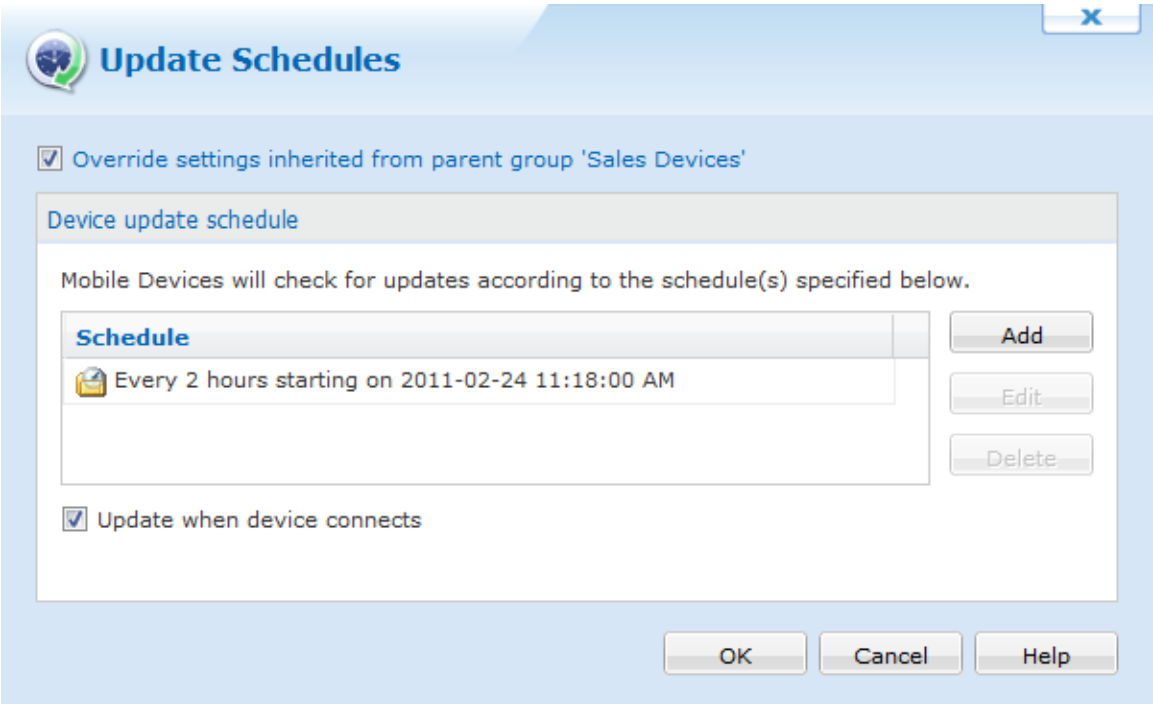
When each of the fields are set and OK is pressed, this information will then be sent down to the devices where this was configured on. When a user opens up their MobiControl agent and goes to the support info tab, they will be able to see the appropriate information.

iOS Update Schedule

The device update schedule specifies when the device(s) should query the Deployment Server(s) for updates. Updates may include the addition, update, or removal of packages and modifications to device settings.

If the Deployment Server determines there are pending updates for the device, it immediately sends them to the device. The device also sends the Deployment Server a summary of its installed packages and settings. If the Deployment Server identifies an inconsistency, such as a previously-installed package that is missing on the device, the Deployment Server will re-install the package.

The initial device update schedule is specified by the add devices rule used to add the device(s) to the system. You may edit the schedule for an individual device or a group of devices that have been added to the system by selecting the target device or group in the device tree view in the main console window and selecting **Update Schedules** from the **Configure Device(s)** sub-menu.

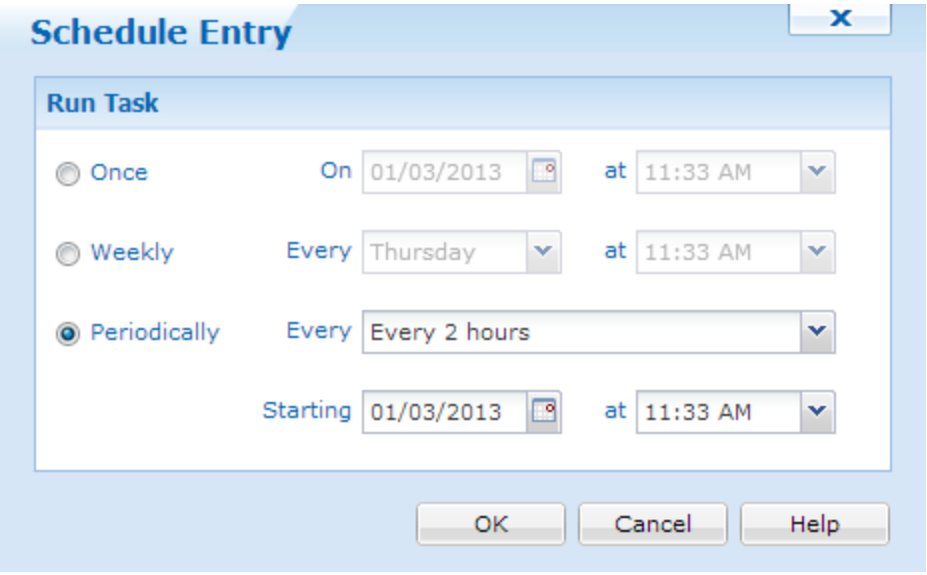


Device Update Schedules dialog box

The following table describes the **Device Update Schedules** dialog box:

Field Name	Description
Add	Select **Add** to specify additional update intervals. The **Schedule Entry** dialog box will be displayed. **EXAMPLE:** To sync a device twice a week, Monday at 06:00 and Friday at 19:00, create two weekly schedule entries.
Edit	Select **Edit** to modify an existing schedule entry. The **Schedule Entry** dialog box will be displayed.
Delete	Select **Delete** to permanently remove an update schedule entry from the dialog box.
Update when device connects	Select this check box to have the device(s) check for updates whenever they connect to a Deployment Server, that is, at every transition from offline to online. If this check box is not selected, the device(s) will only check for updates according to the schedule defined above.

Schedule Entry



Schedule Entry dialog box

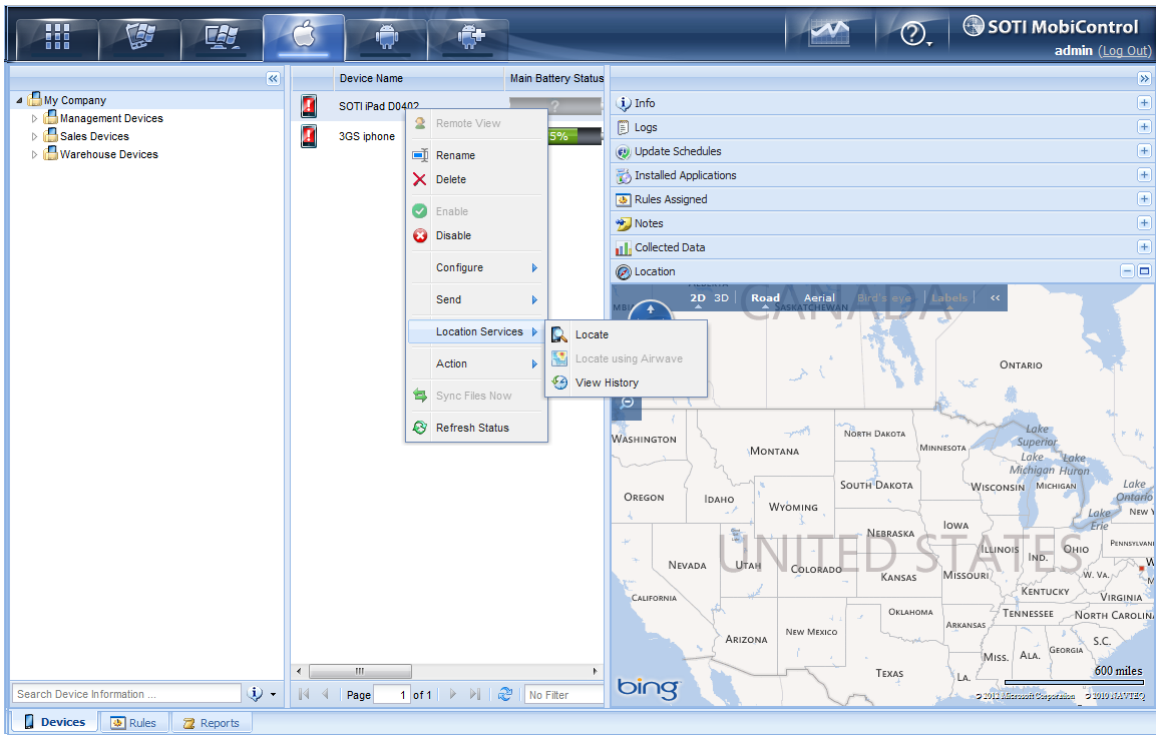
The **Schedule Entry** dialog box allows you to specify schedule entries as one-time or periodic events.

Field Name	Description
Once	The device will check for updates once at the specified date and time.
Weekly	The device will check for updates once a week, on a specific day at a specific time.
Periodically	The device will check for updates periodically, at the specified interval from the set start date and time.

iOS Location Services

MobiControl's Location Services provides the ability to locate and track mobile devices that are equipped with a GPS receiver that is internal or external to the unit. In order to locate a device, the GPS must be enabled and correctly configured on your device. The GPS determines the current location based on its position relative to orbiting satellites. In order for this to happen, the device requires a clear view of the sky. Determining location may not be possible if the device is inside buildings or has an obstructed view of the sky.

You can activate Location Services for a device in MobiControl by right- clicking on a device and selecting the **Location Services** option from the menu. The first time you select an option from the Location Services menu for a device, it will automatically use the next available license. If there are no more licenses available, you will be notified to contact SOTI for information on acquiring additional licenses for Location Services.



iOS Location Services

Please See the "Contact Us" page to contact us for more details on acquiring additional licensing.

NOTES:

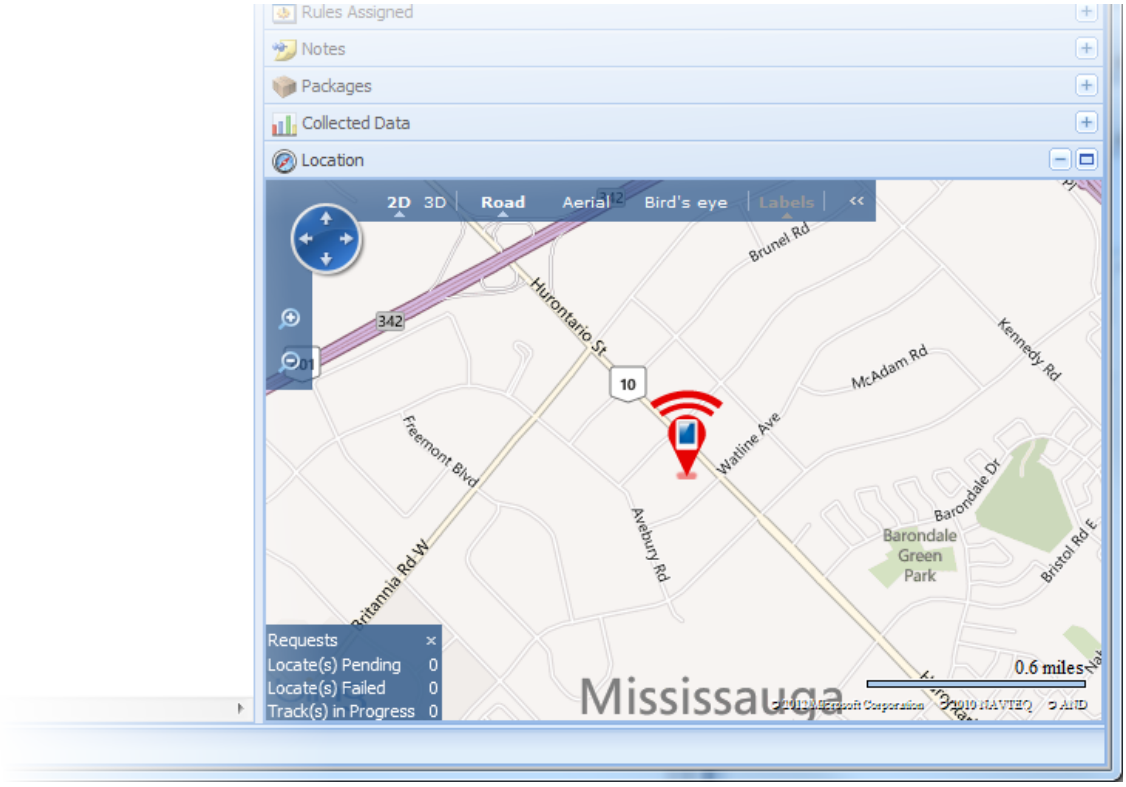
- When using Location Services in MobiControl to track devices, Internet Explorer 7 or higher is required.
- The Current Format for Regional and Language Options on your PC MUST be compatible with Bing Maps. Click here for a list of supported Bing Map control settings.

iOS Locate Feature

To use the Locate feature in MobiControl's Location Services, right-click on the device you wish to locate, select **Location Services,** and click **Locate.**

The locate feature will use the GPS unit associated with your mobile device to determine the current latitude and longitude of the device. These coordinates are returned to MobiControl and displayed in the Location panel using Microsoft's Virtual Earth. The coordinates plotted in the Location panel represent the exact position of the device at the time of the request. To follow the position of the device in real time, use the **Track** option under the **Location Services** menu.

You can locate the position of multiple devices at once: select the parent folder or hold the CTRL key and select all the devices you wish to locate, right-click, select **Location Services,** and click on **Locate.** In order to use the Locate feature, the device(s) must be online and communicating with the MobiControl Deployment Server. The status of the current (and completed) Locate and Track commands is displayed in the lower left hand corner of the screen.



Location Services locate user interface

Th

NOTE:

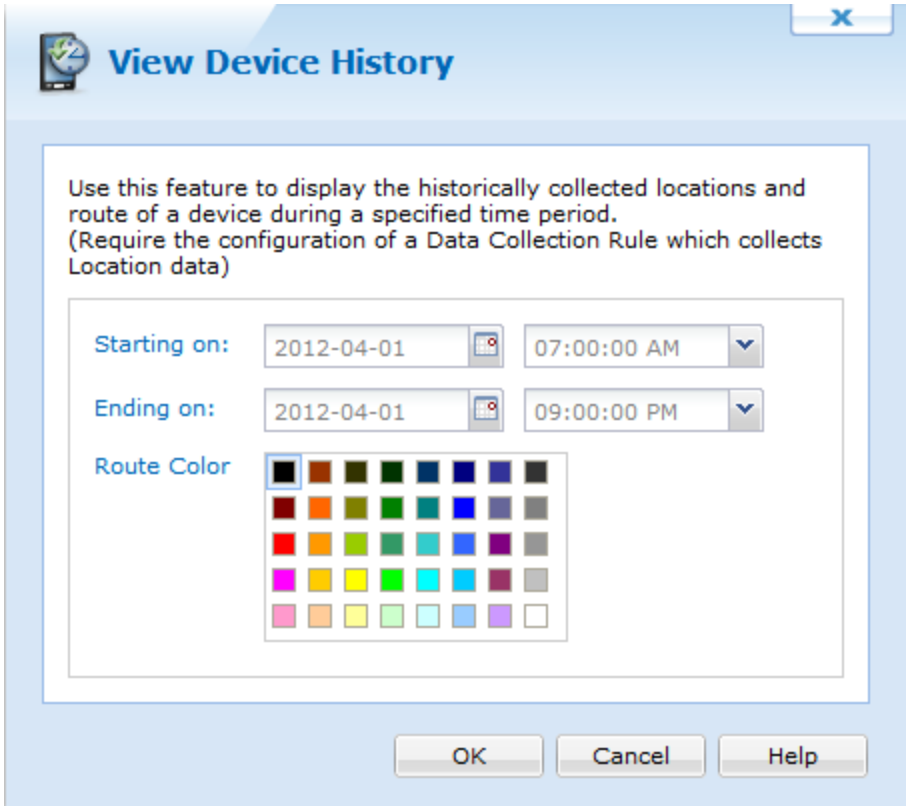
If the MobiControl Manager is behind a proxy server and you are unable to use Location Services, please run the following command through the **Start** menu then **Run**:
`netsh winhttp set proxy -server="http=<ProxyServerIP>: <Port>; https=<SSLProxyServerIP>: <Port>"` (on Windows Vista, **with no spaces between the quotation marks**.)
This command will update the WinHTTP service with the settings from Internet Explorer.

Show Tracking History

The show history feature will use the GPS unit associated with your mobile device, allowing you to view where the device has been over a given period of time. To use this feature, you need to set up a data collection rule that collects the location information from the device on a given schedule. The data will be sent back to the deployment server, or, if there is no active data connection on the device, it will be

collected and stored in a temporary file and then sent back to the server the next time the device connects. The show history feature does not require the device to be online and communicating with the MobiControl Deployment Server. You can plot information from the history that has been transmitted back to the server during the last active connection.

To use the show history feature, right-click on the device you wish to view, select **Location Services,** and click **Show History.** You will then be prompted to enter the time period for which information is desired, and the route color. Once this is filled in, click **OK** and the path will be plotted.

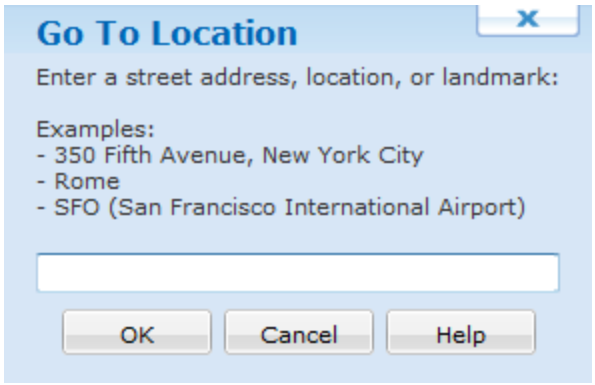


View Device History dialog box

Feature	Description
Starting On	Enter the date and time that you wish to start.
Ending On	Enter the date and time that you wish to stop.
Route Color	Select the color to be used on the map when connecting the co-ordinates.

Go To Location

Go To Location allows you to quickly centre and zoom the map to a specific location. Go To Location is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "iOS Location Services" topic on page 1014 for more information.

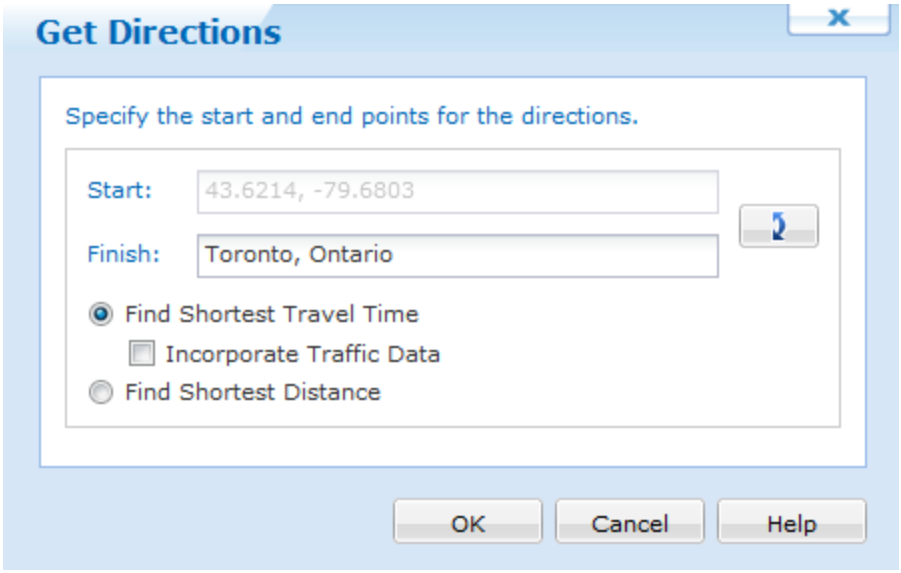


Go To Location dialog box

To use this feature, right click on the Location panel and select "Go To..." from the pop-up menu that appears to open the Go To Location window. You can then enter an address, location, landmark, or the name of an existing geofence. Once you have entered the location information, click the OK button and the map will reload centring on the information you provided. If you entered the name of an existing geofence, the map will change to the location of that geofence and display it on the screen in red.

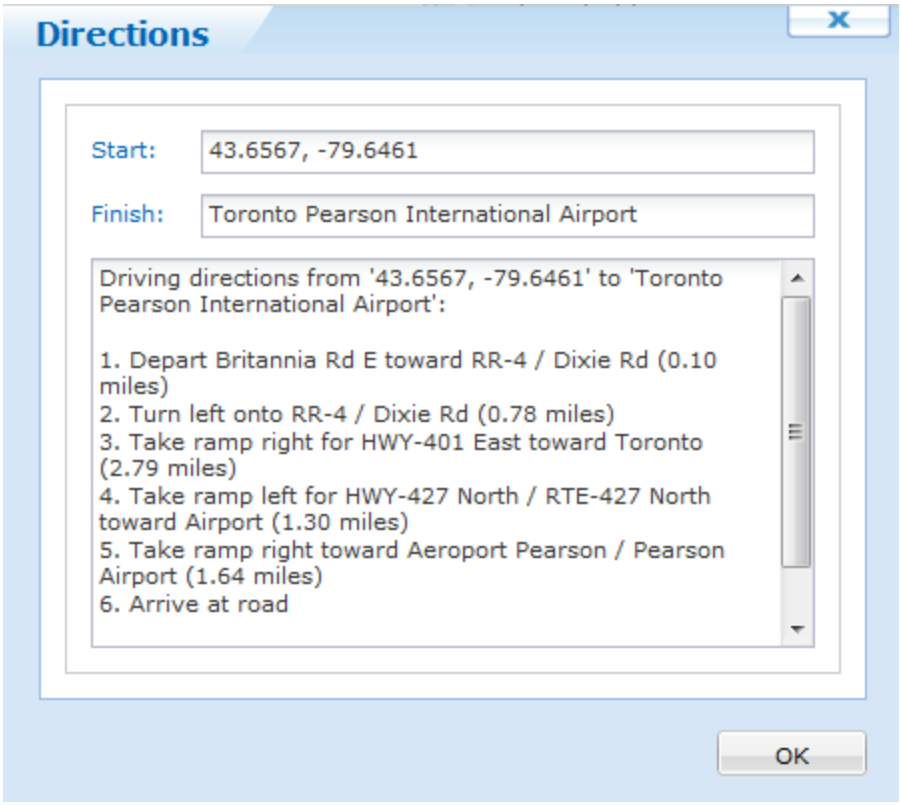
iOS Get Directions

Powered by Microsoft's Bing Maps, MobiControl's Get Directions will return turn-by-turn directions between two locations on the map. These directions can be sent directly to the device, or they can be pasted into an email and sent to a larger group of people. Get Directions is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "iOS Location Services" topic on page 1014 for more information.



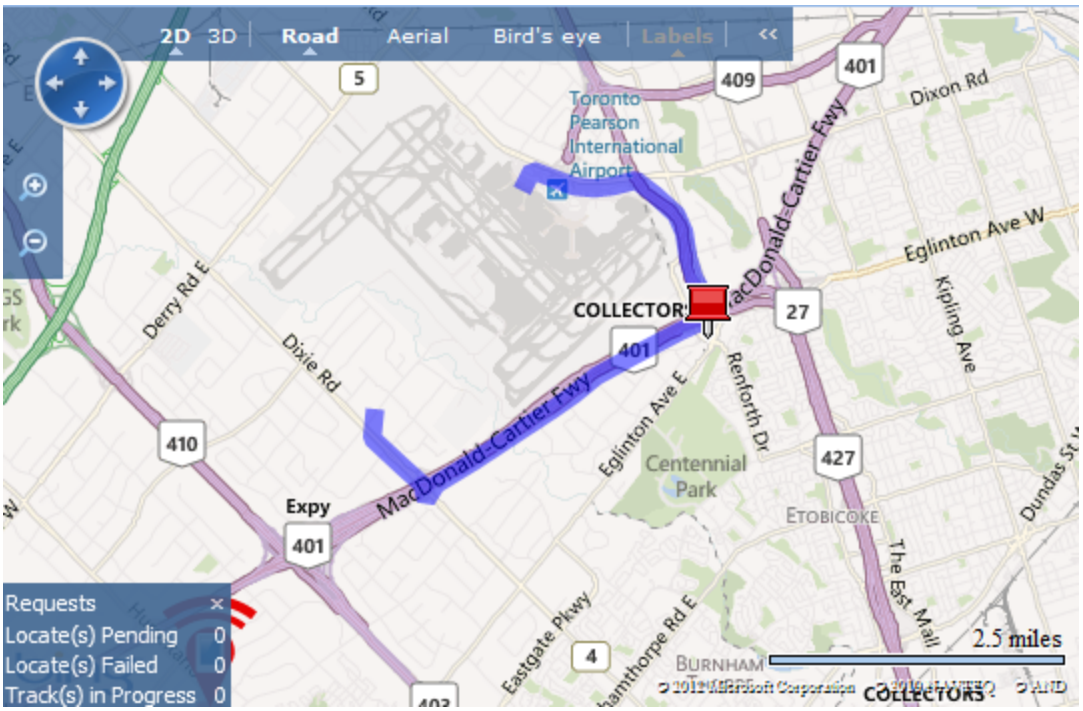
Get Directions dialog box

To use Get Directions, in the Location panel right click on any device or a point on the map and select "Get Directions" from the pop-up menu. The Get Directions dialog box will appear. Be default, the device or map location clicked on will be used as the starting point. To change this, click the double arrow button located to the left of the Start and Finish fields. You can enter GPS co-ordinates, landmarks, or an address. Directions can be optimised by selecting shortest travel time or shortest distance from the options list and press the OK button.



Driving Directions window

MobiControl will determine the turn-by-turn driving directions between the two locations you specified. The resulting directions will be displayed in the Driving Directions window. If you started by right clicking on a device, the "Send to Device" button will be enabled and you can send the instructions directly to the device. You can copy the directions from this window and paste them into an email or document or your choice.

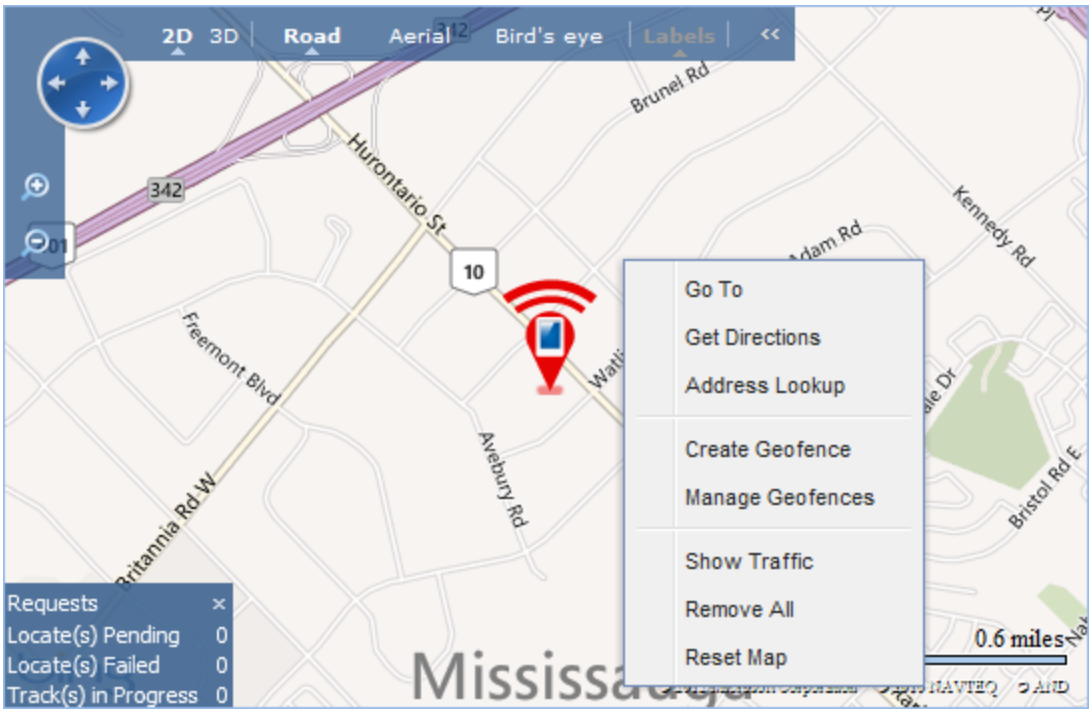


Driving directions displayed on the Map

The Location panel will reload the map to show the driving route highlighted. If the map is in Bird's Eye view, the highlight will not be displayed. Both Aerial and Road view will display the highlighted route.

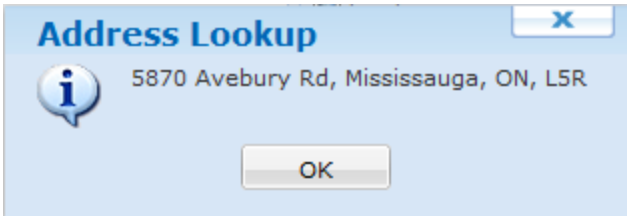
iOS Address Lookup

The Address Lookup feature allows you to determine the address of a specific point on the map displayed on the Location panel. Address Lookup is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "iOS Location Services" topic on page 1014 for more information.



Location panel right click menu with Address Lookup option

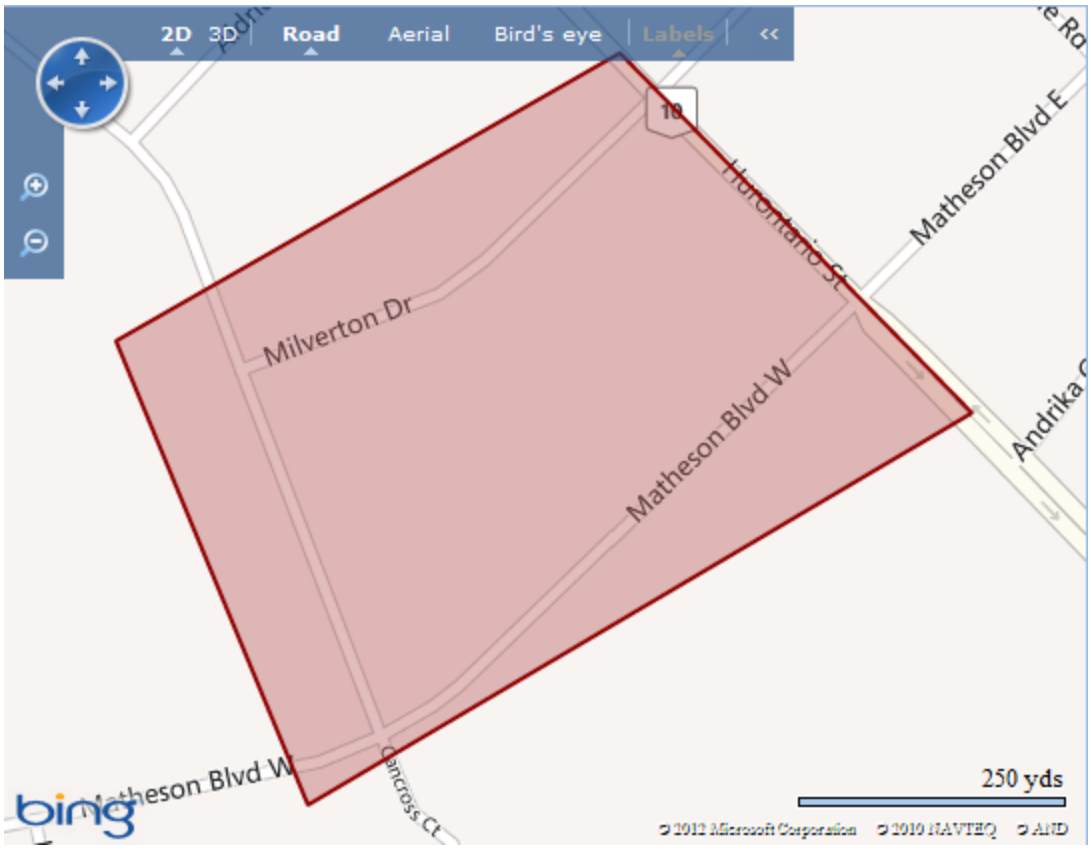
To use the Address Lookup feature, right click anywhere on the map in the Location panel and select the Address Lookup option from the menu that appears. The address of that location will be displayed in a new information window.



Address Lookup window

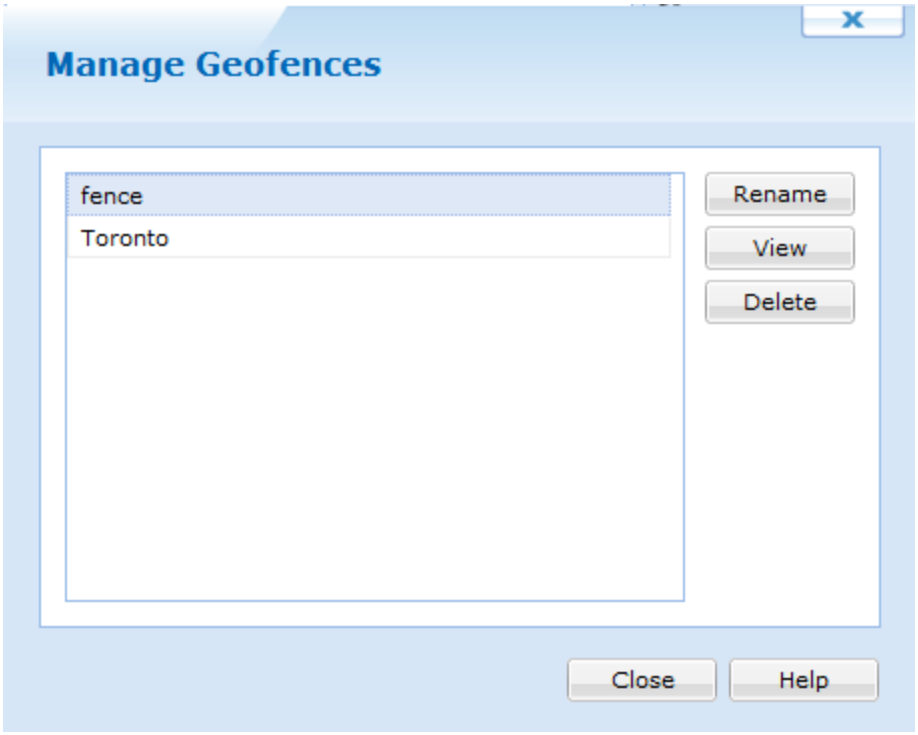
Using Manage Geofences

The Manage Geofences feature provides an area in which to rename, delete or view current created Geofences. You also have the option to create a new geofence from the drop down menu.



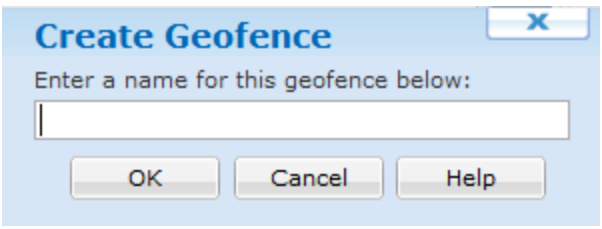
Location panel right click map and select Manage Geofence option

Selecting Manage Geofence brings up the following window.



Field Name	Description
Rename	Allows you to rename a Geofence
View	Allows you to view an already created Geofence on the map
Delete	Allows you to delete a Geofence **NOTE:** In order to Delete the Geofence, no Geofence Event can be associated with it

The **Create Geofence** option allows you to begin drawing on the map. The area drawn on the map will be defined as the Geofence. The defined area must be a complete geometric shape, which means the Start Drawing point will be the same as the End Drawing point. When you have completed a proper geometric shape you be asked to name your geofenced area.



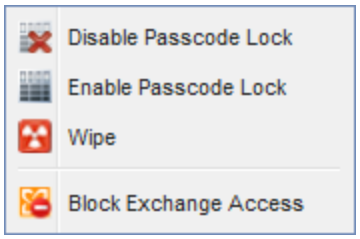
iOS Actions

MobiControlallows you to disable/enable passcode locks, wipe devices and block/unblock Exchange access on a group or an individual device level on iOS devices. These options can be viewed when you right click a device group/device and go to **Action**.

Device Level Actions

Selecting actions on a device level allows you to specifically send actions to that particular device. From here you can disable or enable the passcode, wipe the device, view log file and block or enable Exchange Access. To successfully use the Block/unblock Exchange Access action, you must have the Exchange ActiveSync filter installed on your Exchange Server. For more information on how to install this, please Skin/Formats/CrossReferencePrintFormat(See "Secure Email Access Install The Secure Email Access Filter allows you to achieve greater control with devices receiving email from your Exchange Service. When the filter is installed, you can block access to Exchange on certain devices as well as other controls. To successfully install the Exchange ActiveSync Filter, the MobiControl Root CA must be installed on the server that is publishing the Exchange ActiveSync Service. Below shows how to install the filter on your Exchange Server. Prerequisite StepsInstall MobiControl's Secure Email Access filter(Optional) 3rd party Exchange ActiveSync Filter Configuration Prerequisite StepsThe prerequisite steps show how to install the MobiControl Root CA on the Exchange Server. Go to the MobiControl Administration Utility and go to Certificates. The MobiControlAdministration Utility (MCAU)Click the Export button at beside the MobiControl Root Certificate label. Export the MobiControlRoot CertificateSave the exported certificate in a directory that is easy to remember. Next we need to go to the server with the Exchange ActiveSync Service.Open the Microsoft Management Console (MMC) by opening up the run command and typing mmc. Open the Microsoft Management Console. In MMC, click File then Add/Remove Snap In...Adding Snap-insSelect the Certificates snap-in and click Add >. Adding the Certificates Snap-inA new window will appear asking to select an account. Select the Computer account and click Next. Select the Computer Account. On the next screen select Local Computer and click Finish. Select ComputerAfter clicking Finish, click OK in the Add or remove Snap-ins window. Expand the Certificates (Local Computer) tree on the left side and go to Trusted Root Certification Authorities, then Certificates. Right click the Certificates folder and go to All Tasks then Import.Importing a new CA Follow the steps in the Certificate Import Wizard leaving all settings default. After the wizard has finished you will see the MobiControl Root CA in your Trusted Root Certification Authorities. The MobiControl Root CAInstall MobiControl's Secure Email Access filterMobiControl's Secure Email Access Filter must be installed on the server that is publishing the Exchange ActiveSync service. Typically this is the same computer that is hosting OWA (Outlook Web Access). From the server where the Secure Email Access filter will be installed, open Internet Explorer and browse to the MobiControl Web ConsoleLog in to the Web Console as an Administrator based account that has the "Configure Deployment Servers" permissionSelect the All Devices tab at the top of the MobiControl Web Console and then select the Servers tab located along the bottom of the Web ConsoleRight click on the Secure Email Access filter listed under the Deployment Server, and select Install Exchange ActiveSync FilterSave and then run the ExchangeActiveSyncFilter.exe program. This will place the needed files onto the server. Note: Depending on your Internet Explorer settings, you may be prompted to allow file downloads from the web pageOpen IIS manager and select the web site that is publishing Exchange ActiveSync Select ISAPI filters and select Add from the list of actionsEnter MobiControl Secure Email Access as the filter name For the Executable, If the Exchange ActiveSync site is running in a 32-bit application pool, select \Program Files\SOTI\XAS\mcxas.dll or, if the Exchange ActiveSync site is running in a 64-bit application pool, select \Program files\SOTI\XAS\mcxas64.dllSelect OK to save the filterIn the resulting list of filters, ensure that the MobiControl Secure Email Access filter is listed above the Microsoft Exchange ActiveSync filter. If this is not the case, select View Order List from the available actions, highlight MobiControl Secure Email Access and select Move Up to place it at the top Note: MobiControl's Secure Email Access required communication between the server that is publishing Exchange ActiveSync where the filter is installed, to the MobiControl Web Console. This communication happens over SSL on port 443.3rd party Exchange ActiveSync Filter ConfigurationBefore you begin, the

following components must be installed/enabled.1. IIS 7 with ASP.NET role service enabled.2. URL Rewrite Module installed (version 2.0 is required)3. Application Request Routing version 2.5 (Link)The URL Rewrite Module and Application Request Routing version 2.5 are both installed at the same time. After installation, please follow these steps:Open the IIS managerSelect the server in the tree view on the left hand side and then click on the Application Request Routing feature.Application Request RoutingOn the right menu, click Server Proxy Settings in the Proxy SectionServer Proxy SettingsCheck the Enable Proxy check box. Leave the default values for all the other settings on this page. Click Apply on the right side to commit the change.Enable ProxyNext step is to add the HTTP_ACCEPT_ENCODING server variable and Inbound and Outbound rules. To do this, please go to the left hand panel and select the Default Web Site and then select URL Rewrite. URL rewriteIn the URL Rewrite page, select View Server Variables on the right hand side. View Server VariablesClick the Add... link on the right side of the page to add the HTTP_ACCEPT_ENCODING variable. Click OK then Back to Rules. Adding a server variableClick the Add Rule(s)... link on the right side to add Inbound and Outbound rules. Add rule(s)...When creating the Inbound and Outbound rules, select Blank Rule under the respected heading and click OK.Adding a Blank Inbound or Outbound ruleOn the page shown below, the following fields need to have values entered (Please ensure that you enter your appropriate owa address):NameReverseProxyInboundRule1Pattern^(.*)Rewrite URLhttps://owa.myDomain.com/{R:1} Inbound Rule creation pageAfter the values have been entered, the server variable needs to be added. To do this, expand the Server Variables panel. Click Add and choose HTTP_ACCEPT_ENCODING from the drop down menu. Under value, enter 0, then click OK. Set Server VariableAfter entering all required values, click Apply.Apply Inbound RuleCreate a new blank rule to create an Outbound Rule. Please see below for what values to set on this page: Outbound rule pageUnder precondition, you will need to create a new condition. To do this, select <Create New Precondition...>. When the pop up window appears, click Add... to add a pattern:Add PreconditionAfter entering all required values, Click OK then click Apply.Apply Outbound RuleAfter the rules have been created, click the IIS server, and restart. To confirm that everything has been configured properly, go to C:\inetpub\wwwroot and open the web.config file in notepad. Your file should look similar to this: <?xml version="1.0" encoding="UTF-8"?> <configuration> <system.webServer> <rewrite> <rules> <rule name="ReverseProxyInboundRule1"> <match url="^(.*)" /> <serverVariables> <set name="HTTP_ACCEPT_ENCODING" value="0" /> </serverVariables> <action type="Rewrite" url="https://owa.soti.net/{R:1}" /> </rule> </rules> <outboundRules> <rule name="ReverseProxyOutboundRule1" preCondition="ResponseIsHtml1"> <match filterByTags="A, Form, Img" pattern="^http(s)?://owa.soti.net/(.*)" /> <action type="Rewrite" value="http{R:1}://owa.soti.net/{R:2}" /> </rule> <preConditions> <remove name="ResponseIsHtml1" /> <preCondition name="ResponseIsHtml1"> <add input="{RESPONSE_CONTENT_TYPE}" pattern="^text/html" /> </preCondition> </preConditions> </outboundRules> </rewrite> </system.webServer> </configuration>" on page 1)



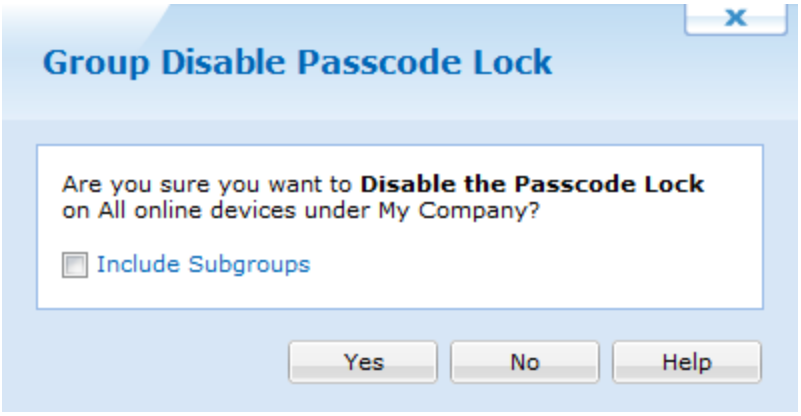
iOS Device Action Selections

Group Level Actions

Below are the options available when you select action from a device group level. Clicking OK on any of the dialog boxes affects every device in the group.

Disable/Enable Passcode Lock

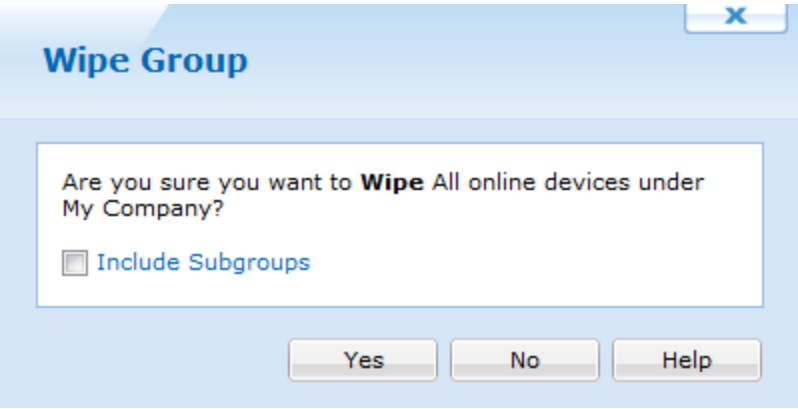
Using the Disable Passcode Lock turns off the pin code on the lock screen in iOS devices. This can be useful when you move multiple devices into a specific group for resetting passcodes. Selecting Enable Passcode Lock enabled the pin code on the lock screen.



Disabling Passcode Lock

Wipe Device

Using the Wipe Device action allows you to delete all information and apps from the devices in the selected group. This can be used when you have devices that pass between multiple users and you do not want users to see previous users accounts or information.



Wipe Group

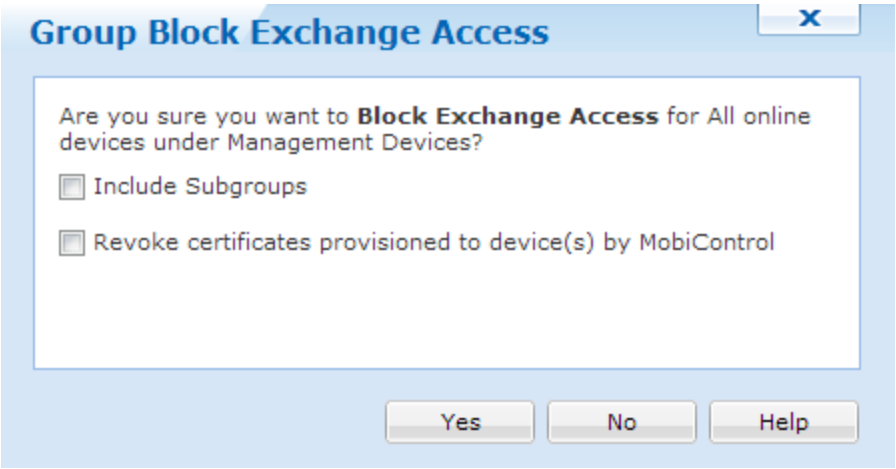
Block/Unblock Exchange Access

Using these options allow you to block and unblock Exchange access to every device in the group. To successfully use this action, you must have the Exchange ActiveSync filter installed on your Exchange Server. For more information on how to install this, please Skin/Formats/CrossReferencePrintFormat (See "Secure Email Access Install The Secure Email Access Filter allows you to achieve greater control with devices receiving email from your Exchange Service. When the filter is installed, you can block access to Exchange on certain devices as well as other controls. To successfully install the Exchange ActiveSync Filter, the MobiControl Root CA must be installed on the server that is publishing the Exchange ActiveSync Service. Below shows how to install the filter on your Exchange Server. Prerequisite StepsInstall MobiControl's Secure Email Access filter(Optional) 3rd party Exchange ActiveSync Filter Configuration Prerequisite StepsThe prerequisite steps show how to install the MobiControl Root CA on the Exchange Server. Go to the MobiControl Administration Utility and go to Certificates. The MobiControlAdministration Utility (MCAU)Click the Export button at beside the MobiControl Root Certificate label. Export the MobiControlRoot CertificateSave the exported certificate in a directory that is easy to remember. Next we need to go to the server with the Exchange ActiveSync Service.Open the Microsoft Management Console (MMC) by opening up the run command and typing mmc. Open the Microsoft Management Console. In MMC, click File then Add/Remove Snap In...Adding Snap-insSelect the Certificates snap-in and click Add >. Adding the Certificates Snap-inA new window will appear asking to select an account. Select the Computer account and click Next. Select the Computer Account. On the next screen select Local Computer and click Finish. Select ComputerAfter clicking Finish, click OK in the Add or remove Snap-ins window. Expand the Certificates (Local Computer) tree on the left side and go to Trusted Root Certification Authorities, then Certificates. Right click the Certificates folder and go to All Tasks then Import.Importing a new CA Follow the steps in the Certificate Import Wizard leaving all settings default. After the wizard has finished you will see the MobiControl Root CA in your Trusted Root Certification Authorities. The MobiControl Root CAInstall MobiControl's Secure Email Access filterMobiControl's Secure Email Access Filter must be installed on the server that is publishing the Exchange ActiveSync service. Typically this is the same computer that is hosting OWA (Outlook Web Access). From the server where the Secure Email Access filter will be installed, open Internet Explorer and browse to the MobiControl Web ConsoleLog in to the Web Console as an Administrator based account that has the "Configure Deployment Servers" permissionSelect the All Devices tab at the top of the MobiControl Web Console and then select the Servers tab located along the bottom of the Web ConsoleRight click on the Secure Email Access filter listed under the Deployment Server, and select Install Exchange ActiveSync FilterSave and then run the ExchangeActiveSyncFilter.exe program. This will place the needed files onto the server. Note: Depending on your Internet Explorer settings, you may be prompted to allow file downloads from the web pageOpen IIS manager and select the web site that is publishing Exchange ActiveSync Select ISAPI filters and select Add from the list of actionsEnter MobiControl Secure Email Access as the filter name For the Executable, If the Exchange ActiveSync site is

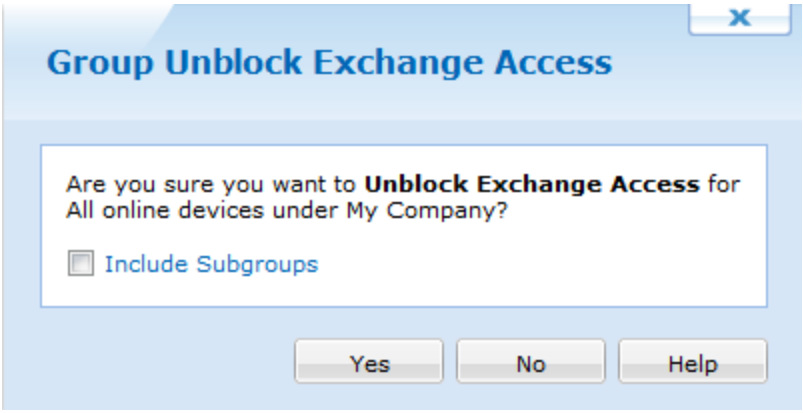
running in a 32-bit application pool, select \Program Files\SOTI\XAS\mcxas.dll or, if the Exchange ActiveSync site is running in a 64-bit application pool, select \Program files\SOTI\XAS\mcxas64.dllSelect OK to save the filterIn the resulting list of filters, ensure that the MobiControl Secure Email Access filter is listed above the Microsoft Exchange ActiveSync filter. If this is not the case, select View Order List from the available actions, highlight MobiControl Secure Email Access and select Move Up to place it at the top Note: MobiControl's Secure Email Access required communication between the server that is publishing Exchange ActiveSync where the filter is installed, to the MobiControl Web Console. This communication happens over SSL on port 443.3rd party Exchange ActiveSync Filter ConfigurationBefore you begin, the following components must be installed/enabled.1. IIS 7 with ASP.NET role service enabled.2. URL Rewrite Module installed (version 2.0 is required)3. Application Request Routing version 2.5 (Link)The URL Rewrite Module and Application Request Routing version 2.5 are both installed at the same time. After installation, please follow these steps:Open the IIS managerSelect the server in the tree view on the left hand side and then click on the Application Request Routing feature.Application Request RoutingOn the right menu, click Server Proxy Settings in the Proxy SectionServer Proxy SettingsCheck the Enable Proxy check box. Leave the default values for all the other settings on this page. Click Apply on the right side to commit the change.Enable ProxyNext step is to add the HTTP_ACCEPT_ENCODING server variable and Inbound and Outbound rules. To do this, please go to the left hand panel and select the Default Web Site and then select URL Rewrite. URL rewriteIn the URL Rewrite page, select View Server Variables on the right hand side. View Server VariablesClick the Add... link on the right side of the page to add the HTTP_ACCEPT_ENCODING variable. Click OK then Back to Rules. Adding a server variableClick the Add Rule(s)... link on the right side to add Inbound and Outbound rules. Add rule(s)...When creating the Inbound and Outbound rules, select Blank Rule under the respected heading and click OK.Adding a Blank Inbound or Outbound ruleOn the page shown below, the following fields need to have values entered (Please ensure that you enter your appropriate owa address):NameReverseProxyInboundRule1Pattern^(.*)Rewrite URLhttps://owa.myDomain.com/{R:1} Inbound Rule creation pageAfter the values have been entered, the server variable needs to be added. To do this, expand the Server Variables panel. Click Add and choose HTTP_ACCEPT_ENCODING from the drop down menu. Under value, enter 0, then click OK. Set Server VariableAfter entering all required values, click Apply.Apply Inbound RuleCreate a new blank rule to create an Outbound Rule. Please see below for what values to set on this page: Outbound rule pageUnder precondition, you will need to create a new condition. To do this, select <Create New Precondition...>. When the pop up window appears, click Add... to add a pattern:Add PreconditionAfter entering all required values, Click OK then click Apply.Apply Outbound RuleAfter the rules have been created, click the IIS server, and restart. To confirm that everything has been configured properly, go to C:\inetpub\wwwroot and open the web.config file in notepad. Your file should look similar to this: <?xml version="1.0" encoding="UTF-8"?> <configuration> <system.webServer> <rewrite> <rules> <rule name="ReverseProxyInboundRule1"> <match url="^(.*)" /> <serverVariables> <set name="HTTP_ACCEPT_ENCODING" value="0" /> </serverVariables> <action type="Rewrite" url="https://owa.soti.net/{R:1}" /> </rule> </rules> <outboundRules> <rule name="ReverseProxyOutboundRule1" preCondition="ResponseIsHtml1"> <match filterByTags="A, Form, Img" pattern="^http(s)?://owa.soti.net/(.*)" /> <action type="Rewrite" value="http{R:1}://owa.soti.net/{R:2}" /> </rule> <preConditions> <remove name="ResponseIsHtml1" /> <preCondition name="ResponseIsHtml1"> <add input="{RESPONSE_CONTENT_TYPE}" pattern="^text/html" /> </preCondition> </preConditions> </outboundRules> </rewrite> </system.webServer> </configuration>" on page 1) If the filter is not installed, a confirm message will appear.

If any certificates were provisioned by MobiControl to devices, we can revoke them when we block Exchange access.

No Filter installed



Blocking Exchange Access



Unblocking Exchange Access

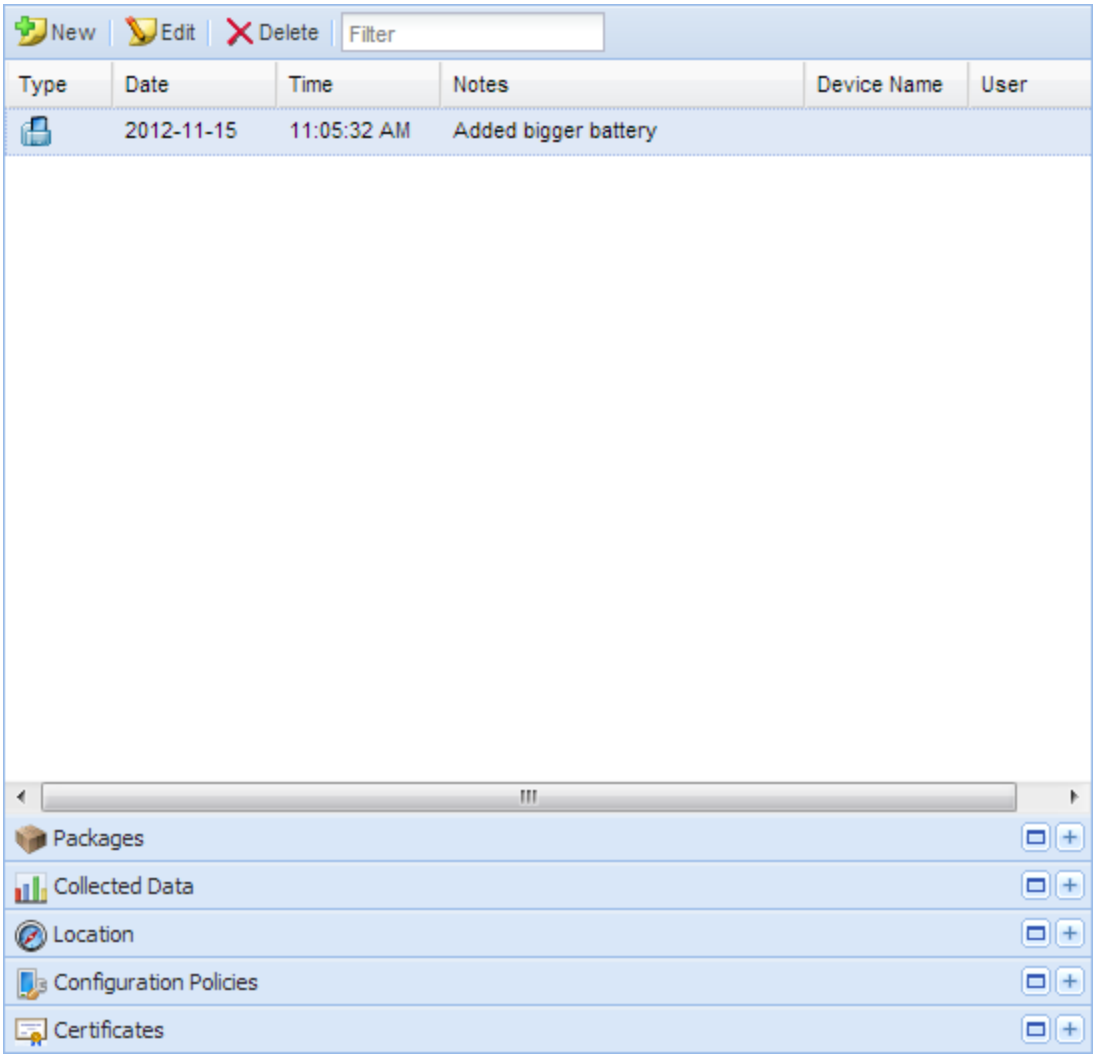
Device Notes

The Device Notes feature allows you to create a note for a device and archive it for future reference and tracking purposes. Each note is editable and includes the date and time when the note was added or edited. The note includes the name of the user creating the note and can be assigned different colors for

color-coded categorization.

This feature is useful for creating a "trouble ticket" for help desk tracking in an end-user support or CRM (Customer Relationship Management) environment. It also allows users with access to the MobiControl Web Console to document a device-specific issue and share their comments and memos related to that device with other users of the MobiControl Web console.

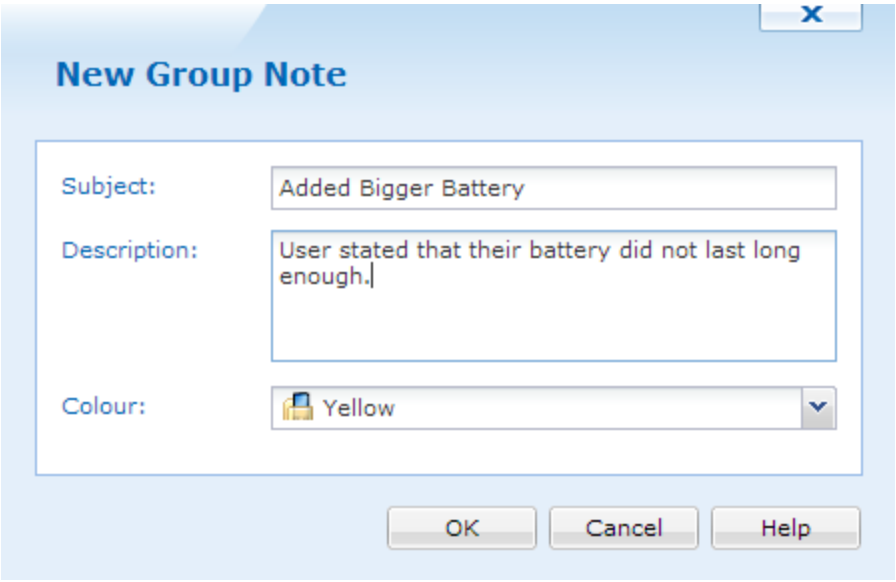
To view and edit notes for a device, select the Devices view (tab) in any of the All Devices, Windows Mobile, Windows Desktop, iOS, Android or Android Plus tab. Select a device and the notes for that device appear in the Notes panel.



Device Notes

Adding or Editing a Note

From within the Notes panel, click **New** to add a new note for the currently selected device or click **Edit** to make changes to an existing note.



Add Note dialog box

The following table describes the fields of the **Add Note** dialog box:

Field Name	Description
Subject	Text entered in the subject field appears in the Notes panel as the title of the note.
Icon	You can choose different colors for the icon to adopt a color-coding to indicate different priority levels or to distinguish between different departments or users creating the note. Notes can be sorted by icon color for a categorized view.
Description	The description field is available for viewing when the note is opened. This field can contain troubleshooting notes, administrative memos or any other device-specific information.

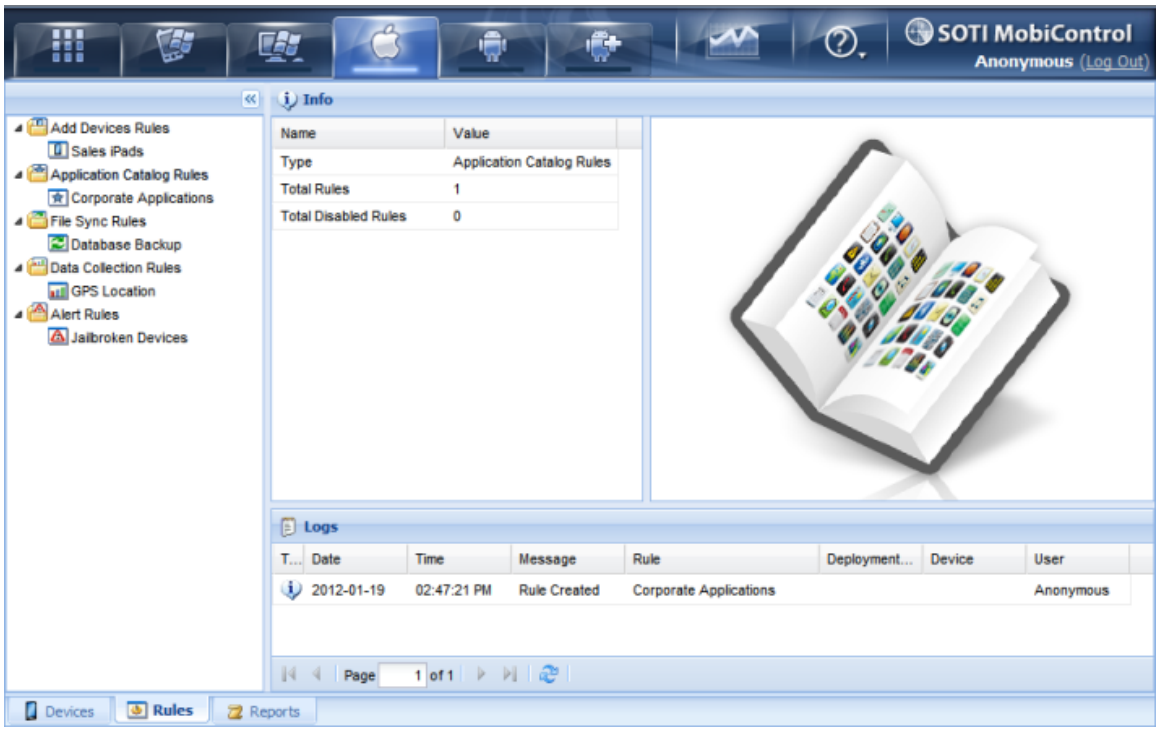
Device Group Notes

MobiControl now offers a way to place notes on a device group level. For example, if you are planning a roll out of devices across the country in phases based on location, you can add device group notes to state which phase each group is in. Therefore, when someone else logs into the MobiControl Web Console, they can see what part of the roll out each group should be in.

To create a device group level note, click a group on the left side of the MobiControl Web Console. After a group has been selected, expand the Notes panel on the right side, and click New.

iOS Rules Tab

MobiControl uses rules to simplify the tasks of device management and configuration. See Below for a description of each rule.



iOS Rules Tab

Add Devices

1. Create an add devices rule.

   An add devices rule allows you to configure the settings that MobiControl uses to set up and communicate with your devices. These settings include: the device group to which devices are added, how often the device is to check for updates, and the parameters to be used for remote control sessions. Please see the "Adding iOS Devices" topic on page 1034 for detailed information about creating an add devices rule.

2. Install the Device Agent onto the devices.

   Once created, there are several options for installing the agent on to your devices. For example, installation can be accomplished via a website download, or by installing the MobiControl Device Agent from the App Store. Please see the "Adding iOS Devices" topic on page 1034 for detailed information about installing the Device Agent.

Application Catalog

1. Create an Application Catalog Rule

   An Application Catalogue Rule allows Administrators to distribute proprietary, in-house applications to employees or members of the organization. Please see the "iOS Application Catalog" topic on page 1050 for detailed information about creating an Alert Rule.

2. Check the Application Catalog Rule Report.

   Once the Application Catalog Rule has been created, you may want to run a report to see what alerts have been generated. You can do this by looking at the Application Catalog Rule Report report in the Reports view (tab). Please see the "Report Types" topic on page 1110 for more detail about reports.

File Sync

1. Create a file sync rule.

   A file sync rule allows you to schedule file(s) to be synchronized between a set of devices and the Deployment Server. When creating a file sync rule, you will need to specify the file(s) you want synced (both their original location and their destination), the interval in between the syncs and which direction the sync should go in (either device to server, or server to device) and which devices should be involved in the sync. Please see the "File Sync Rule" topic on page 344 for detailed information about creating a file sync rule.

2. Check the rule execution status.

   Once the file sync rule has been created, you may want to confirm that the scheduled syncs occurred. You can do this by looking at the rule execution status or by checking the rule execution report in the Reports view (tab). Please see the "Generate Reports" topic on page 390 for more detail about reports.

Data Collection

1. Create a data collection rule.

   A data collection rule allows you to set up rules to collect data from your mobile devices automatically. Please see the "Creating Data Collection Rules" topic on page 318 for detailed information about creating a data collection rule.

2. Check the data collection rule execution status.

   Once the data collection rule has been created, you may want to confirm its execution. You can do this by looking at the rule execution status or by checking the rule execution report in the Reports view (tab). Please see the "Generate Reports" topic on page 390 for more detail about reports.

Alert

1. Create an Alert Rule

   An Alert Rule allows Administrators and Users to be notified when events of interest arise on the system. Please see the "iOS Alerts" topic on page 1068 for detailed information about creating an Alert Rule.

2. Check the Alert Rule execution status.

   Once the Alert Rule has been created, you may want to run a report to see what alerts have been generated. You can do this by looking at the Alert Rule Summary report in the Reports view (tab). Please see the "Report Types" topic on page 1110 for more detail about reports.

Telecom Expense

1. Create an Telecom Expense Rule

   A Telecom Expense Rule allows Administrators and Users to be notified on current usage of company data and voice minutes. Please see the "iOS Telecom Expense Management" topic on page 1103 for more information.

2. Check the Telecom Expense Rule execution status.

   Once the Alert Rule has been created, you may want to run a report to see what alerts have been generated. You can do this by looking at the Telecom Expense Rule Summary report in the Reports view (tab). Please see the "Generate Reports" topic on page 623 for more details about reports.

Adding iOS Devices

To Add iOS Devices you need to create an **Add Devices Rule** and then provide your users with instructions to enroll their devices.

Add devices rules allow MobiControl to name devices, place devices in the appropriate device group, and to generate a customized Enrollment ID that, when enrolled by the user, allows MobiControl to manage the devices.

To create an add devices rule, select the Apple iOS Tab within MobiControl Web Console, then select the **Rules** Tab. Right-Click the **Add Devices Rules** folder and select **Create Add Devices Rules**.

Apple iOS Tab

The six steps below describe how the Create Add Devices Rule Wizard can be used to create an add devices rule:

1. Start the Wizard

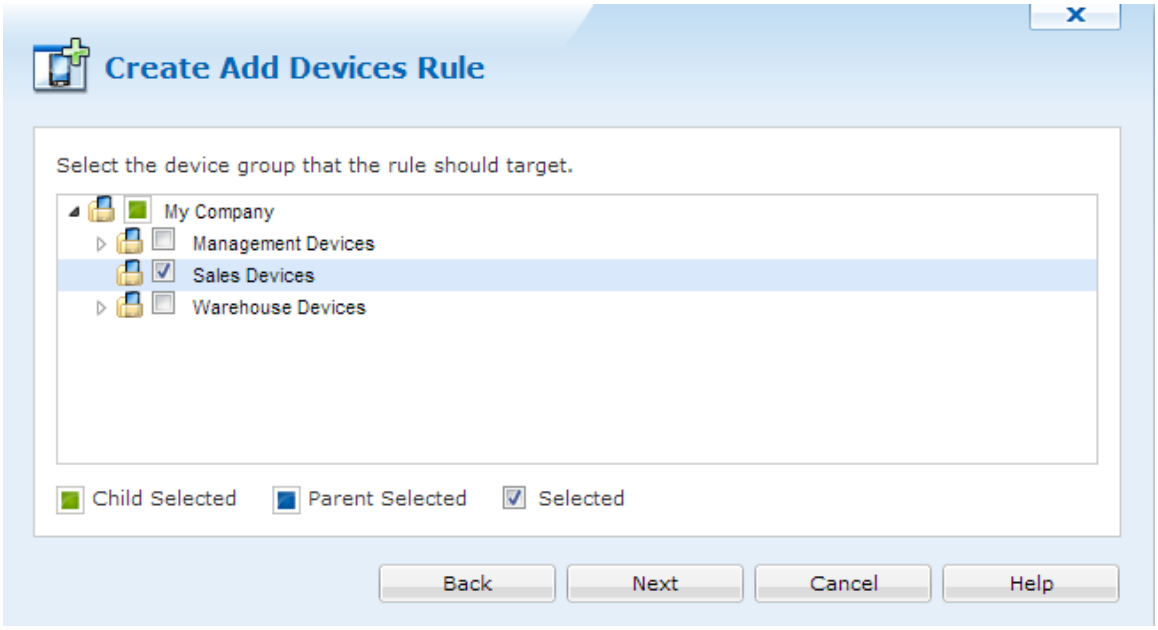
   Select the **Rules** Tab, from the **Apple iOS** Tab, then Right-Click the **Add Devices Rules** folder and select **Create Add Devices Rules**. The first page of the Create Add Devices Rule Wizard will be displayed.

   Enter a descriptive name for the add devices rule you are creating and click **Next.**

First page of the Create Add Devices Rule Wizard

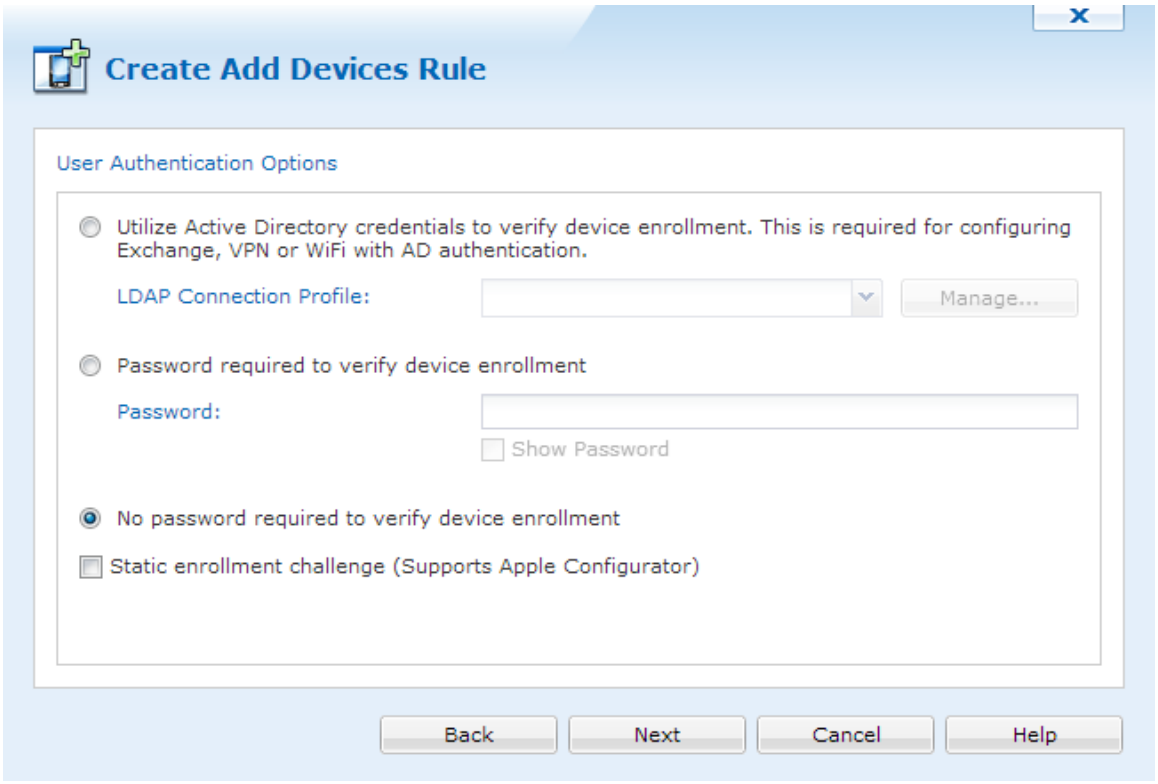
2. Configure the Device group

First, select to which device group the devices configured by this rule will be added. The dialog box below displays the current device tree. Select the group where devices need to be inserted and then click **Next.**



Device Group Selection page

3. Configure Authentication Options



User Enrollment Authentication

Select a user authentication method for enrolling devices. A password may be set to ensure unwanted devices are unable to enroll in your network.

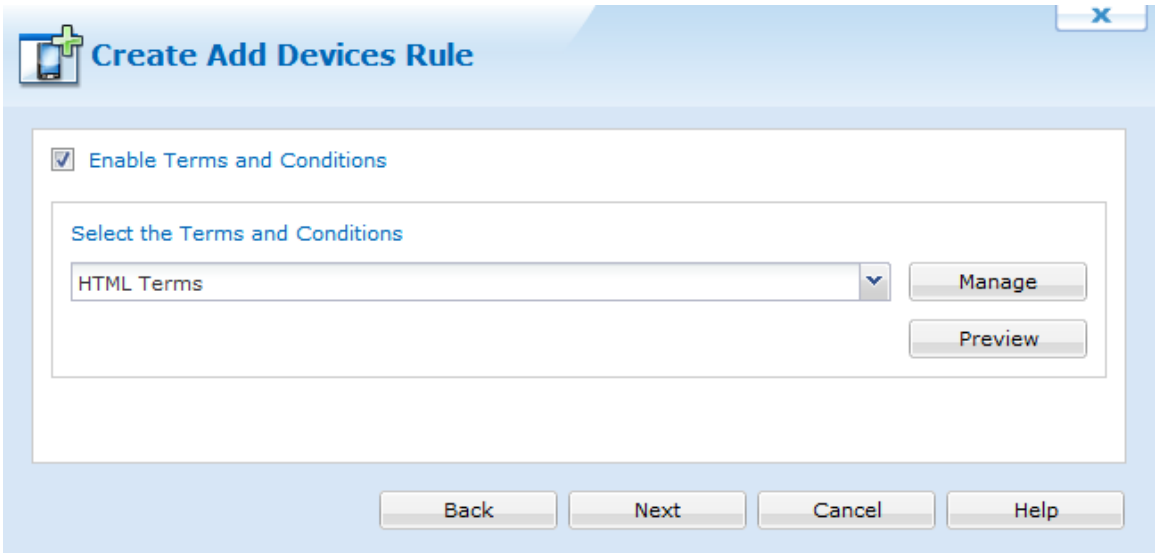
If Utilize Active Directory credentials is selected, choose the connection type from the drop down menu. If there is no connections, click Manage to create a new connection. Please see the "LDAP Connections Manager" topic on page 616 for more information regarding LDAP connections.

NOTE:

Checking off Static enrollment challenge allows us to download the enrollment or the MobiControl trust profiles so that iOS devices can be enrolled through the iPhone Configuration Utility.

4. Terms and Conditions

The terms and conditions page allows us to send terms and conditions to devices. Users must accept these terms before they are able to enroll their device to MobiControl. If they do not accept the terms and conditions, the device will not connect. If Terms and Conditions is required, click "Enable Terms and Conditions".



Terms and conditions

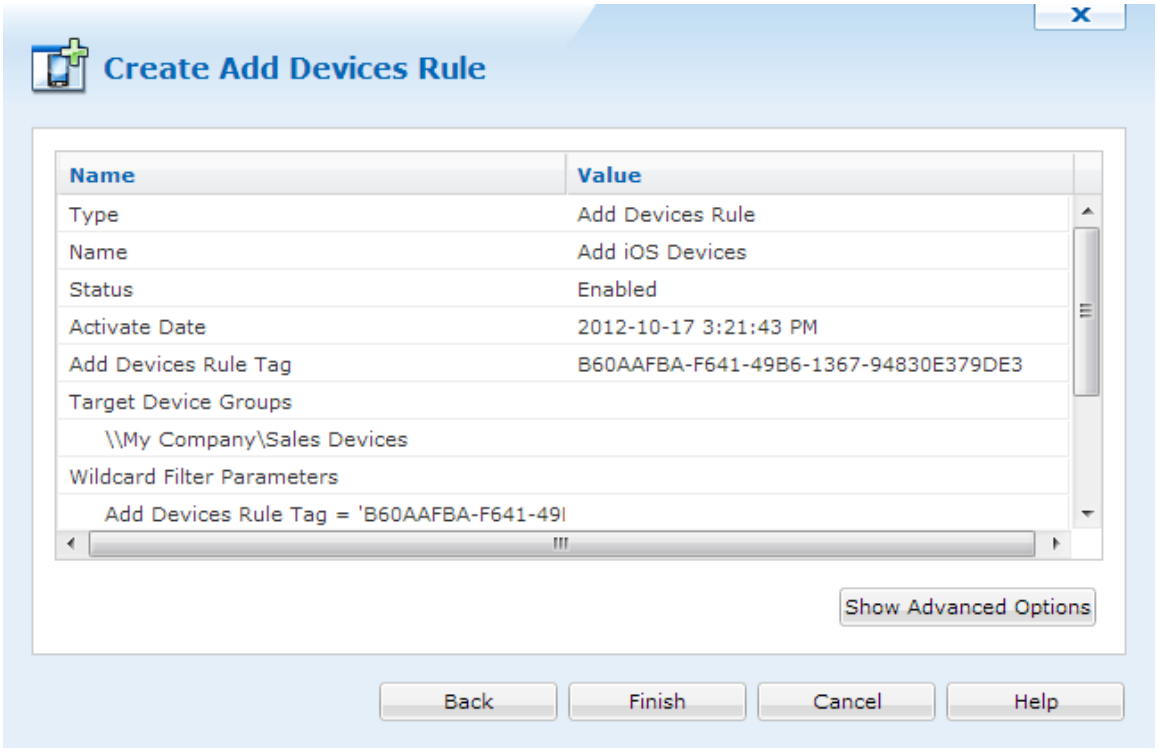
To add new Terms and Conditions to the Add Devices rule, click Manage. Once clicked, we can see the Terms and Condition Manager. Please see the "Terms and Conditions" topic on page 619 for more information.

After selecting the Terms and Conditions, click **Next** to continue the creation of the rule.

5. Review Summarized Information

The **Rule Summary Information** page summarizes the settings configured on the previous pages of the wizard.

If you are satisfied with the configured settings, click on the **Finish** button to create the device rule, otherwise use the **Back** button to go to previous screens and make adjustments.

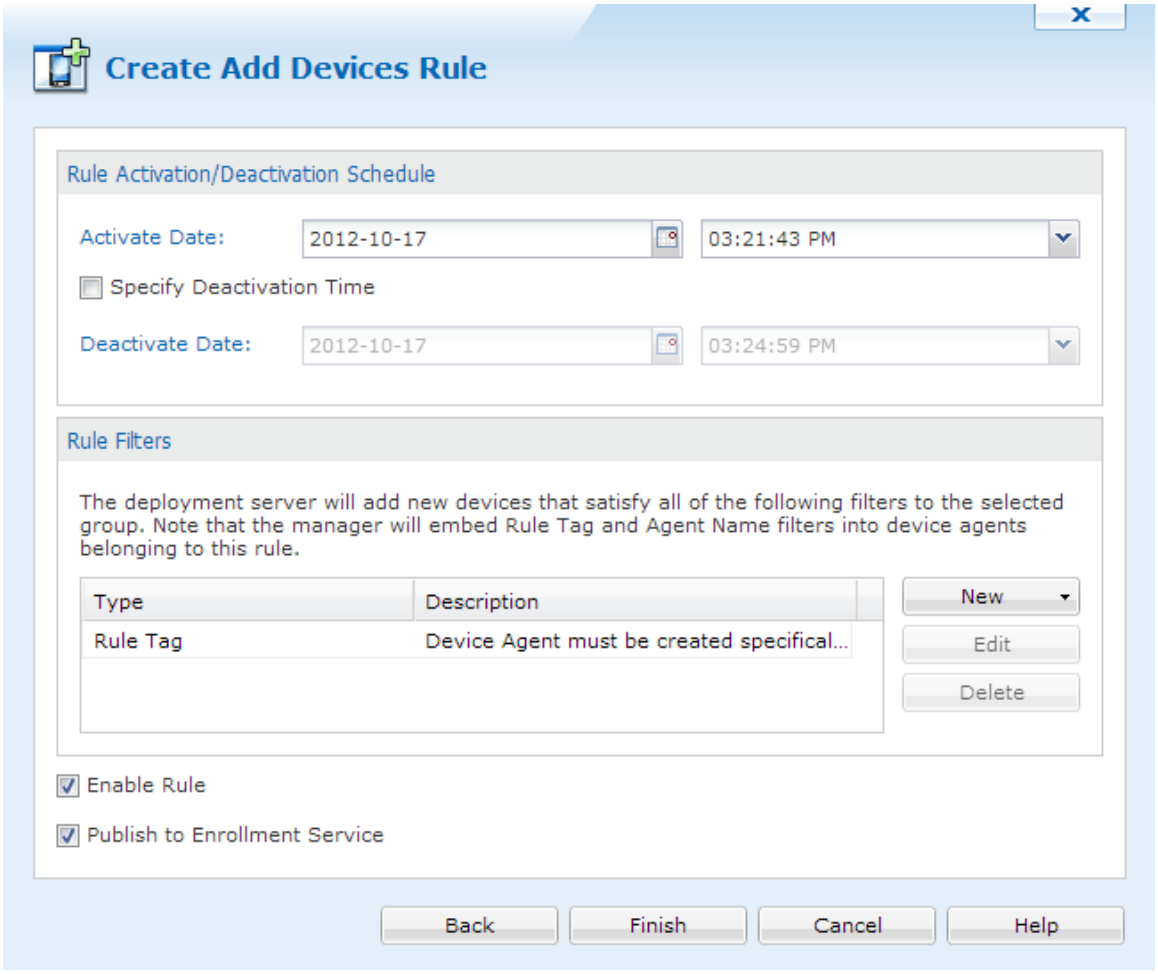


Rule Summary Page

6. Advanced Settings

The **Advanced Settings** button allows you to specify which devices are to be configured by this rule. By default, MobiControl will use this rule to configure only those devices that are running a Device Agent created specifically for this device rule. By using advanced settings filters, you can broaden or further restrict which devices get configured by this rule when they connect to MobiControl.

Once you have made the changes, click **Next.**



Advanced Settings Page

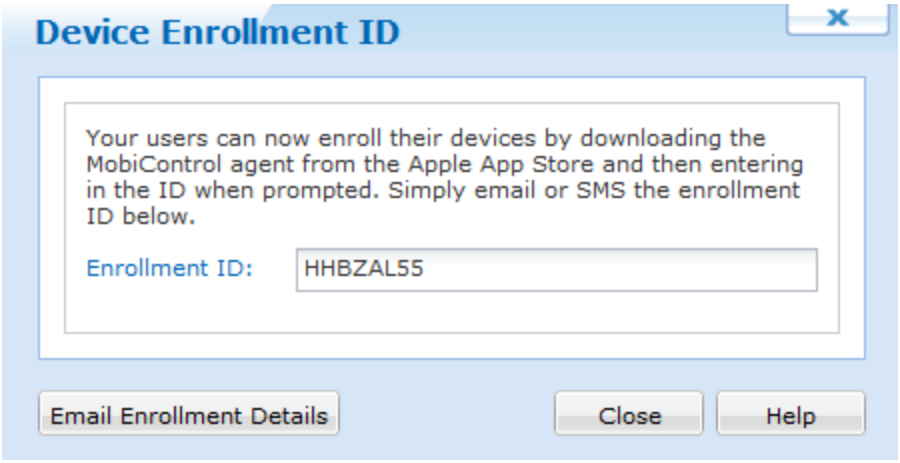
The "Publish to Enrollment Service" allows a code to be generated and used on the iOS Device Agent . When an iOS Device Agent is installed from the App Store there is no way for the device agent to know which Deployment Server it wants to connect to. Using the Enrollment ID created when you "Push to Enrollment Service" allows the generic agent from the App Store to find the correct Deployment Server information.

NOTE:

If no iOS Device Agent has been downloaded from the App Store, make sure to uncheck "Publish to Enrollment Service" and use the Enrollment URL.

6. Receive a Device Enrollment ID

   To enroll an **Apple iOS** device, users must download the MobiControl Device Agent on their device. After downloading the Device Agent the user must enter the Enrollment ID shown. You are also able to email the Enrollment Details to users. Please see the "iOS Agent Install Methods" topic on page 949 for more information.



Device Enrollment ID

Enrolling iOS devices

After you create your Add devices rule for your iOS device you must then install profiles on your device. Please see the "Adding iOS Devices" topic on page 1034 for more information.

If you install a Device Agent then the profile installation process is semi-automatic, if you have decided to go agentless, you must go to your device's Safari browser and enter the URL that is shown in the MobiControl web console.

When installing iOS profiles, there are two options to choose. The first option to choose is when a third party signed certificate is installed on the Deployment Server. The second option is using a certificate generated by your server which is not signed by a third party.

Having a signed certificate allows enrolling iOS devices to trust your server. If your server is trusted then the enrollment process is faster and easier. If your server does not have a signed certificate then you have to install a MobiControl generated certificate called the Trust Profile on your iOS device. The Trust Profile will allow your iOS to accept the enrollment profile.

NOTE:

If "Static enrollment challenge" is checked off while creating the Add devices rule, then we can download the Enrollment and MobiControl Trust profile. To do this, right click the rule, and click either profile to download.
If a third party certificate is used, then the Enrollment Profile is the only one needed, if not, then we must download the MobiControl Trust Profile as well.
We can then install these profiles with the iPhone Configuration Utility.

The two options for enrolling are listed below:

Signed Certificate

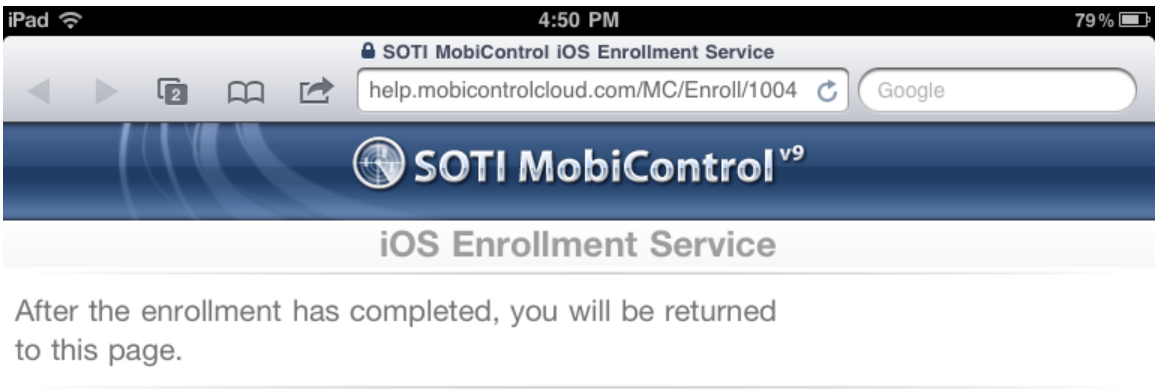
Unsigned Certificate

Signed Certificate

Below shows the process of when you have a signed third party certificate signed on your Deployment Server.

1. Download the MobiControl iOS profile

   When you successfully enroll your iOS device through the Device Agent or directly go to Safari and enroll agentless, the following web page will appear.



Safari showing the enrollment process

2. Confirm installation

After the Profile has been downloaded in Safari, you will be brought to Profile settings. Once there, you can verify the profile and install it.

Installing the MobiControl Profile

Confirm installation

3. Warning

When you tap **Install Now**, your iOS device will show you a warning message giving you a brief explanation on what the MobiControl Device Profile will do.

Warning Message

4. Profile Installed

   After you tapped **Install** on the warning panel, the MobiControl profile will now be installed. It goes through multiple steps which are automatic and require no user interaction. Once the profile is installed all that is left to do is tap **done**.

MobiControl iOS profile Installed

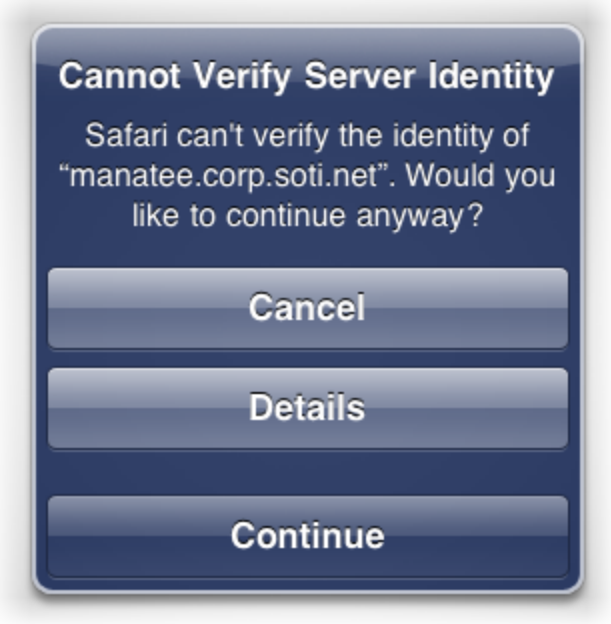
After the profile has been installed you will then be brought back to Safari. You can now see in the MobiControl Web Console that your iOS device is fully enrolled.

Unsigned Certificate

If you do not have a signed certificate installed on your Deployment Server, iOS enrollment has a different process. Below shows the process of how to enroll an iOS device with an unsigned certificate.

1. Going to the iOS Enrollment Service Web Page

   When you successfully enroll your iOS device through the Device Agent or directly go to Safari and enroll agentless, a pop up will appear stating that it cannot verify the server identity. Tap **continue** to view the iOS Enrollment Service web page.



Cannot Verify Server Identify

The iOS Enrollment Service Web Page

2. Download the MobiControl Trust Certificate

Tap **Step 1** to begin downloading the MobiControl Trust Profile. This profile will install the MobiControl Root CA on your iOS device. This is implemented to verify the MobiControl Device Enrollment profile. Tap **install** to continue with the enrollment process.

The MobiControl Trust Profile

Install the MobiControl Trust Profile

Profile installed

3. Download the MobiControl Enrollment Certificate

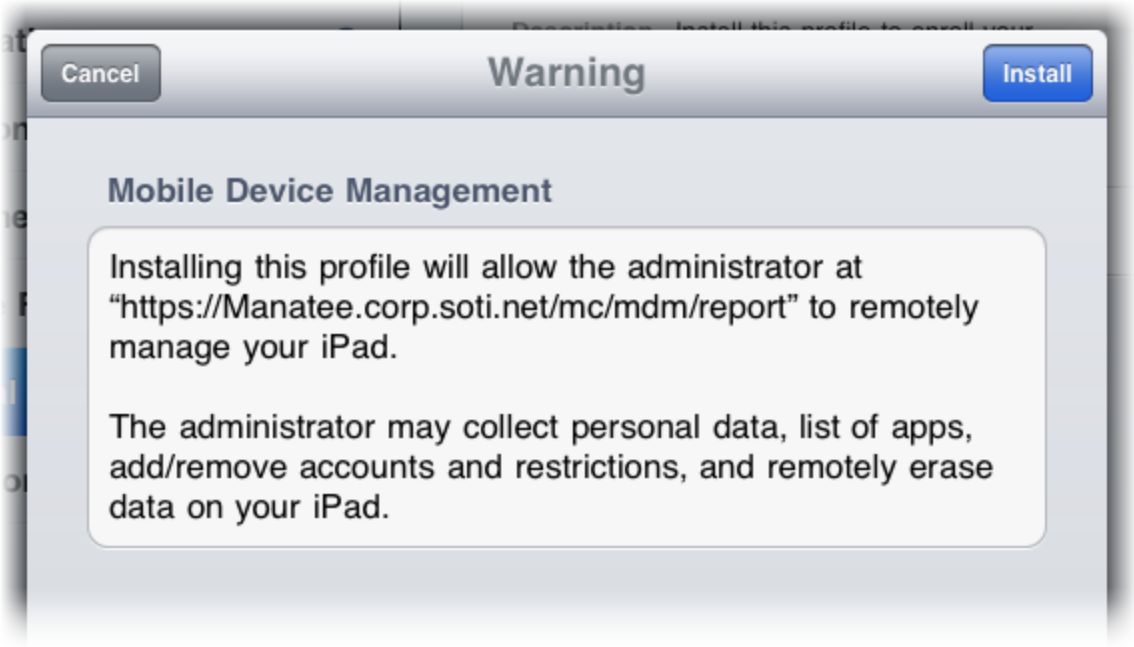
After the MobiControl Trust Profile has been installed, you will be redirected back to Safari to continue the enrollment process. When you are returned back to Safari, tap Step 2 to download the Enrollment Certificate. The MobiControl Device Enrollment Profile will now be shown. Tap **install** then **Install Now**.

The MobiControl Device Enrollment Profile

Confirm installation

4. Warning

When you tap **Install Now**, your iOS device will show you a warning message giving you a brief explanation on what the MobiControl Device Profile will do.



Warning Message

5. Profile Installed

   After you tapped **Install** on the warning panel, the MobiControl profile will now be installed. It goes through multiple steps which are automatic and require no user interaction. Once the profile is installed all that is left to do is tap **done**.

MobiControl iOS Profile Installed

After the profile has been installed you will then be brought back to Safari. You can now see in the MobiControl Web Console, that your iOS device is fully enrolled.

iOS Application Catalog

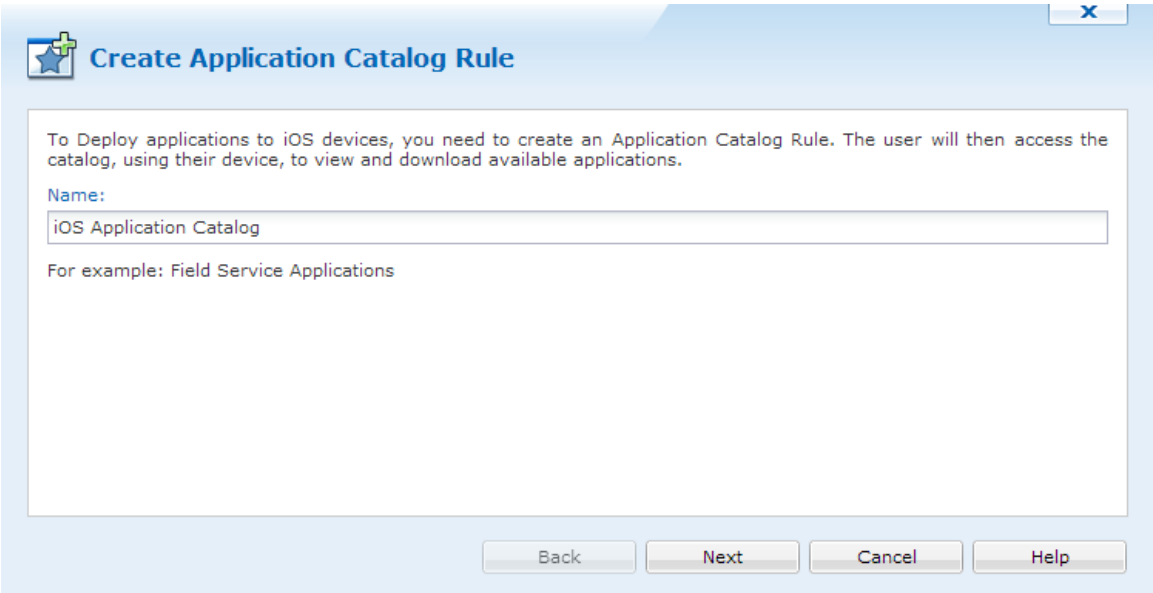
The Application Catalog allows us to let users know what approved apps they are able to download on their device. We can configure App Store applications to appear, set it to be mandatory so that users must download it, or set it as optional. We can also upload enterprise built applications without posting them into the App Store.

If an application is set to mandatory, the user will constantly be prompted to download it.

To create an Application Catalog, we must first create it's rule. To do this, go to the iOS rule tab. Right click Application Catalog then click **Create Application Catalog Rule**.

Naming the Rule

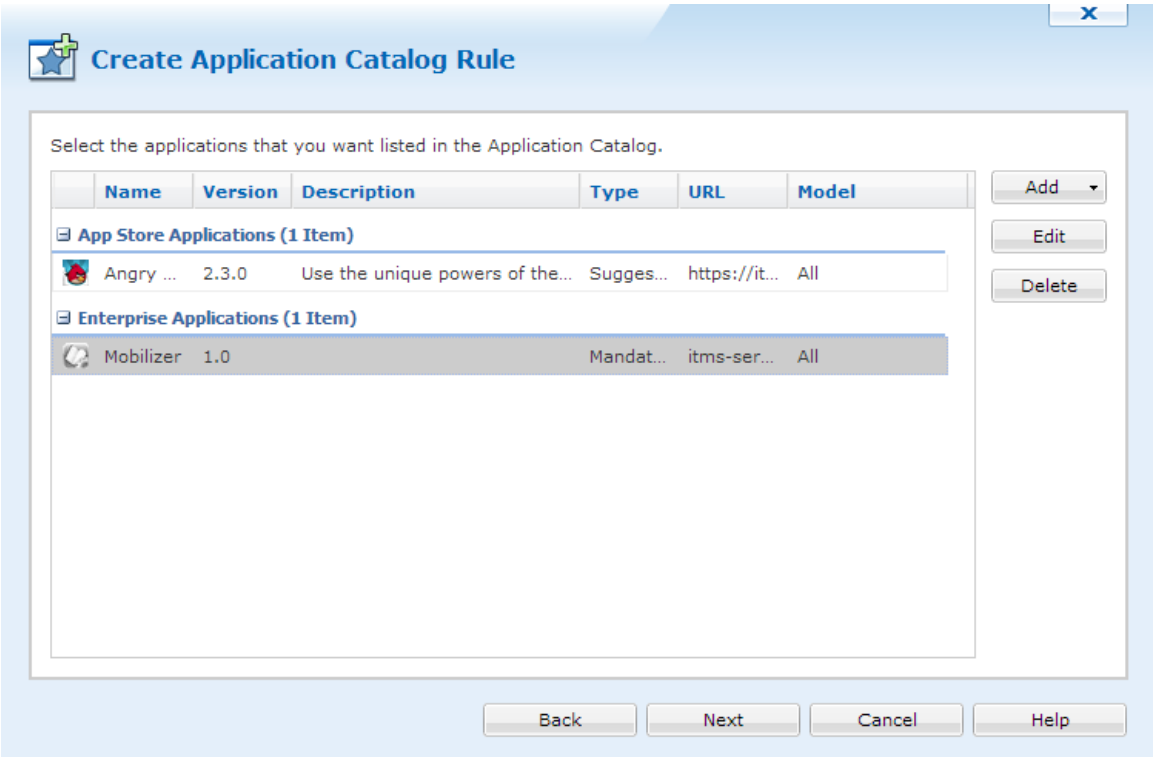
When the Application Catalog wizard appears, enter a name then click Next



Name the Application Catalog

Application Selection

The next panel will allow us to add App Store or Enterprise Apps.



Adding Applications

Click Add and select either Enterprise Applications or App Store Applications.

Clicking each header below will reveal more information about each topic:

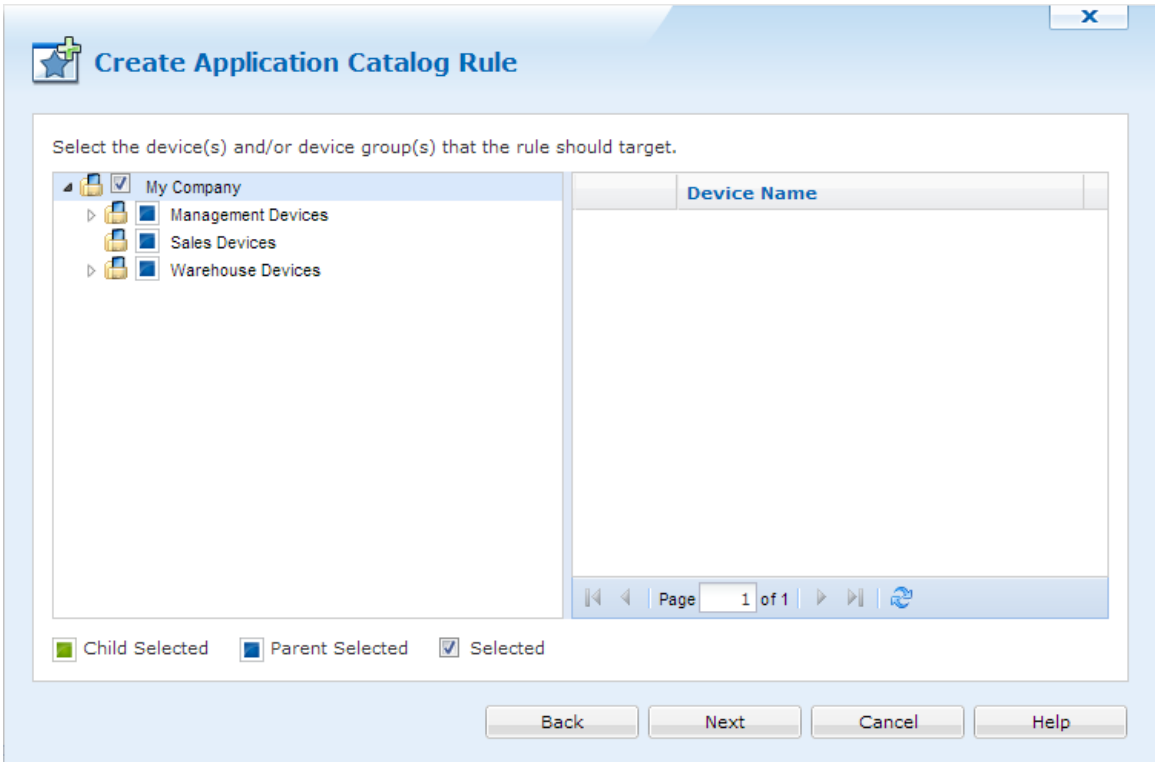
Enterprise Applications

App Store Applications

After all required apps are added, click Next.

Select Devices and Groups

The next panel will let us choose which groups and/or devices will receive this Application Catalog.

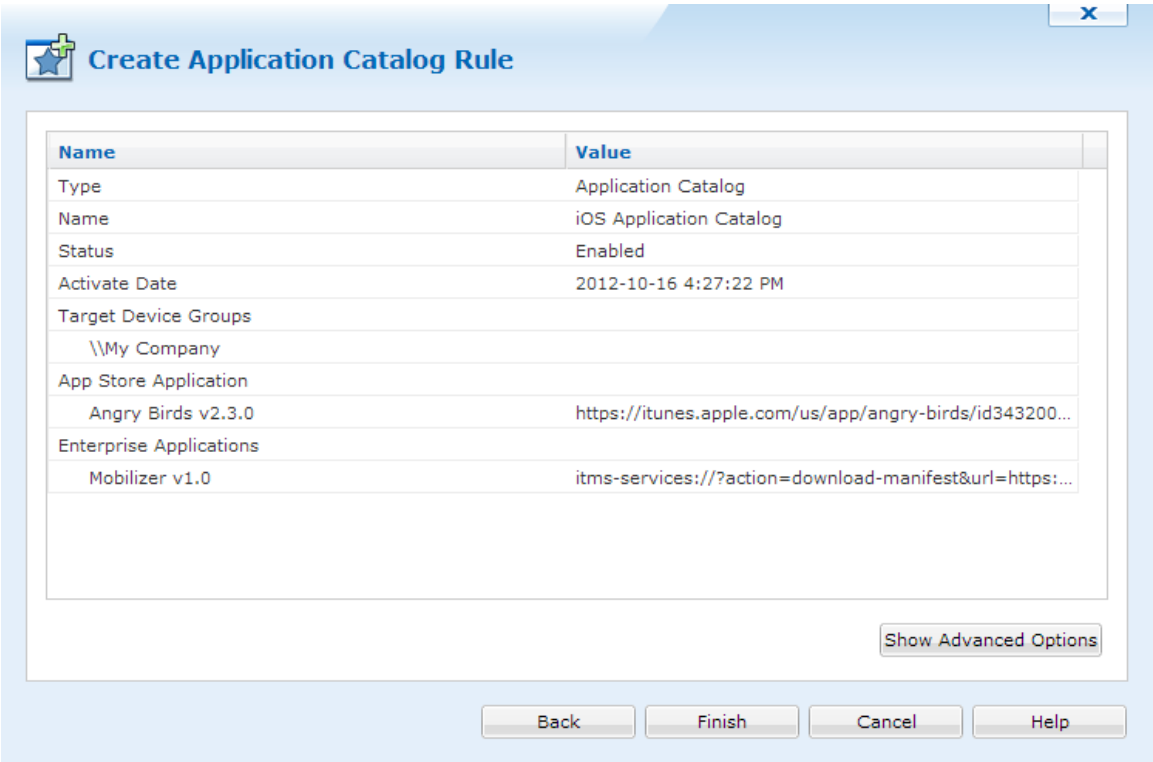


Target Groups or Devices

When devices are selected, click Next.

Summary

The last panel will show us a summary of the Application Catalog.



Application Catalog Summary

Clicking **Show Advanced Options** will allow us to configure more settings for the Application Catalog. Some of these settings include changing the Application Catalog icon and the banner.

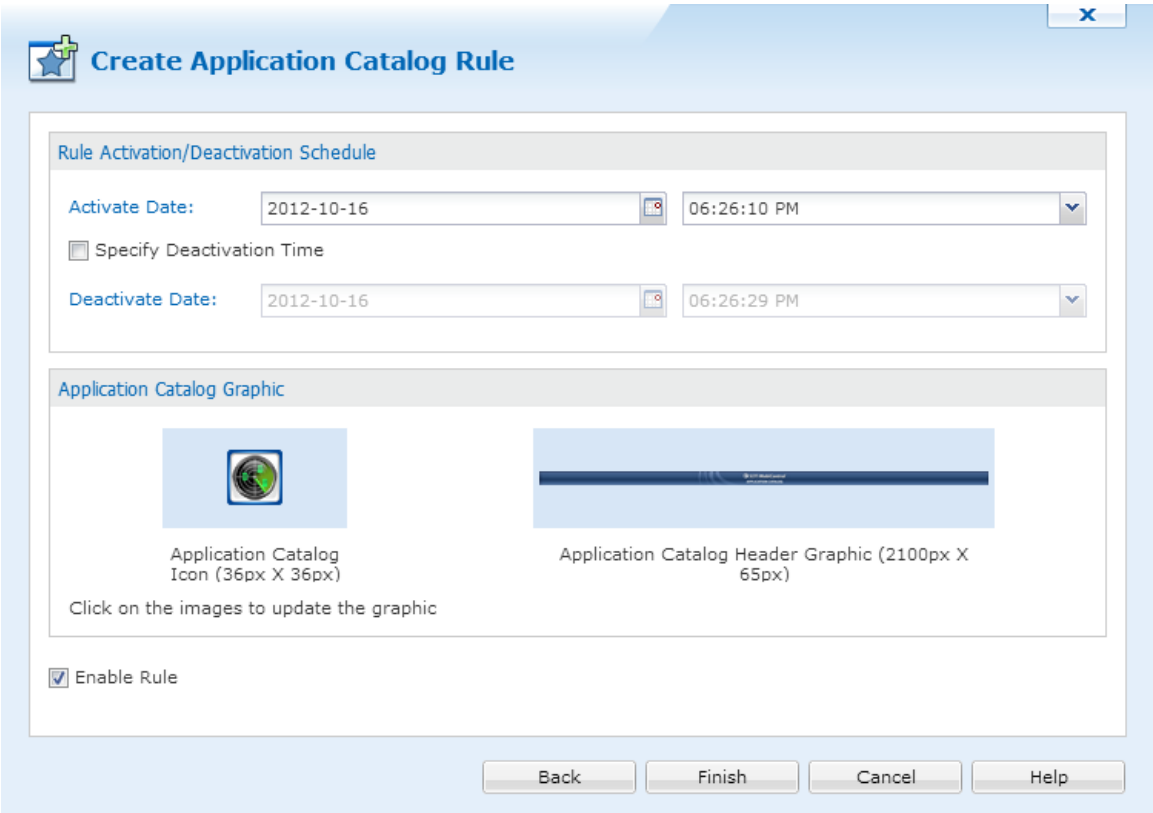
Advanced Options

Here we are able to set when this rule will be activated and deactivated, and change the Application Catalog graphics.

The Application Catalog icon is what would appear on the home screen, while the Application Catalog Header is what appears in the actual catalog. Clicking each image will allow us to upload new images.

NOTE:

The Application Catalog icon must be 36px X 36px, while the Application Catalog Header can be 2100px X 65px.



Application Catalog Advanced Options

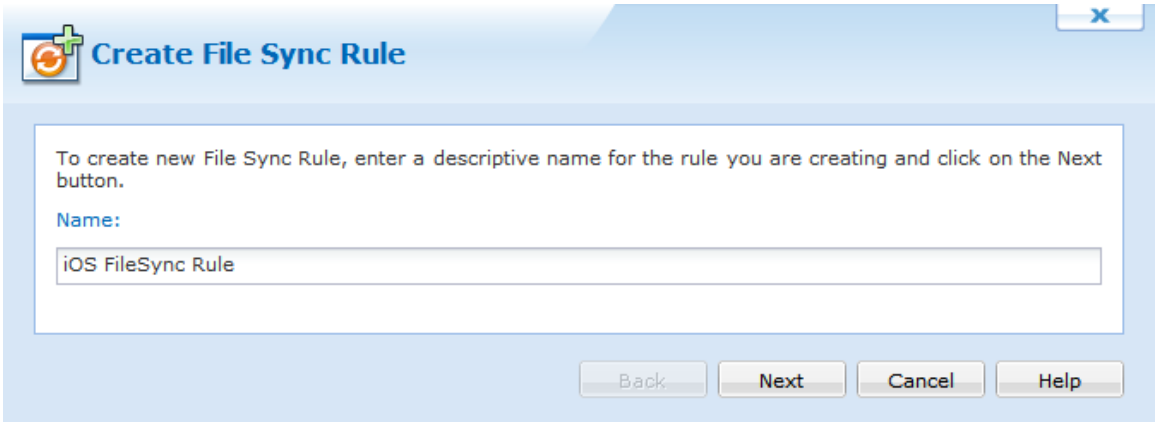
After everything is configured, click Finish to save and close the wizard.

Creating File Sync Rules on iOS Devices

File sync rules allow you to synchronize files and folders between your devices and a server. File collection, also referred to as file uploading, is a very convenient method for gathering information from devices, for example a transaction log file. File dissemination, also referred to as file downloading, is a quick and easy way to send one or more files to a set of devices such as an updated product listing or configuration file.

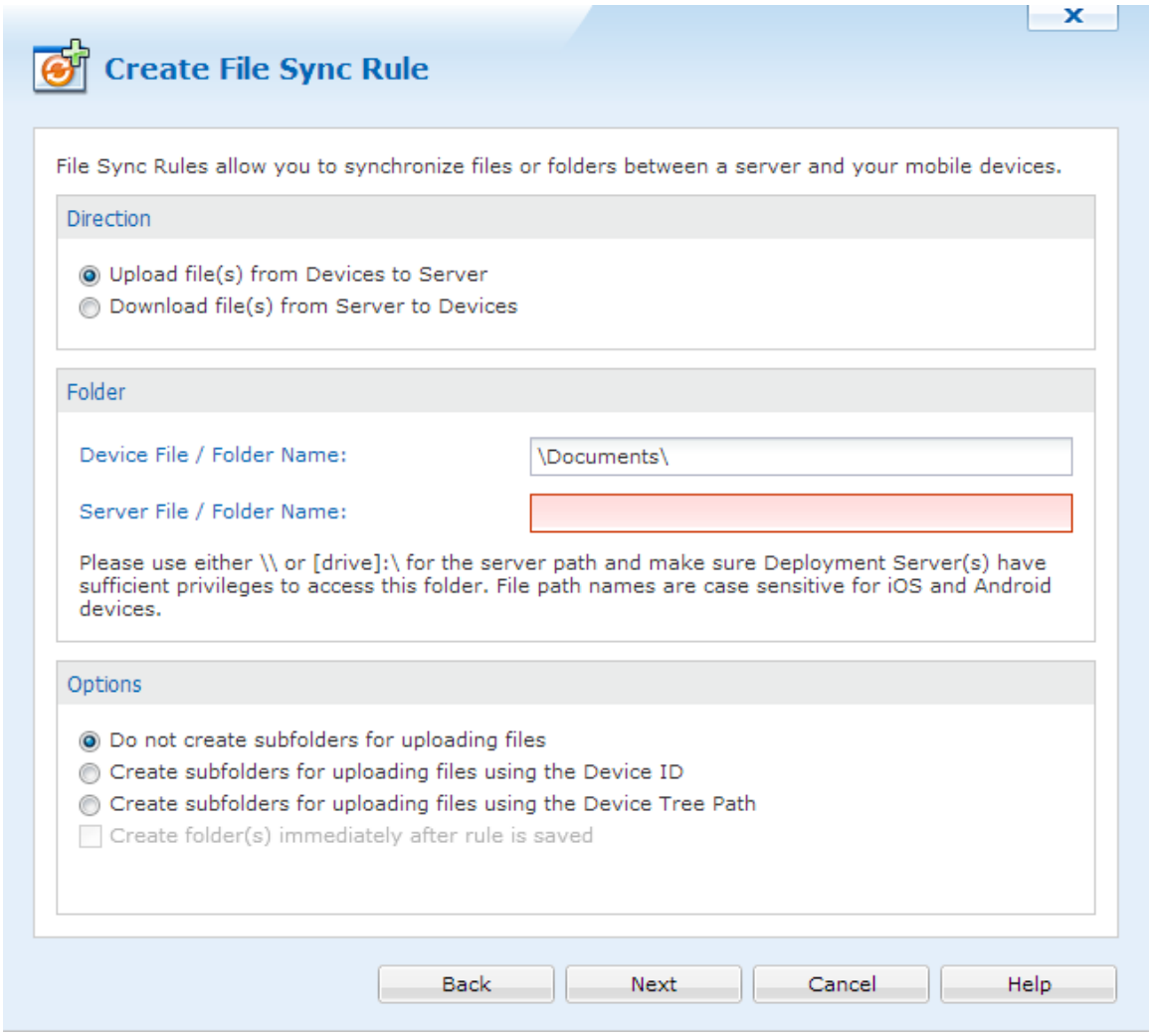
1. Start the wizard.

   Select the Rules view (tab), then click **Rule,** point to **Create Rule,** and click **File Sync Rule.** Enter a meaningful name for the rule.



First page of the Create File Sync Rule Wizard

2. Configure file synchronization source and destination.



Configure file sync source and destination

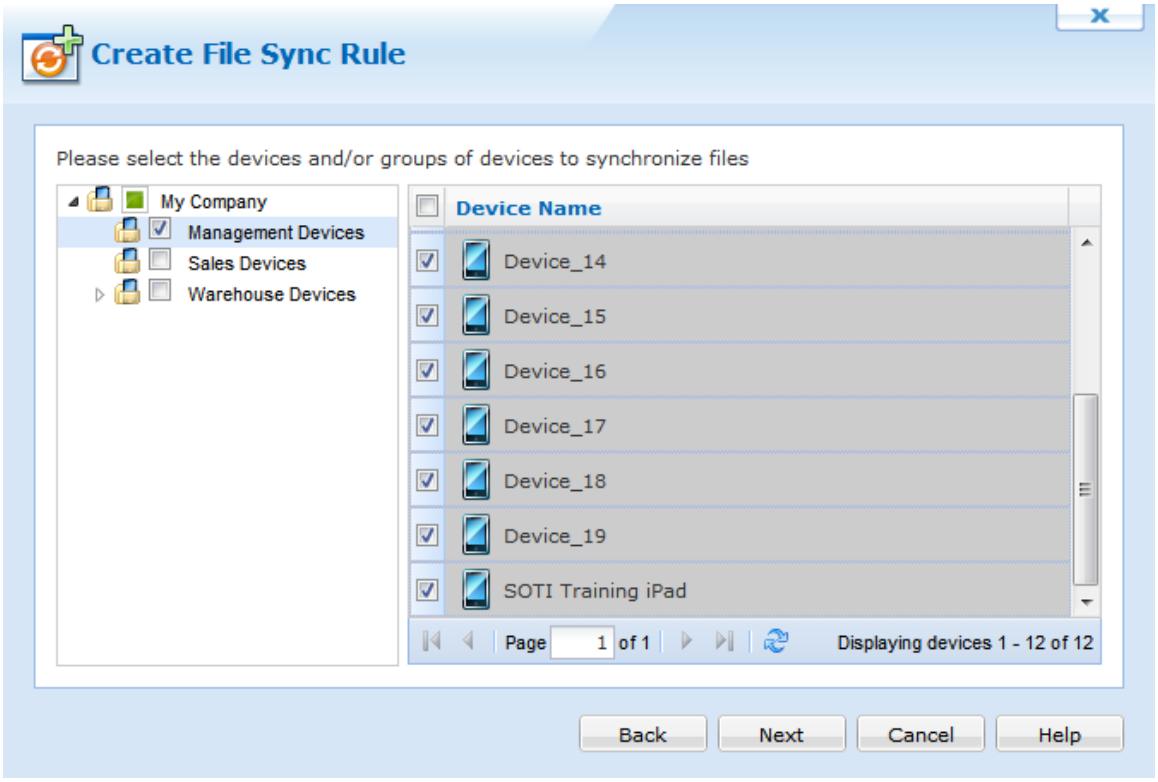
The following table describes the fields of this page of the wizard:

Field Name	Description
Direction	• **Upload** (File collection) The rule will be used to upload files from the devices to a server. • **Download** (File dissemination) The rule will be used to download files from the server to devices.
Device File/Folder	Specifies the complete file system path to the files or folders being synchronized on the device. iOS devices only support the \Documents\ folder.

Field Name	Description
Server File/Folder	Specifies the complete file system path to the files or folders being synchronized on the server It is strongly recommended that a UNC (Universal Naming Convention) path be used. A local path (i.e. `C:\MyFiles`) can be used if only one Deployment Server is being used and the local path is on the computer running the Deployment Server. **NOTE:** It is important that the Deployment Servers have sufficient permission to read and write to the source or destination UNC path. Best practice is to run the Deployment Server under its own Active Directory user profile.
Server-side Folder Options	For **upload rules,** files collected from the devices can be written to: • A single shared folder, meaning files could potentially be overwritten if they have the same name. • A per-device subfolder, named using the device ID (i.e {00135304-41D7-019E-5800-0050BF3F5173}) • A per-device subfolder, named using the device tree path (i.e. `.\Management Devices\Device 0001`) For **download rules,** files disseminated from the server can be read from: • A single shared folder, meaning all devices get the same file(s). • A per-device subfolder, named using the device ID (i.e. {00135304-41D7-019E-5800-0050BF3F5173}) • A per-device subfolder, named using the device tree path (i.e. `.\Management Devices\Device 0001`) When the **Create folder(s) immediately after rule is saved** option is enabled, the server-side folders will be created immediately after the file sync rule is saved. This allows adding files to the folders on the servers that are synchronized with the devices when the file sync event occurs.

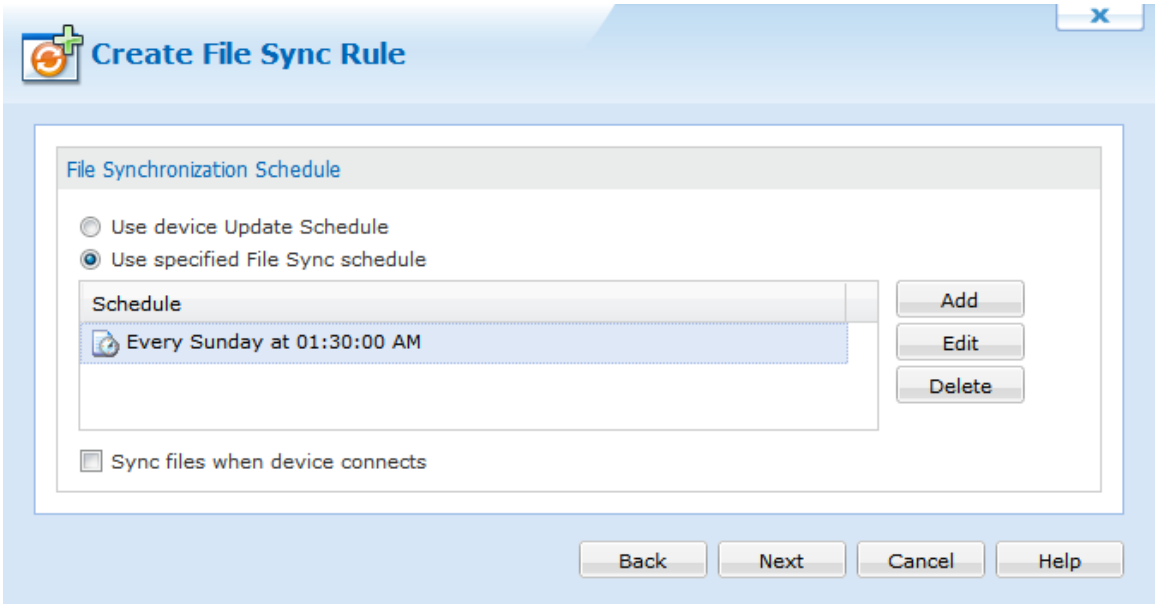
3. Select devices.

   Select the device(s) and group(s) for which the file sync rule will apply.



Device Group selection page

4. Specify the synchronization and activation or deactivation schedule.



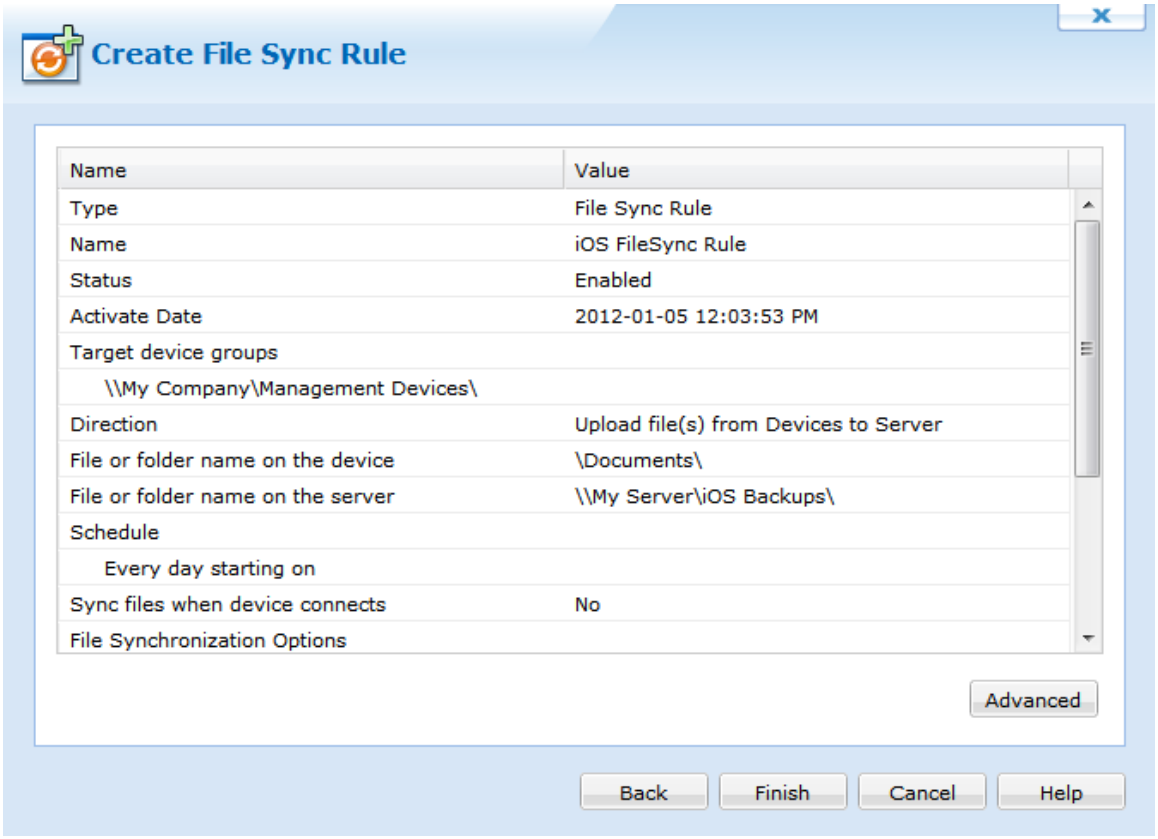
Rule activation schedule

Field Name	Description
Use Device Update Schedule	By default, the device update schedule (specified by the file sync rule used to add the devices to the system) triggers file synchronization
Use Specified File Sync Schedule	If you specify a file synchronization schedule in this dialog box, only that schedule will be used, and the device synchronization schedule will not trigger file synchronization. To Specify the custom schedule click the **Add** button.

By default, the file sync rule will be activated immediately upon completion of the wizard. If you wish to delay the activation you can modify the activate date. A deactivate date can optionally be entered to specify a date from which the rule will be disabled. A file sync rule can also be explicitly disabled by clearing the **Enable Rule** check box.

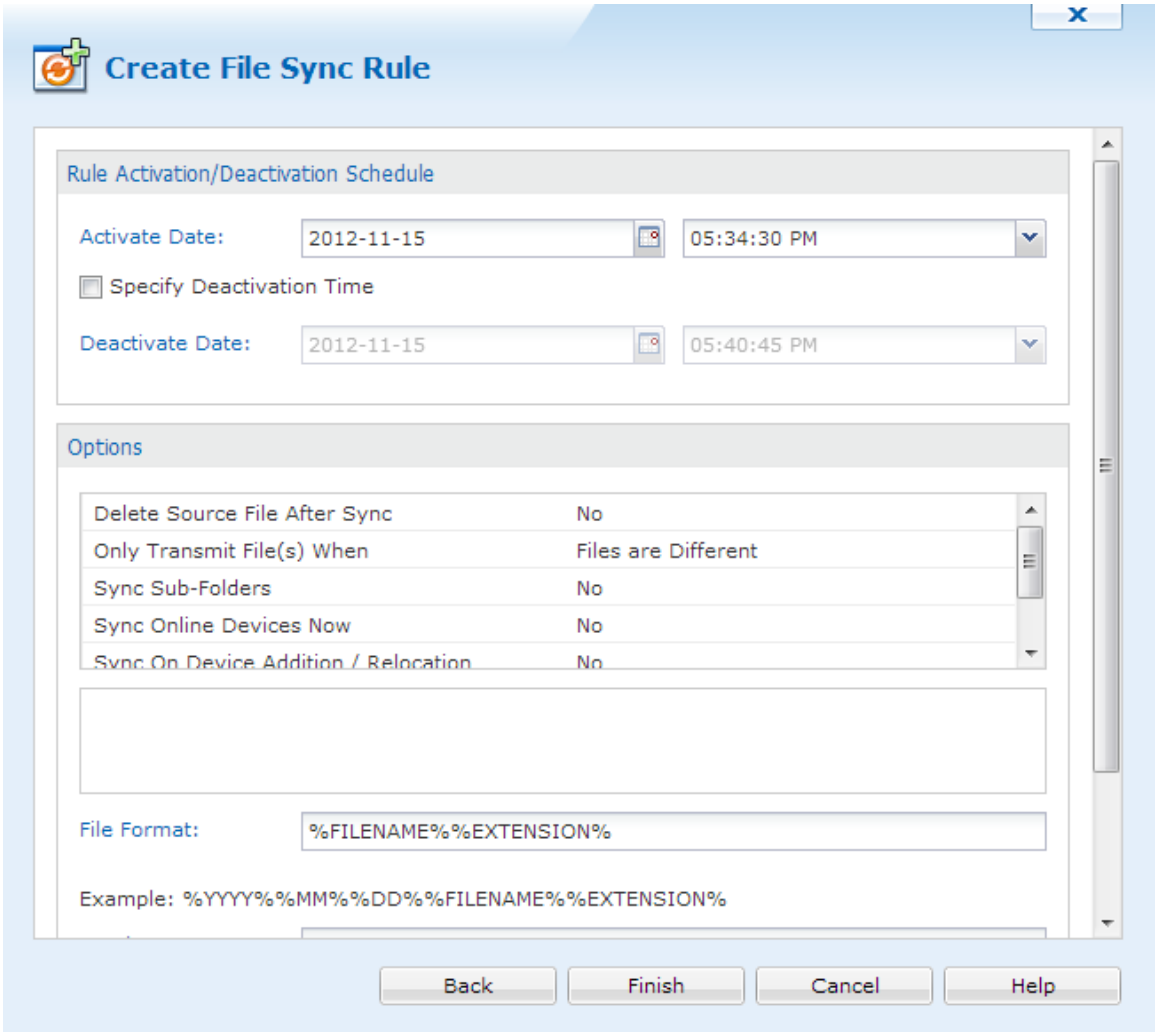
5. Review summarized information.

   Review information on the **file sync rule summary page**. This page gives you an opportunity to review the settings of the file sync rule before committing them. If you wish to make any corrections, click the **Back** button.



Summary page

6. Advanced Options



File synchronization options

The following table describes the file synchronization options on this page of the Create File Sync Rule Wizard:

Field Name	Description
Delete Source File After Sync	(This applies only to upload rules.) When selected, the source file(s) on the device are transmitted to the server and then deleted from the device.

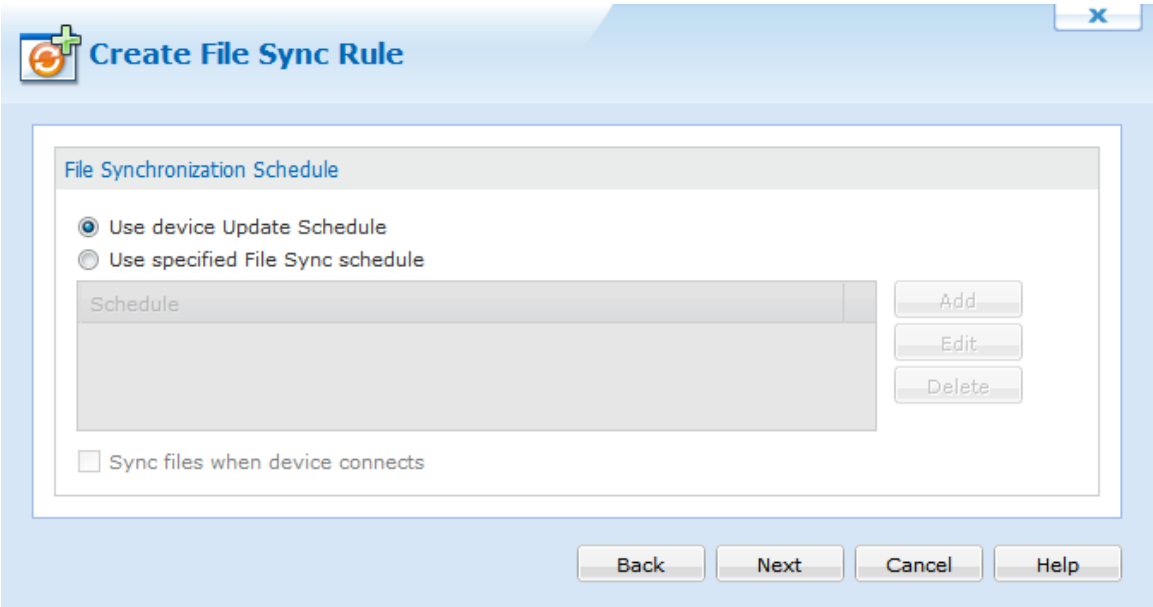
Field Name	Description
Only Transmit File (s) when	• The **Always Transmit** option will cause file(s) to be uploaded or downloaded regardless of whether or not the source and target are different or the same. • The **Files are different** option will cause file(s) to be uploaded or downloaded only if the source file is different from the destination file. • The **Source file is newer** option will cause file(s) to be uploaded or downloaded only if the source file has a more recent date-time stamp. • The **Destination file does not exist** option will cause file(s) will cause file(s) to be uploaded or downloaded only if the destination file does not exist.
Sync Sub-Folders	Synchronize files in sub-folders in addition to the files located in the target folder
Sync Online Devices Now	File synchronization will be executed immediately following the completion of the wizard for online devices.
Sync On Device Addition or Relocation	Perform file synchronization when a device is added or relocated to a device tree group for which this rule has been configured This setting is useful to easily invoke file synchronization when a device is moved from one group to another in the device tree.
Network Restriction	Restrict whether file synchronization should take place over cellular data networks (i.e. GPRS)
Upload File Name Format	Allows you to customize the names of the files that are uploaded from the devices For example, you can augment a file name with the date-time stamp of when it was uploaded. These are available file-name macros: • **%YYYY%** is for the year (e.g. 2006). • **%MM%** is for the month of year (e.g. 12 is December). • **%DD%** is for the day of month (e.g. 31). • **%H%** is for the hour in the 24-hour format (e.g. 14). • **%M%** is for the minutes (e.g. 30). • **%S%** is for the seconds (e.g. 55). • **%FILENAME%** is for the original file name (e.g. `mylogfile`). • **%EXTENSION%** is for the original file extension (e.g. `.txt`).
Use Common Cache Mode	The option to use the new, advanced caching mode of the files being disseminated is applicable only when syncing files from the server to the device. This option is set to **Yes** by default. When enabled, a single, shared, cached copy of each file being disseminated is stored on the Deployment Server. If you are experiencing issues with file synchronization, set this option to **No.**

File Synchronization Schedules

The file synchronization schedule specifies when the Deployment Server(s) should check device(s) for synchronization.

If the Deployment Server identifies an inconsistency, such as a mismatch in the file size or finds the new file, the Deployment Server will act according to the file sync rule.

By default, the device synchronization schedule, specified by the add devices rule used to add the devices to the system, is selected for file synchronization. You may add, edit or delete the custom schedule using the following dialog box.



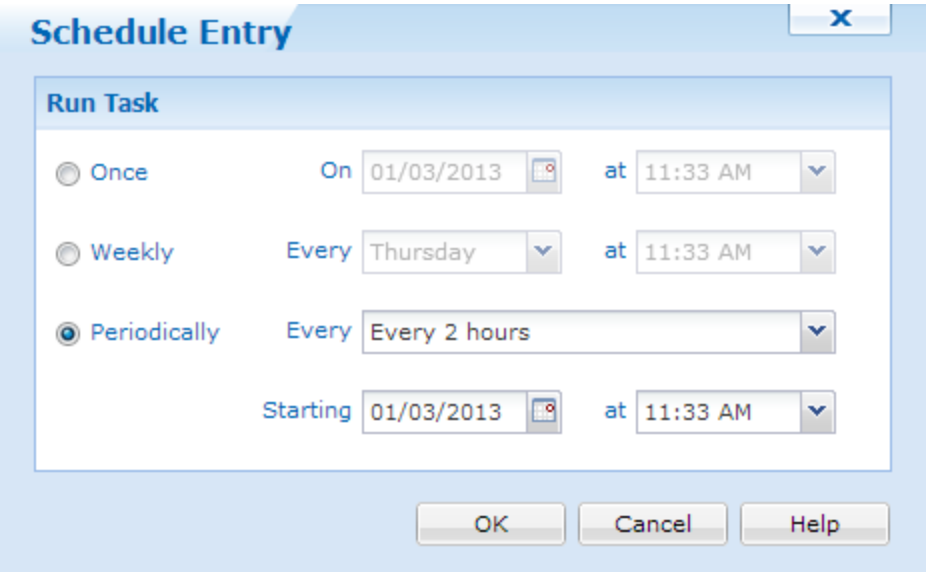
Create File Sync Rule Wizard dialog box

The following table describes the fields of the Create File Sync Rule Wizard dialog box.

Field Name	Description
Add	Specify your own file synchronization intervals. When you select **Add,** the **Schedule Entry** dialog box is displayed. **EXAMPLE:** To sync twice a week (Monday at 06:00 and Friday at 19:00), create two weekly schedule entries.
Edit	Select **Edit** to modify an existing schedule entry. The **Schedule Entry** dialog box is will be displayed.
Delete	Permanently remove a file sync schedule entry from the dialog box
Sync Files when device connects	Sync whenever devices under this rule connect to a Deployment Server (i.e. transition from offline to online)

Schedule Entry

The **Schedule Entry** dialog box allows you to specify schedule entries as one-time or periodic events.



Schedule Entry dialog box

Field Name	Description
Once	Device will check for file synchronization once at the specified date and time.
Weekly	Device will check for file synchronization once a week, on a specified day and time.
Periodically	Device will check for file synchronization periodically at the specified interval from the set, start date-time.

Creating Data Collection Rules on iOS Devices

The Data collection rule for iOS allows administrators to collect location data from iOS devices that have a Device Agent installed.

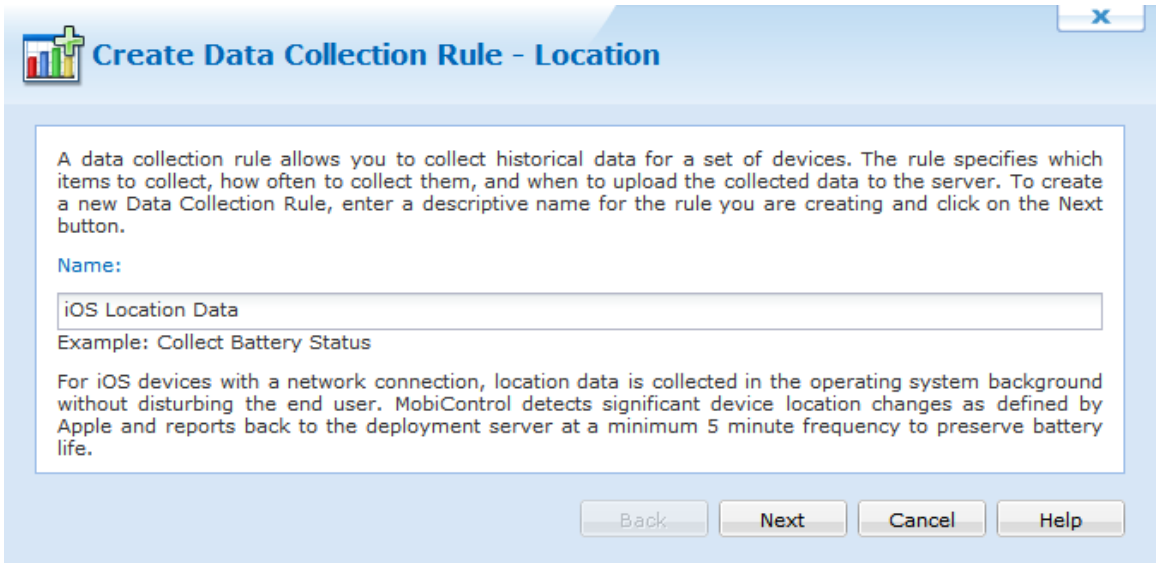
NOTE:

With devices that do not have a SIM card, location data cannot be collected if a Wi-Fi hotspot is not reachable. This occurs because location services uses a GPS signal, cell tower location and Wi-Fi hotspots to determine approximate location. This only affects both the iPod touch and the iPad (Wi-Fi only).

The following series of steps describes how to use the Create Data Collection Rule Wizard to create a data collection rule:

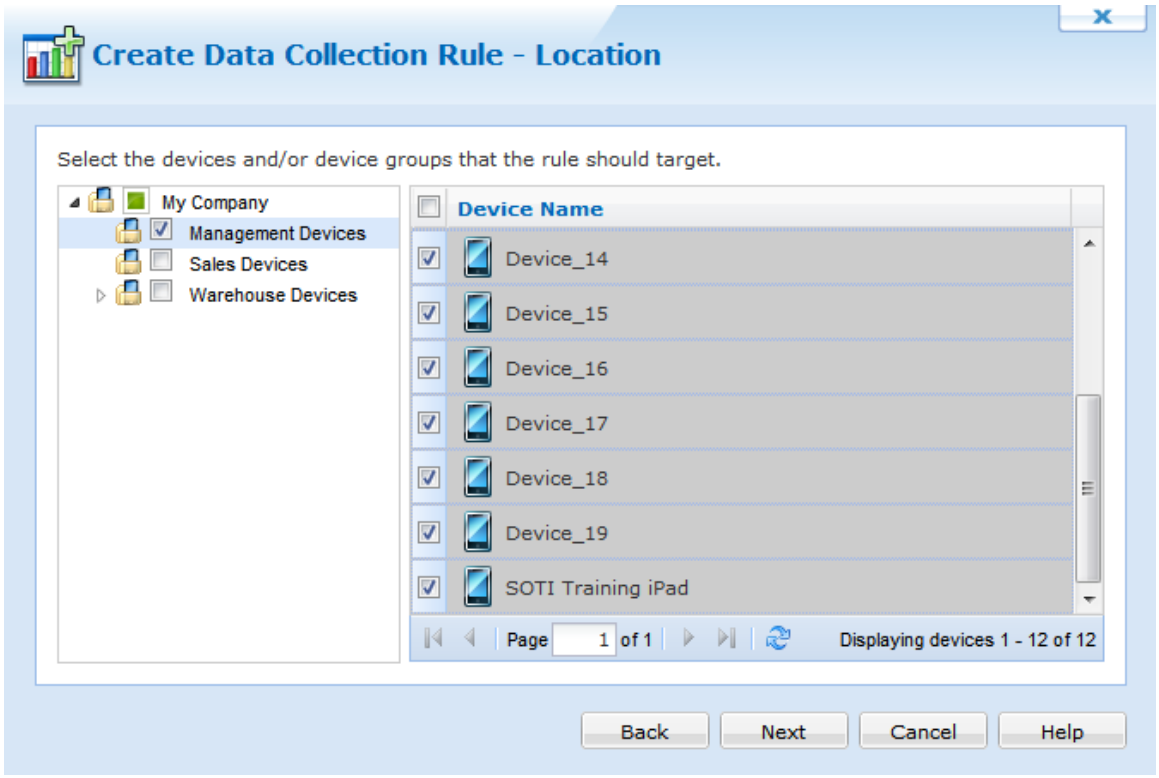
1. Start the wizard.

   From MobiControl Manager, select the Rules view (tab), then click **Rule,** click **Create Rule,** and click **Data Collection Rule**. Enter a meaningful name for your new data collection rule and then click **Next**.



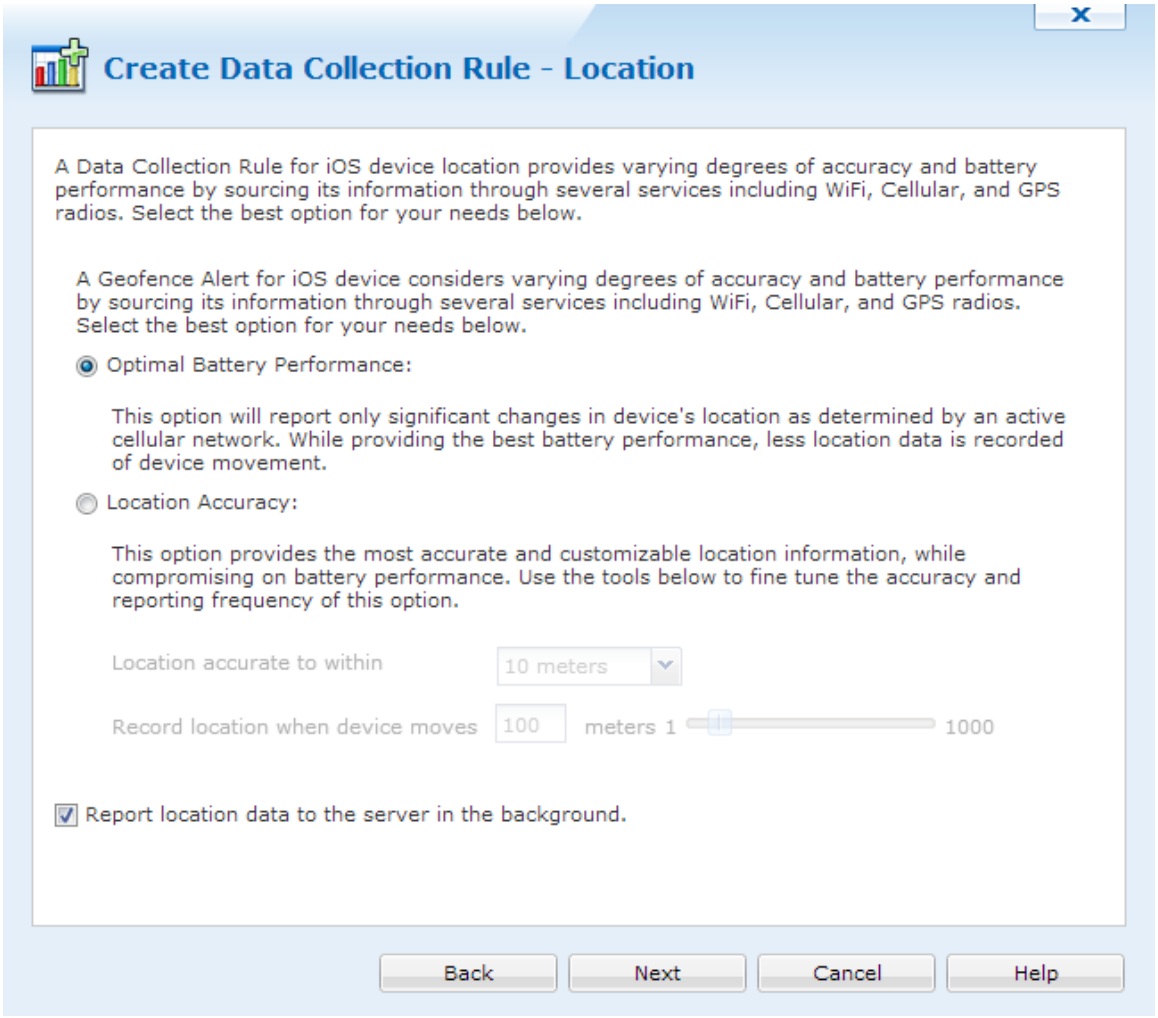
2. Select devices.

   Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



3. Configure the Collection Type.

Choose the collection type that is wanted to be used. We can select two types of collection: Optimal Battery Performance or Location Accuracy.



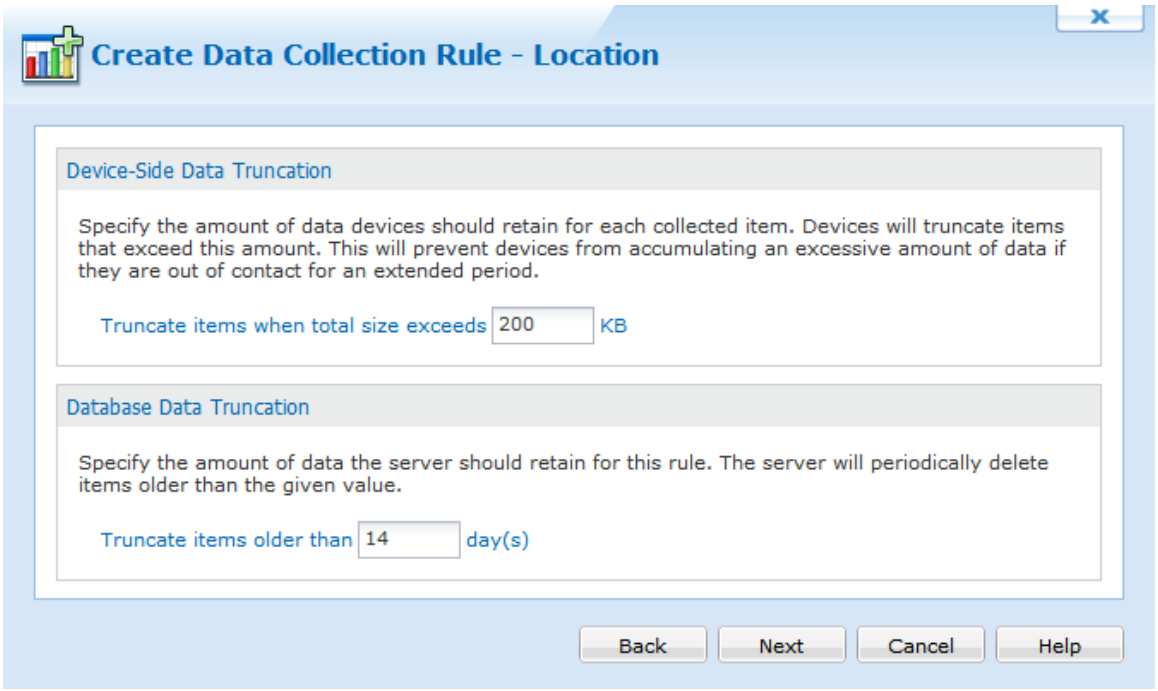
Section Name	Description
Optimal Battery Performance	Selecting this option will report the device's location based on any significant change. This uses a cellular network rather than a GPS signal. If a device has not changed cellular towers, the device may look like it is not moving. Using this causes highly inaccurate locations to be reported, as it may appear to be jumping around a map.
Location Accuracy	Selecting this option will use all available resources for the iOS device. This includes GPS and other location based services. Using the GPS causes a lot of strain on the battery. Use this if having the most pin point accuracy is more important than battery life.
Report location	Selecting this will allow the device to send it's location data back to

Section Name	Description
data to the server in the background	MobiControl through APNS. If not checked, users will have to open the device agent to send location data back to the server.

After entering your choice(s) in the above dialog box, click the **Next** button.

4. Configure data truncation settings.

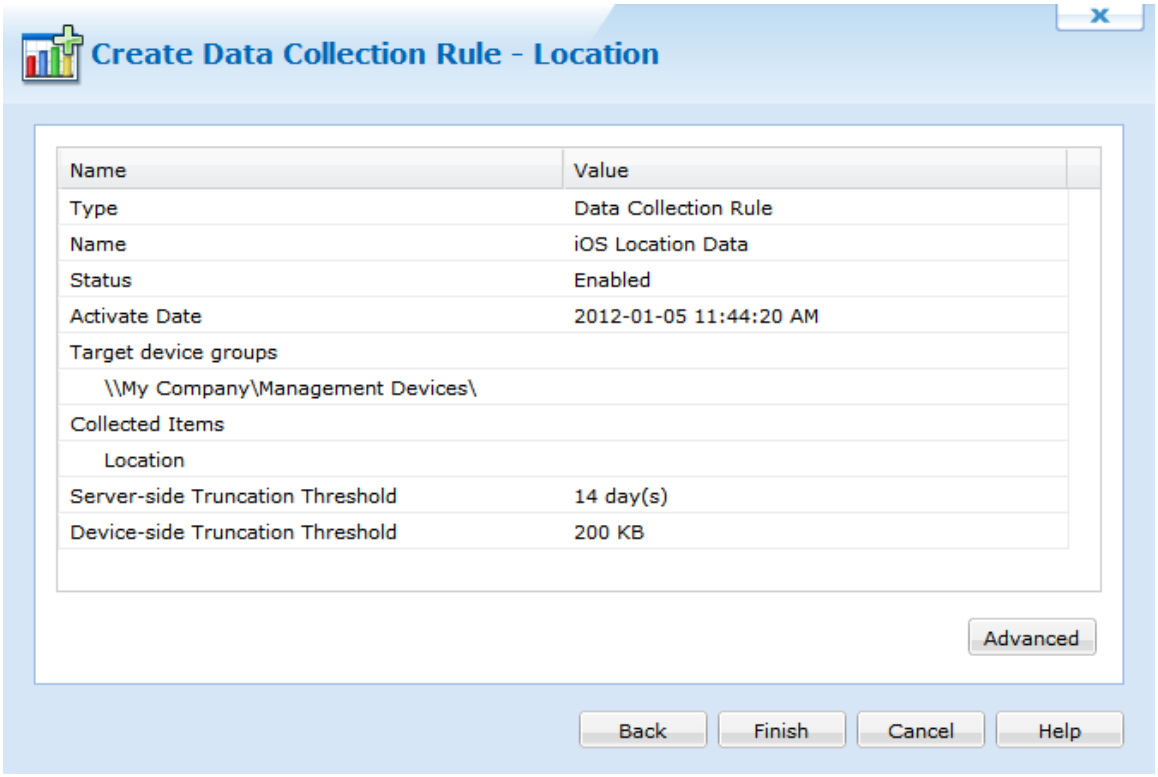
Choose the size of the data being collected. This helps control memory used on the device and the number of days you would like to retain the data in the database.



Section Name	Description
Device-Side Data Truncation	Specify the maximum size of data to be stored from the data collection ruleon the device(s).
Database Data Truncation	Specify the number of day(s) that you would like to retain the information in your database. Data collected older than the number of days listed will be deleted from the database

After entering your choice(s) in the above dialog box, click the **Next** button.

5. Review the summarized information.



The data collection rule can be deployed real-time or at a pre-set time. The data collection rule, although set to be activated at a scheduled time, can also be set to be deactivated. The deactivation setting is optional.

Click **Finish** to complete the wizard.

iOS Alert Rules

Alert Rules allow Administrators to be notified when events of interest arise on the system. This notification system allows Administrators to quickly and effortlessly communicate an event message to large groups of people via email, and notifies users via the MobiControl Manager Alert tab. For every type of scenario, whether it is a Rule Change or a Device Error, the system will rapidly deliver your message to a designated audience.

NOTE:

The Deployment Server must be online in order for Alerts to be generated and sent out.

The MobiControl Web Console allows you to create Alerts based on the Devices Operating System (OS). Some Alerts are specific to the OS Tab that has been selected . For detailed information on the Alerts Available please see below.

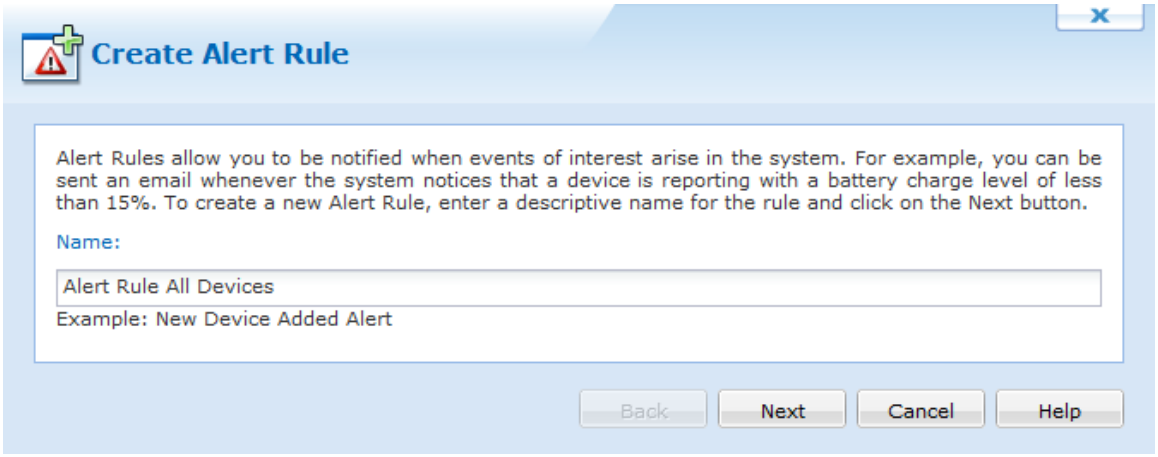
Type	Description
Device Event	Trigger alerts based on an assortment of device specific conditions.
Device Status and Custom Data	Trigger alerts based on Custom Data vales that you have configured.
Geofence Event	Trigger alerts based on devices entering or exiting geofenced areas.

The steps below describe how the Create Alert Rule Wizard can be used to create an Alert using the MobiControl Web Console:

1. Start the wizard.

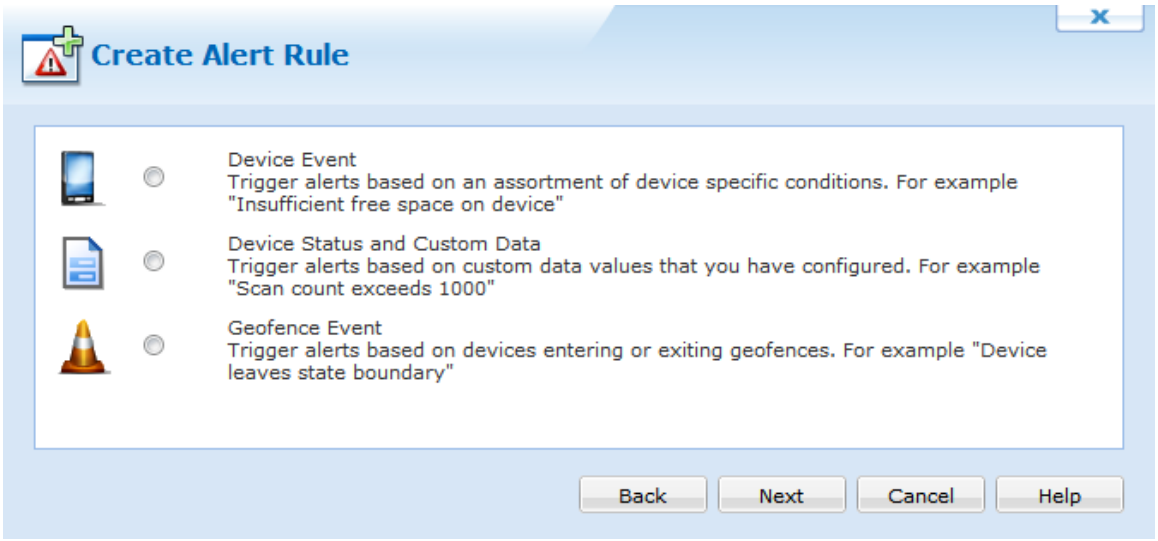
   Select the All OS's Tab, then select the Rules tab, then Right click on the **Alert Rule** folder, and select **Create Alert Rule**. The first page of the Create Alert Rule Wizard will be displayed.

   Enter a descriptive name for the Alert Rule you are creating and click **Next.**



First page of the Alert Rule Wizard

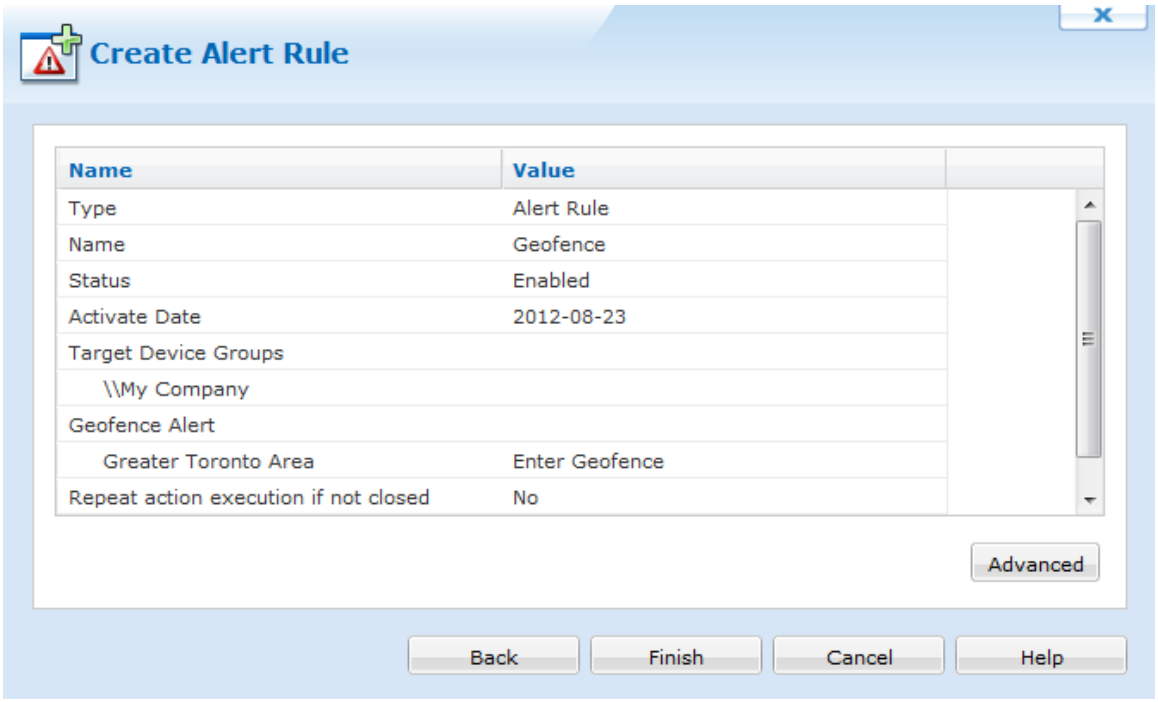
2. Select the Alert Rule Type.



Select the Alert Rule Type and click Next. After Clicking Next you will be asked to specify the Alert Options for the selected Alert Type. Select the type of alert below for more information on the Alert Options available.

Type	Description
Device Event	Trigger alerts based on an assortment of device specific conditions.
Device Status and Custom Data	Trigger alerts based on Custom Data vales that you have configured.
Geofence Event	Trigger alerts based on devices entering or exiting geofenced areas.

3. Review the summarized information.



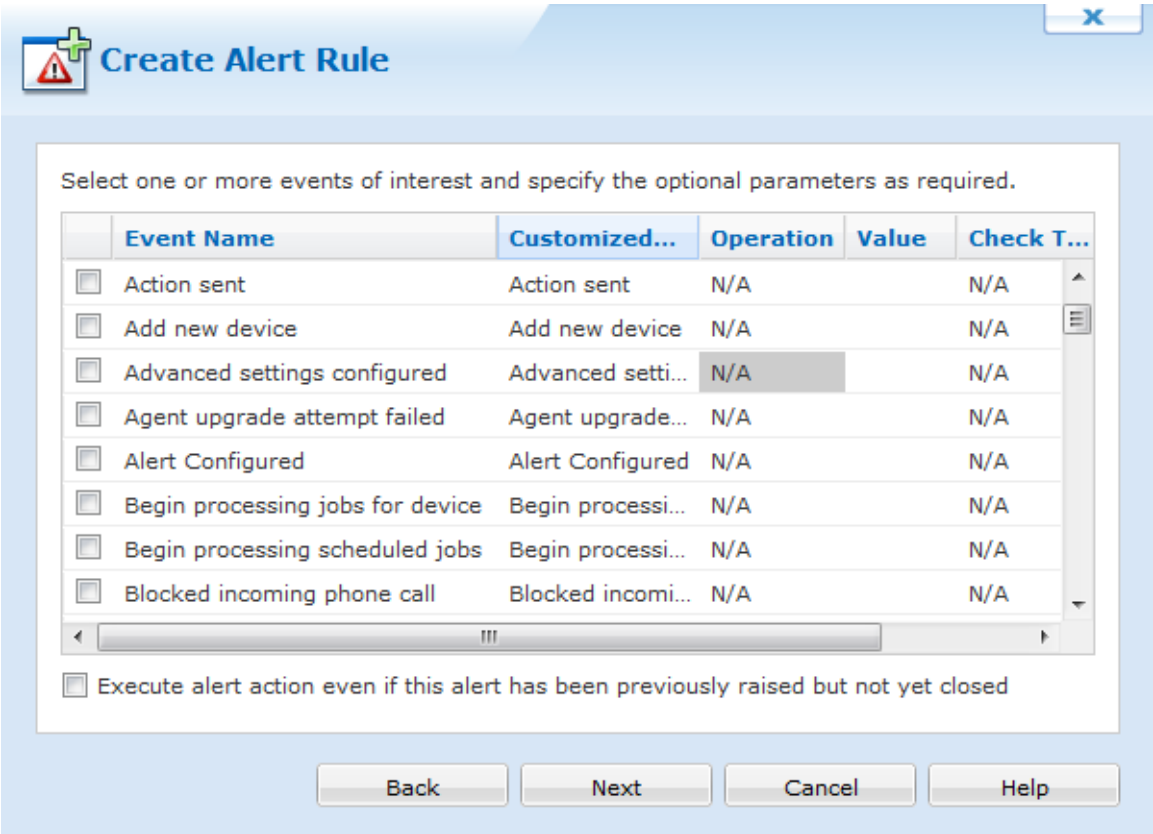
Click **Finish** to complete the wizard.

Device Event

A Device Event is an alert triggered based on an assortment of device specific conditions. See below for a full list.

Windows Devices

The Device Events listed below are specific to Windows Devices.



Device Event Notification Selection Window

The below table shows all available default Device events:

Log Event	Description
<Custom Alert>	Triggers an alert based on a custom alert
Add new device	Triggers an alert based on when a new device is added
Advanced settings configured	Triggers an alert based on when advanced settings are configured
Agent upgrade Attempt failed	Triggers an alert based on when an agent upgrade attempt failed
Alert Configured	Triggers an alert based on when an alert is configured
Begin processing scheduled jobs	Triggers an alert based on when processing scheduled jobs begin
Blocked incoming phone call	Triggers an alert based on when an outgoing phone call is blocked
Change password failure	Triggers an alert based on when a password change failed
Change password success	Triggers an alert based on when a password

Log Event	Description
	change was successful
Custom Data configured	Triggers an alert based on when custom data is configured
Custom log	Triggers an alert based on when custom logs are created
Data Collected	Triggers an alert based on when data is collected
Data Collection configured	Triggers an alert based on when data collection is configured
Dependent packages not installed	Triggers an alert based on when dependent packages are not installed
Device connected	Triggers an alert based on when a device is connected
Device disabled	Triggers an alert based on when a device is disabled
Device disconnected	Triggers an alert based on when a device is disconnected
Device Enabled	Triggers an alert based on when a device is enabled
Device has not been connected for %VALUE% minutes	Triggers an alert based on when a device has not been connected for %VALUE% minutes
Device Manually relocated	Triggers an alert based on when a device is manually relocated
Device relocated	Triggers an alert based on when a device is automatically relocated
Device security configured	Triggers an alert based on when device security is configured
Error creating file on device	Triggers an alert based on when there was an error creating a file on a device
Error message received from device	Triggers an alert based on when an error message was received from a device
Error receiving file	Triggers an alert based on when there was an error receiving a file
Error sending file	Triggers an alert based on when there was an error sending a file
Error sending message	Triggers an alert based on when there was an error sending a message
Error writing to file on device	Triggers an alert based on when there was an error writing to a file on a device
Exchange ActiveSync configured	Triggers an alert based on when Exchange ActiveSync is configured

Log Event	Description
File synchronization failed	Triggers an alert based on when a file synchronization failed
File synchronization was aborted by pre-sync script	Triggers an alert based on when file synchronization was aborted by pre-sync script
File(s) synchronized	Triggers an alert based on when file(s) are synchronized
File synchronization failed	Triggers an alert based on when file synchronization failed
Geofencing Configured	Triggers an alert based on when Geofencing is configured
Inaccurate device date-time detected	Triggers an alert based on when there is inaccurate date-time detected on a device
Incompatible platform, processor or os version	Triggers an alert based on when there is incompatible platform, processor or os version
Installation aborted by user	Triggers an alert based on when installation is aborted by user
Installation was aborted by install script	Triggers an alert based on when installation was aborted by install script
Insufficient free space on device	Triggers an alert based on when there is insufficient free space on device
Invalid device software version	Triggers an alert based on when invalid device software version is detected
Invalid message received from device	Triggers an alert based on when an invalid message is received from device
Lockdown removed	Triggers an alert based on when the lockdown removed
Logon failure	Triggers an alert based on when logging onto a device fails
Logon success	Triggers an alert based on when logging onto a device is successful
Multiple packages with the same name in job list	Triggers an alert based on when there are multiple packages with the same name in job list
No Package ID in installation report	Triggers an alert based on when there is no Package ID in installation report
Package file is corrupted	Triggers an alert based on when a package file is corrupted
Package file not found	Triggers an alert based on when a package file not found
Package uninstalled	Triggers an alert based on when a package is uninstalled

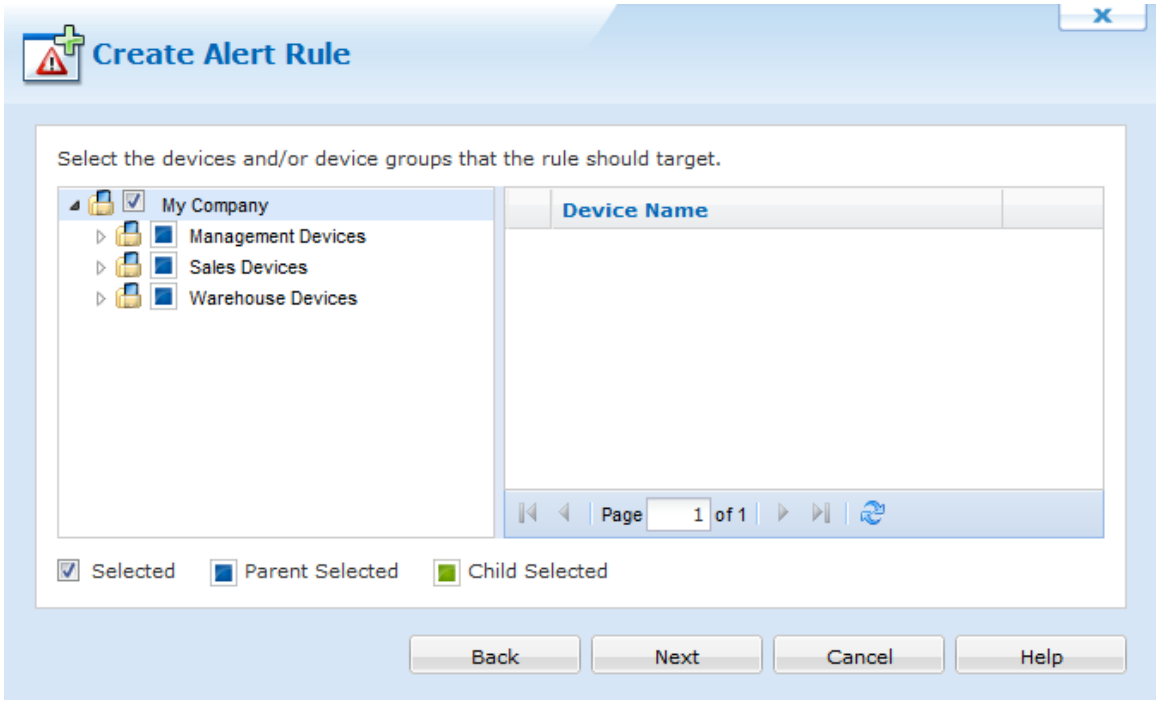
Log Event	Description
Package with higher version number already installed on the device	Triggers an alert based on when a package with a higher version number is already installed on the device
Pending jobs cannot be processed until device user is authenticated	Triggers an alert based on when pending jobs cannot be processed until device user is authenticated
Process Learned	Triggers an alert based on when processes are learned
Processed successfully	Triggers an alert based on when processed successfully
Remote Control	Triggers an alert based on when a device is remote controlled
Stopped illegal process	Triggers an alert based on when an illegal process is stopped
Time Sync Configured	Triggers an alert based on when time sync is configured

The following list of variables are only available within the Customized Alert Message field:

Type	Description
%RULENAME%	The name of the rule
%PACKAGENAME%	The name of the package

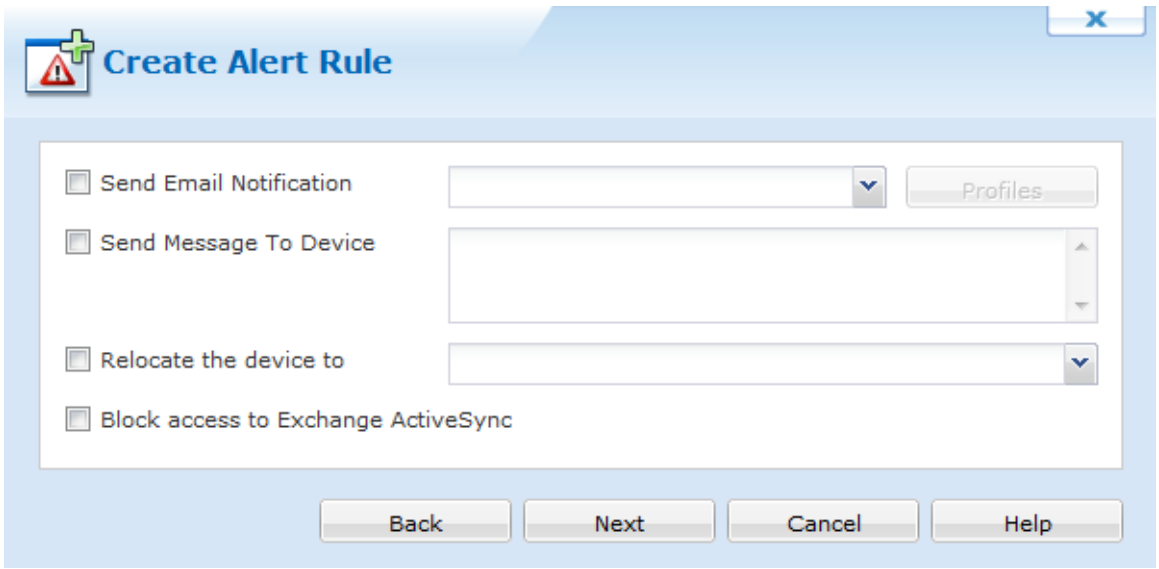
Select devices.

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



Select Actions.

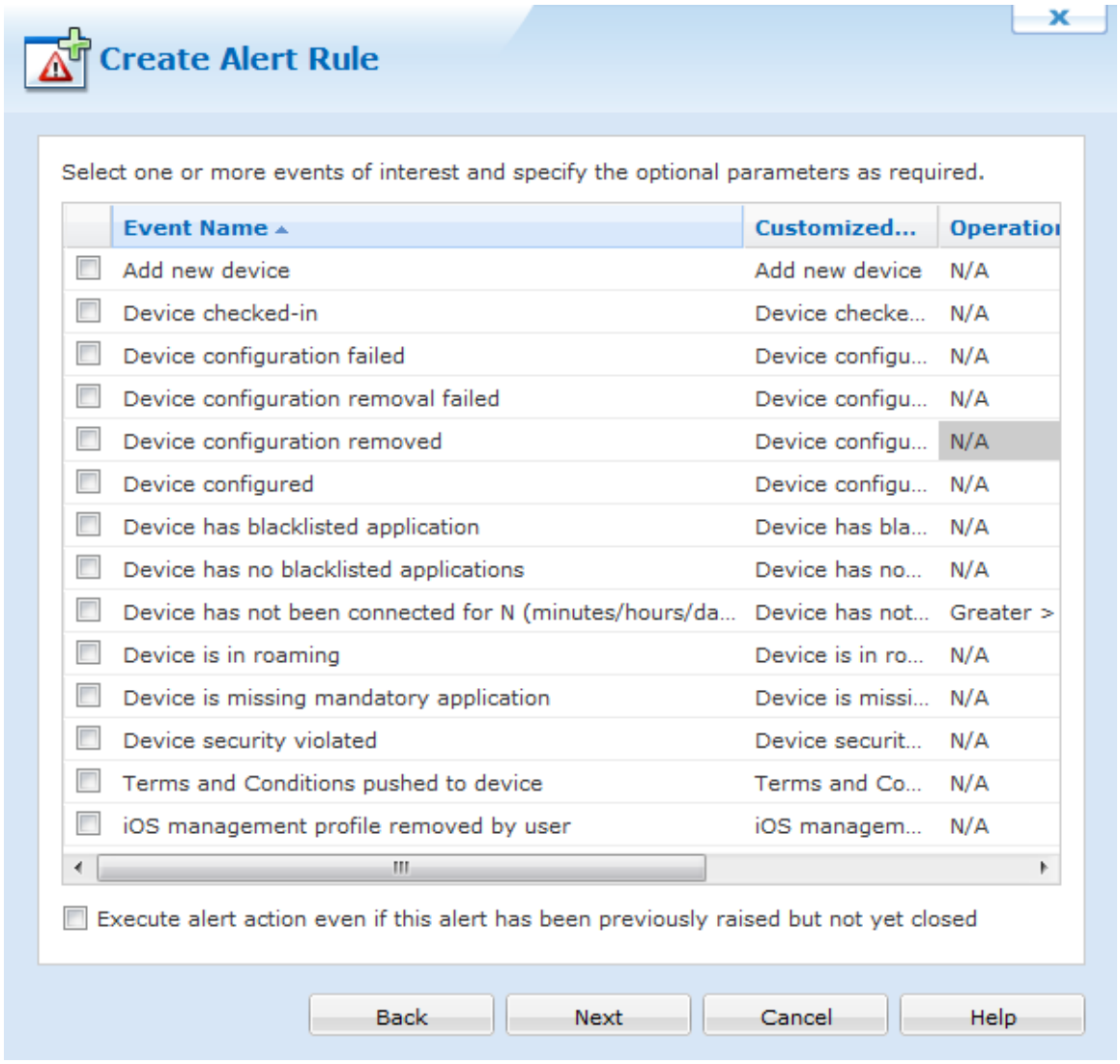
Select any action to be done when the alert has been triggered. MobiControl gives the option to send an email to administrator groups, send a message to the device, relocated the device to a different group, or block access to Exchange Active Sync. One or many of these options can be selected.



After selecting your Profile and Actions, click Next and continue the Alert Rule Wizard here.

iOS Devices

The Device Events listed below are specific to iOS Devices.



Device Event Notification Selection Window

Severity is set to Minor by default and can be altered.

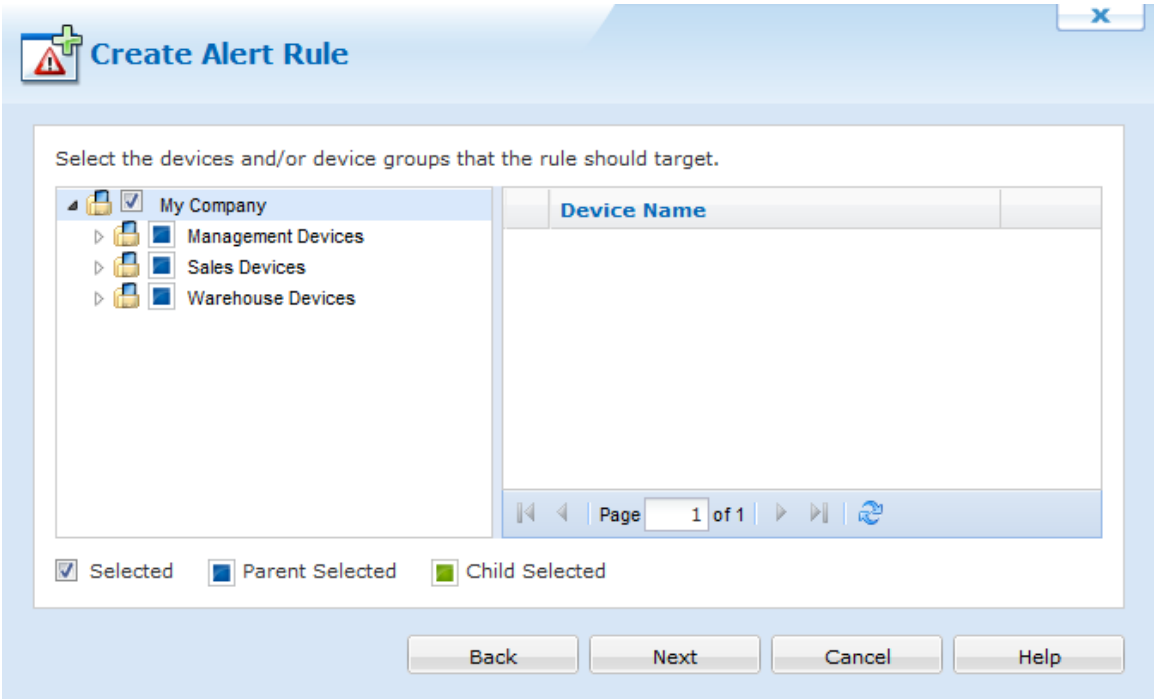
The below table shows all available default Device events:

Log Event	Alert Message (Customisable)
Add new device	A new device has been added.

Log Event	Alert Message (Customisable)
Device Checked-in	A device has checked-in with the Deployment Server
Device Configuration Failed	Device Configuration Failed
Device Configuration Removal Failed	Device Configuration Removal Failed
Device Configuration Removed	Device Configuration Removed
Device Configured	Device Configured
Device has blacklisted application	Device has blacklisted application
Device has not been connected for N (minutes/hours/days)	Device has not connected to the Deployment Server for N (minutes/hours/days).
Device is Roaming	Device is roaming away from it's home zone.
Device is missing mandatory application	Device is missing mandatory application
Device security violated	Device has been jail broken.
iOS management profile removed by user	A user has removed the iOS management profile from the device.

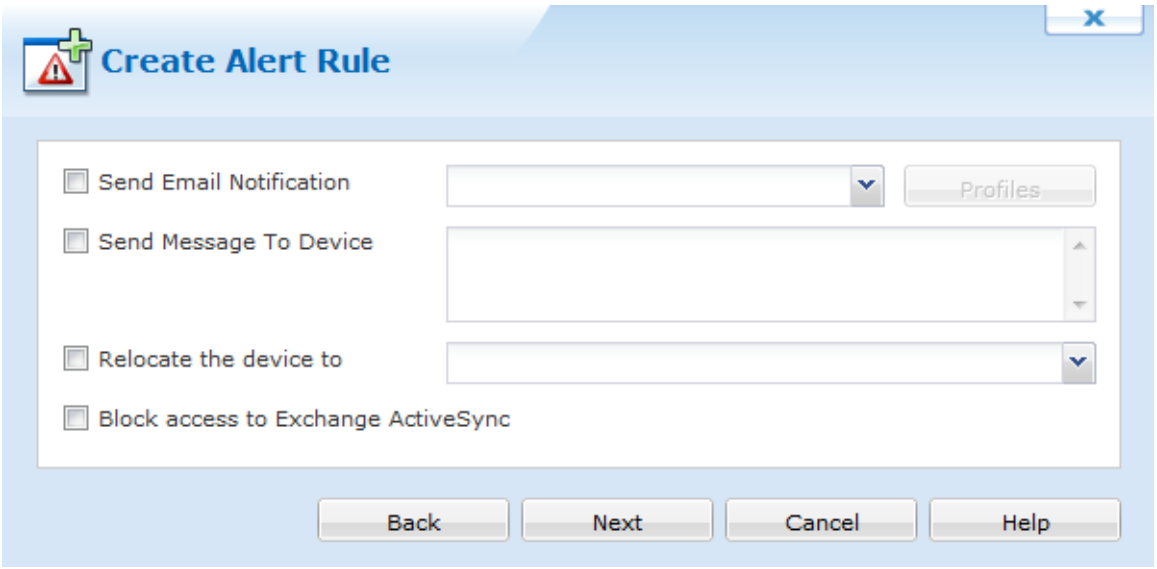
Select devices.

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



Select Actions.

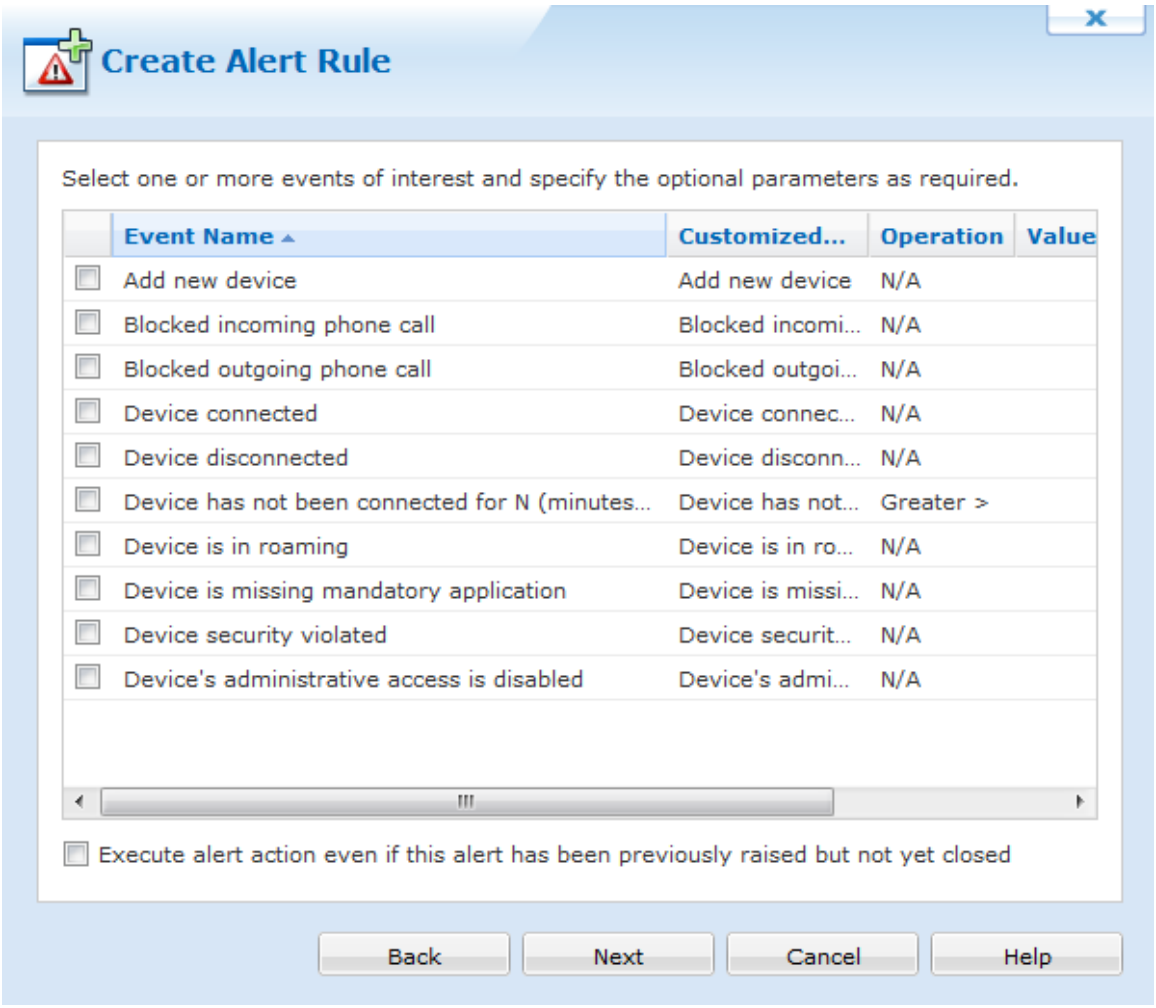
Select any action to be done when the alert has been triggered. MobiControl gives the option to send an email to administrator groups, send a message to the device, relocated the device to a different group, or block access to Exchange Active Sync. One or many of these options can be selected.



After selecting your Profile and Actions, click Next and continue the Alert Rule Wizard here.

Android Devices

The Device Events listed below are specific to Android Devices.



Device Event Notification Selection Window

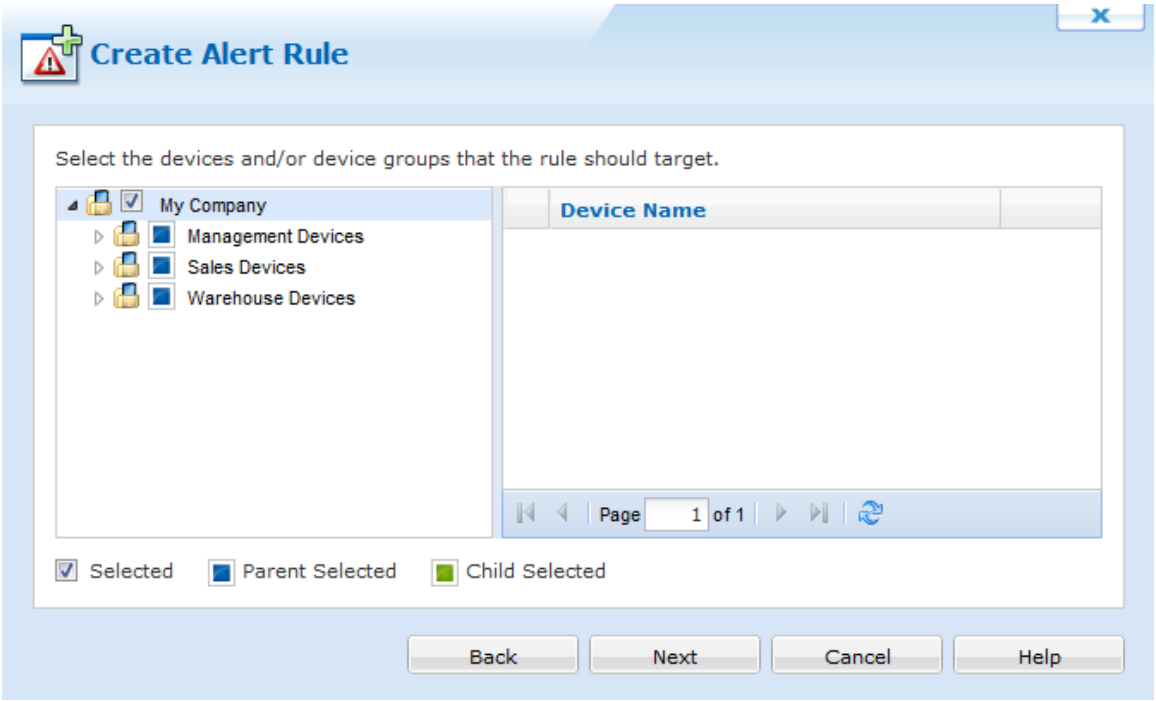
Severity is set to Minor by default and can be altered.
The below table shows all available default Device events:

Log Event	Alert Message (Customisable)
Add new device	A new device has been added.
Blocked incoming phone call	An incoming phone call has been blocked
Blocked outgoing phone call	An outgoing phone call has been blocked
Device Connected	Device has connected to the Deployment Server.
Device Disconnected	Device has disconnected from the Deployment Server.
Device has not been connected for N (minutes/hours/days)	Device has not connected to the Deployment Server for N (minutes/hours/days).
Device is Roaming	Device is roaming away from it's home zone.
Device is missing mandatory application	Device is missing mandatory application

Log Event	Alert Message (Customisable)
Device security violated	Device has been rooted.
Device's administrative access is disabled	The device agent's administrative access has been disabled.
Malware application detected	MobiControl found an application classified as malware
Malware application quarantine	MobiControl placed the application in the quarantine folder
Malware application quarantine reset	The malware application quarantine list has been reset
Malware file detected	MobiControl found a file classified as malware
Malware file quarantine	MobiControl placed the file in the quarantine folder
Malware file quarantine reset	The malware file quarantine list has been reset
Terms and Conditions pushed to device	The terms and conditions have been pushed to the device
URL blocked	An alert triggered when URL is blocked
User accept Terms and Conditions	An alert triggered when a user accepts the Terms and Conditions
User rejected Terms and Conditions	An alert triggered when a user rejects the Terms and Conditions

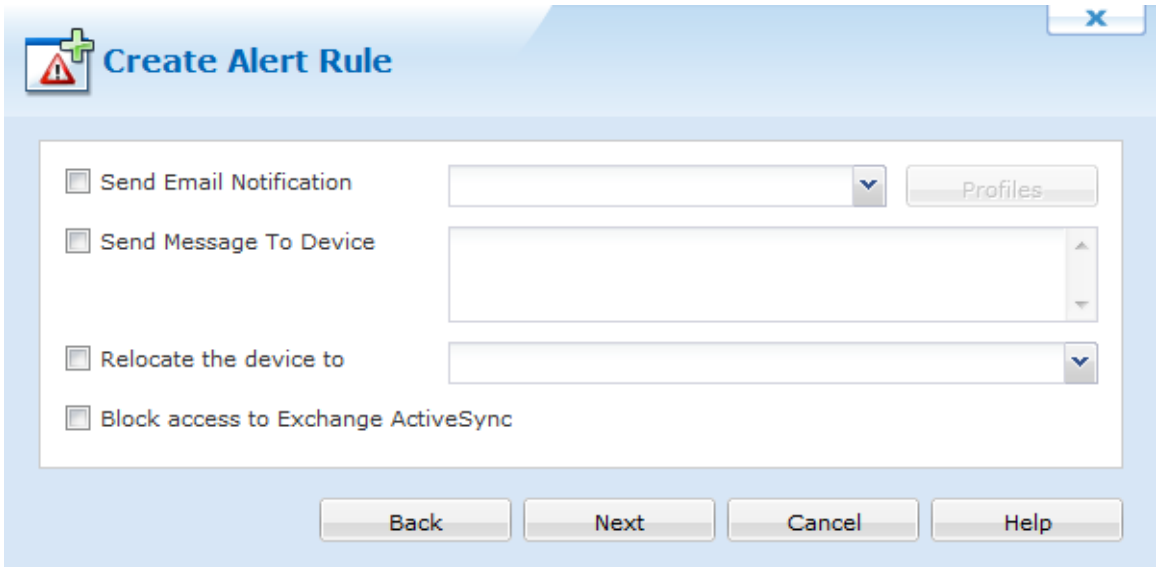
Select devices.

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



Select Actions.

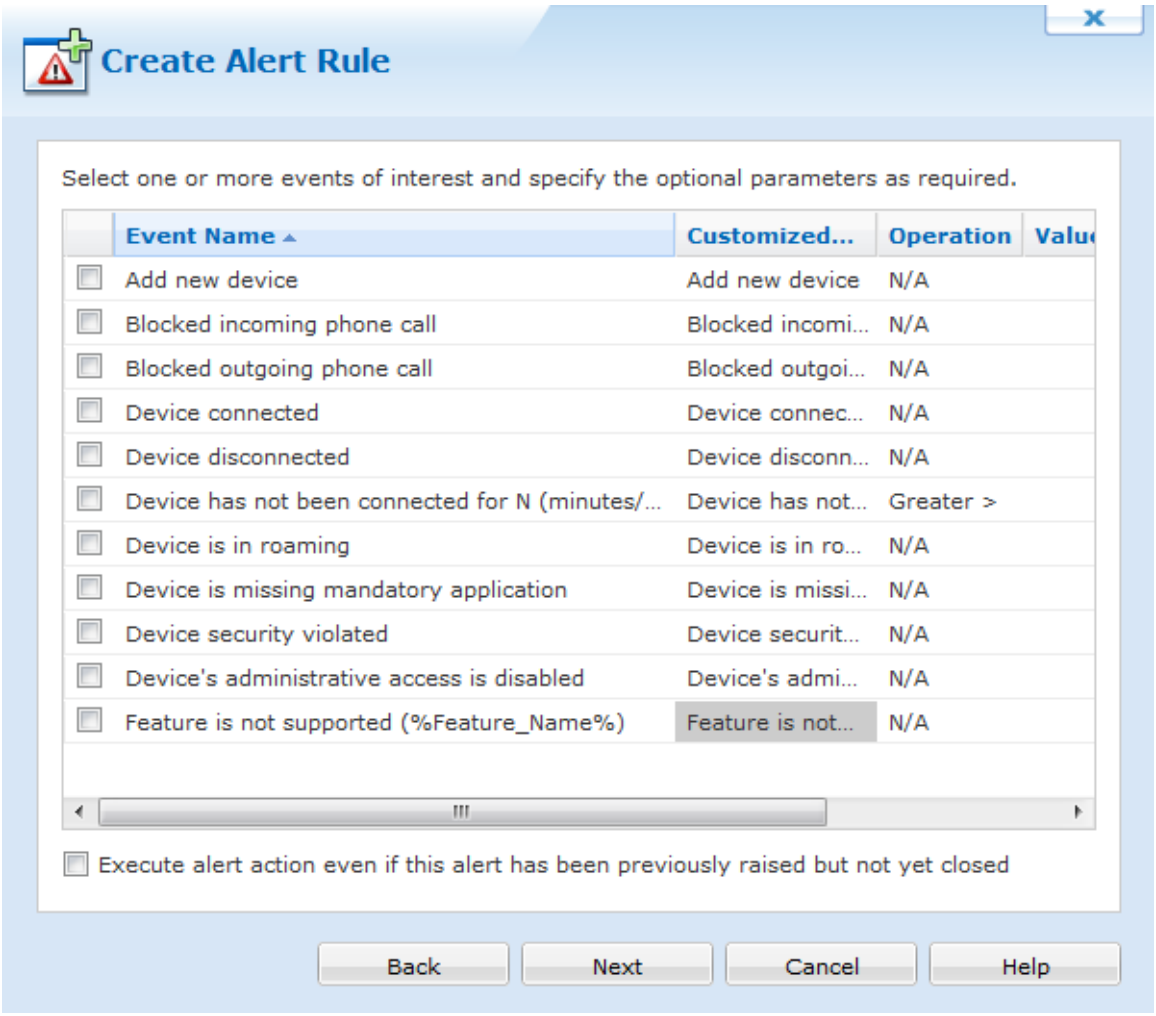
Select any action to be done when the alert has been triggered. MobiControl gives the option to send an email to administrator groups, send a message to the device, relocated the device to a different group, or block access to Exchange Active Sync. One or many of these options can be selected.



After selecting your Profile and Actions, click Next and continue the Alert Rule Wizard here.

Android Plus Devices

The Device Events listed below are specific to Android Plus Devices.



Device Event Notification Selection Window

Severity is set to Minor by default and can be altered.

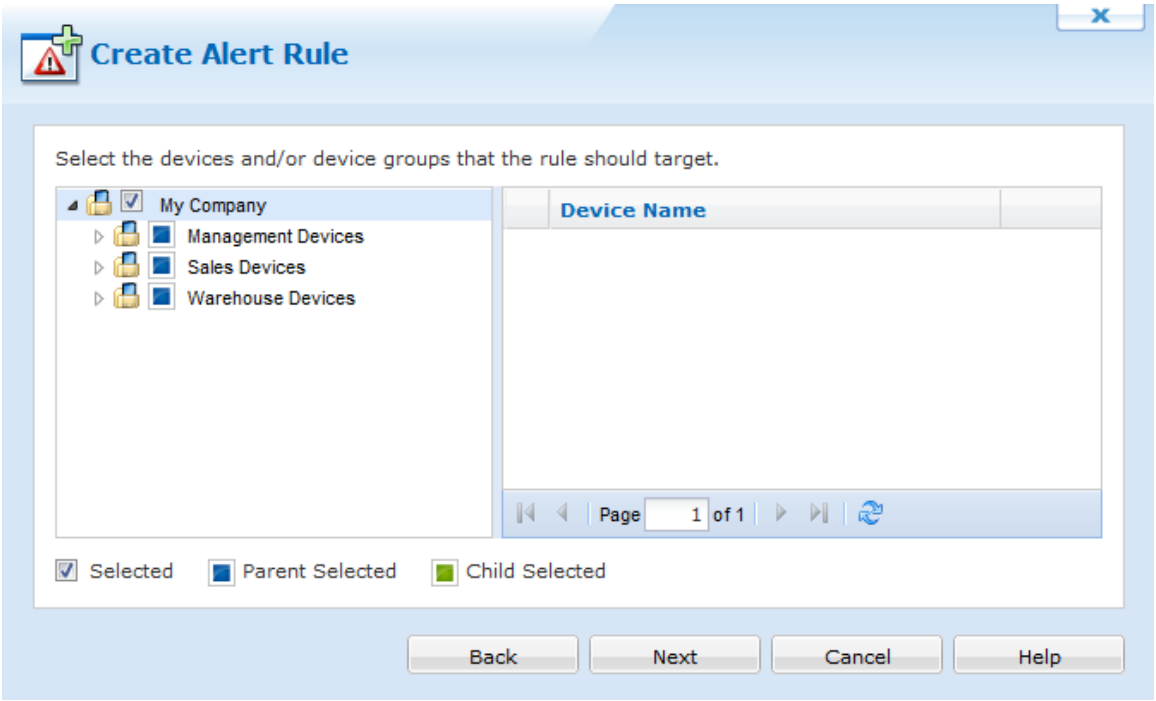
The below table shows all available default Device events:

Log Event	Alert Message (Customisable)
Add new device	A new device has been added.
Blocked incoming phone call	An incoming phone call has been blocked
Blocked outgoing phone call	An outgoing phone call has been blocked
Device Connected	Device has connected to the Deployment Server.
Device Disconnected	Device has disconnected from the Deployment Server.
Device has not been connected for N (minutes/hours/days)	Device has not connected to the Deployment Server for N (minutes/hours/days).
Device is Roaming	Device is roaming away from it's home zone.
Device is missing mandatory application	Device is missing mandatory application

Log Event	Alert Message (Customisable)
Device security violated	Device has been rooted.
Device's administrative access is disabled	The device agent's administrative access has been disabled.
Malware application detected	MobiControl found an application classified as malware
Malware application quarantine	MobiControl placed the application in the quarantine folder
Malware application quarantine reset	The malware application quarantine list has been reset
Malware file detected	MobiControl found a file classified as malware
Malware file quarantine	MobiControl placed the file in the quarantine folder
Malware file quarantine reset	The malware file quarantine list has been reset
Terms and Conditions pushed to device	The terms and conditions have been pushed to the device
URL blocked	An alert triggered when URL is blocked
User accept Terms and Conditions	An alert triggered when a user accepts the Terms and Conditions
User rejected Terms and Conditions	An alert triggered when a user rejects the Terms and Conditions

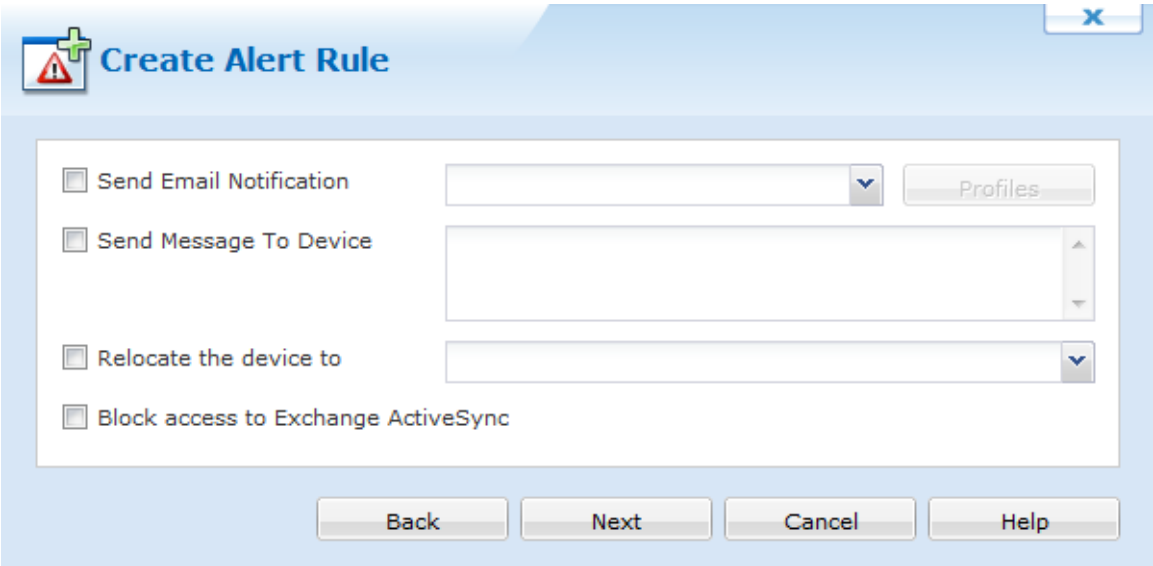
Select devices.

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



Select Actions.

Select any action to be done when the alert has been triggered. MobiControl gives the option to send an email to administrator groups, send a message to the device, relocated the device to a different group, or block access to Exchange Active Sync. One or many of these options can be selected.



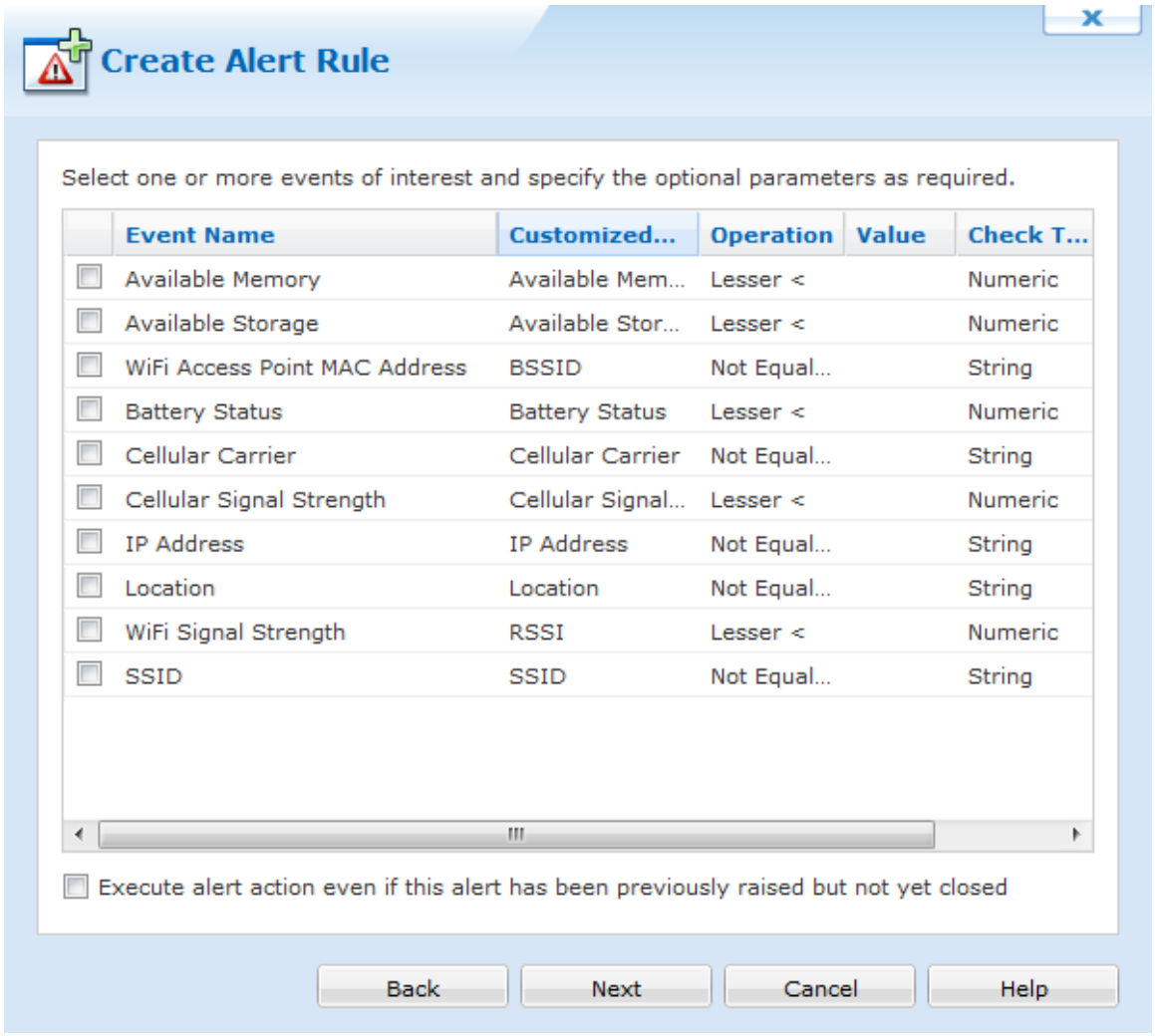
After selecting your Profile and Actions, click Next and continue the Alert Rule Wizard here.

Device Status and Custom Data Event

A Device Status and Custom Data Event is an alert triggered based on an assortment of data values that you have set. See below for a full list.

Windows Devices

The Device Status and Custom Data Events listed below are specific to Windows Devices.



Device Status and Custom Data Event Notification Selection Window

The Operation and Value fields allows to filter out Alerts based on specific values or value ranges. The Operation field specifies at which point an alert will be created for the data value you have specified. Severity is set to Minor by default and can be altered.

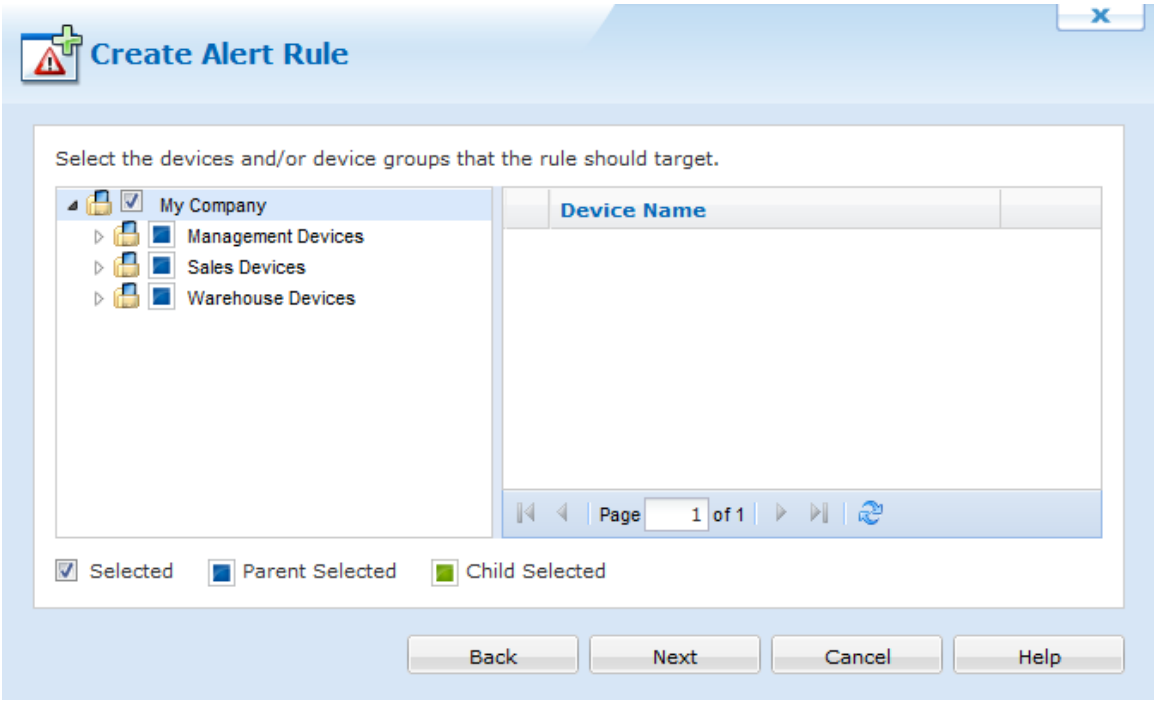
The below table shows all available default Device Status and Custom Data Event events:

Log Event	Description
Available Memory	Triggers an alert based on the numeric value entered for available memory
Available Storage	Triggers an alert based on the numeric value entered for available storage
WiFi Access Point MAC Address	Triggers an alert based on the string value entered for WiFi MAC addresses
Battery Status	Triggers an alert based on the numeric value entered for battery status
Cellular Carrier	Triggers an alert based on the string value entered for cellular

Log Event	Description
	carrier
Cellular Signal Strength	Triggers an alert based on the numeric value entered for cellular signal strength
IP Address	Triggers an alert based on the string value entered for IP Address
Location	Triggers an alert based on the string value entered for location
Wi-Fi Signal Strength	Triggers an alert based on the numeric value entered for Wi-Fi Signal Strength
SSID	Triggers an alert based on the string value entered for SSID

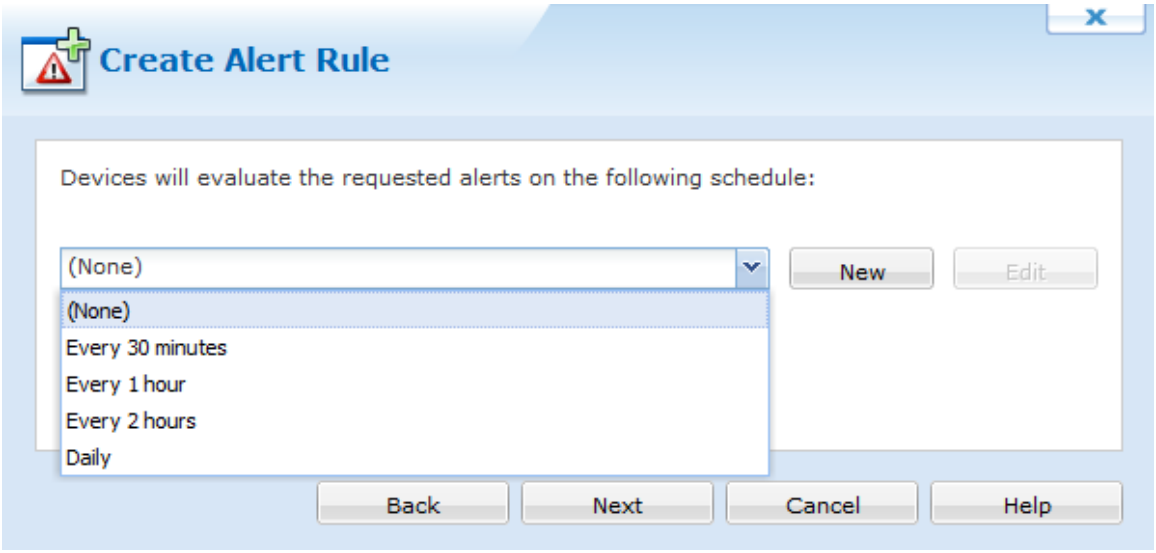
Select devices.

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



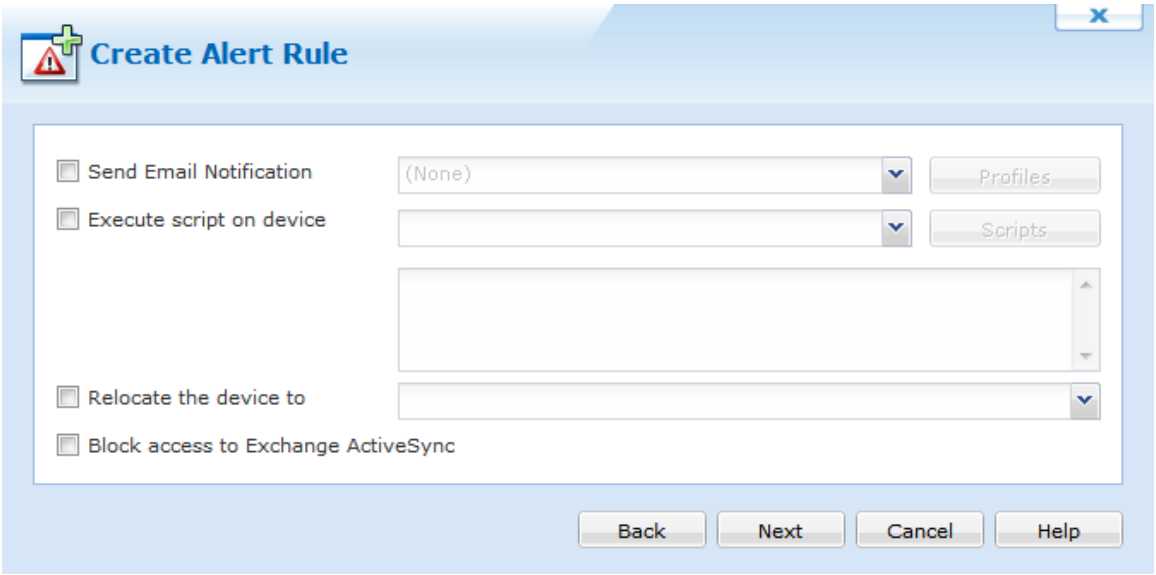
Select Schedule.

Select how frequently the devices should be checked for the requested Alert information. Once you have completed this section, click the **Next** button.



Select Actions.

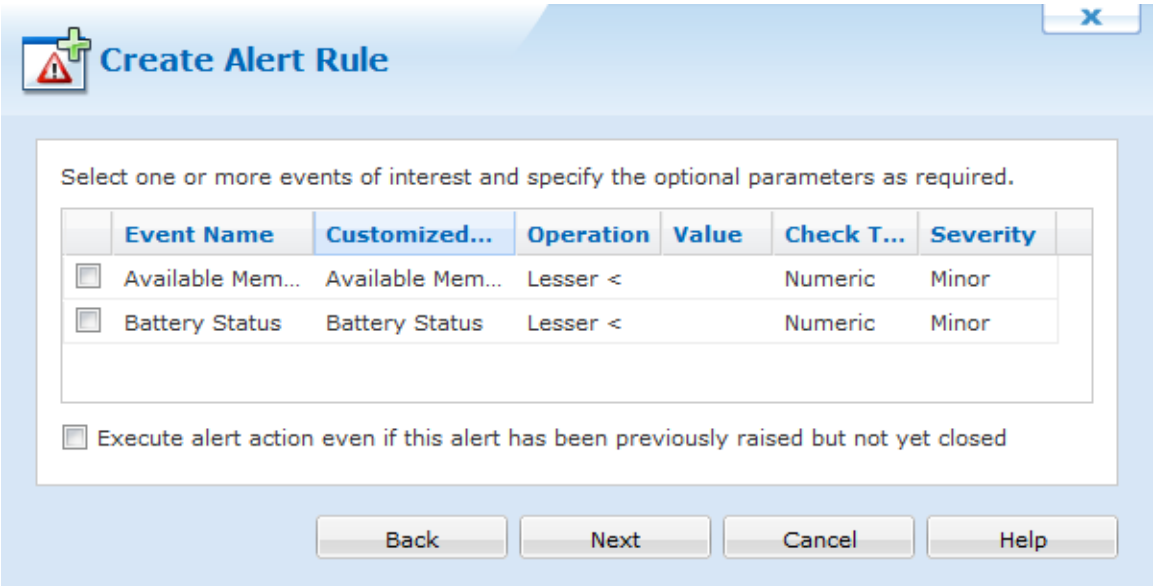
Select any action to be done when the alert has been triggered. MobiControl gives the option to send an email to administrator groups, send a message to the device, relocated the device to a different group, or block access to Exchange Active Sync. One or many of these options can be selected.



After selecting your Profile and Actions, click Next and continue the Alert Rule Wizard here.

iOS Devices

The Device Status and Custom Data Events listen below are specific to iOS Devices.



Device Status and Custom Data Event Notification Selection Window

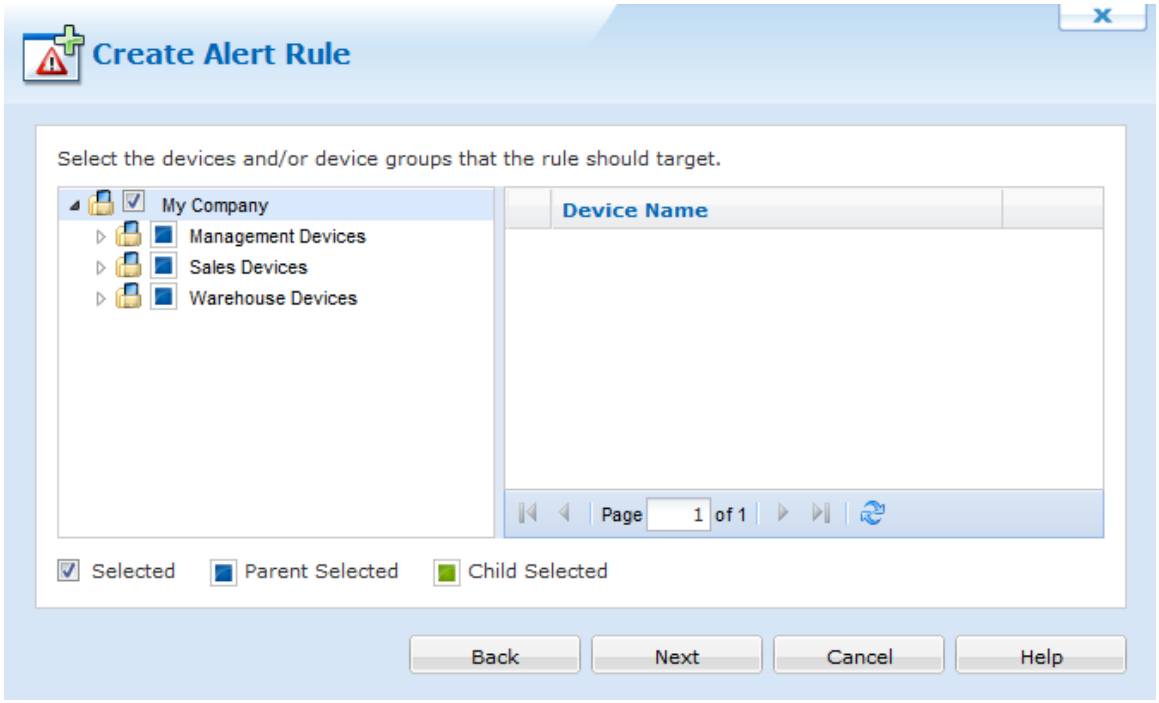
The Operation and Value fields allows to filter out Alerts based on specific values or value ranges. The Operation field specifies at which point an alert will be created for the data value you have specified. Severity is set to Minor by default and can be altered.

The below table shows all available default Device Status and Custom Data Event events:

Log Event	Description
Available Memory	Triggers an alert based on available memory
Battery Status	Triggers an alert based on battery status
Available Storage	Triggers an alert based on available storage
IP Address	Triggers an alert based on IP Address
Cellular Carrier	Triggers an alert based on cellular carrier
Wifi Access Point MAC Address (BSSID)	Triggers an alert based on MAC address
Operating System Version	Triggers an alert based on the device's operating system.

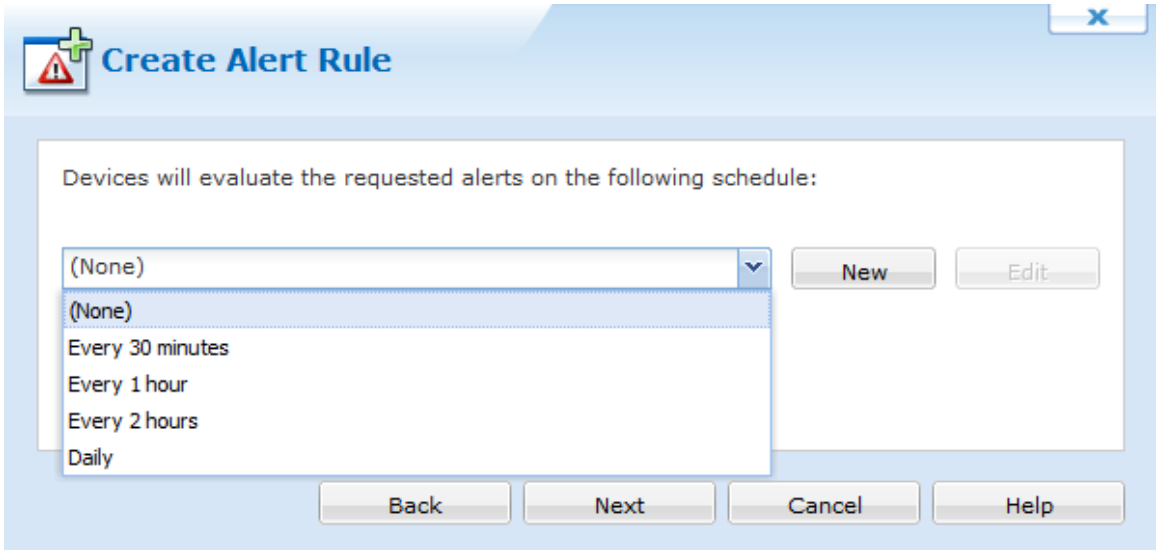
Select devices.

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



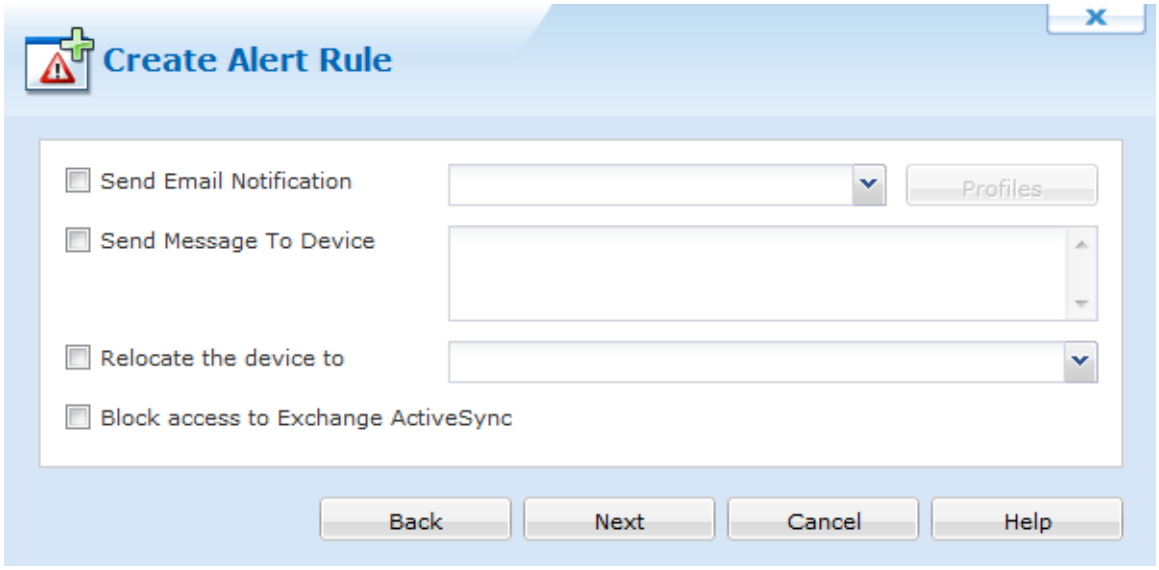
Select Schedule.

Select how frequently the devices should be checked for the requested Alert information. Once you have completed this section, click the **Next** button.



Select Actions.

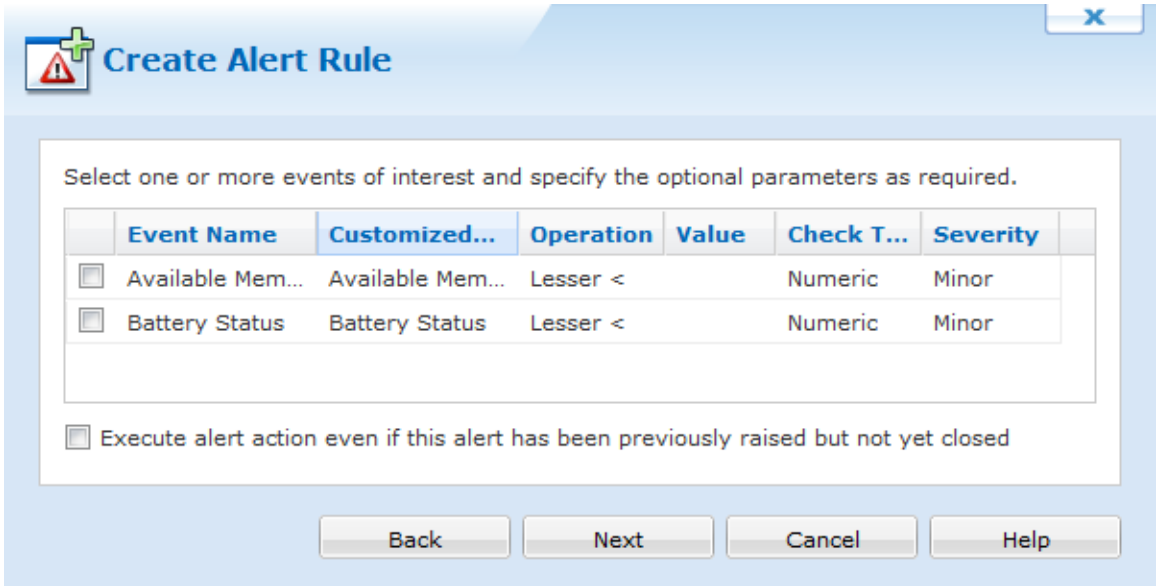
Select any action to be done when the alert has been triggered. MobiControl gives the option to send an email to administrator groups, send a message to the device, relocated the device to a different group, or block access to Exchange Active Sync. One or many of these options can be selected.



After selecting your Profile and Actions, click Next and continue the Alert Rule Wizard here.

Android Devices

The Device Status and Custom Data Events listen below are specific to Android Devices.



Device Status and Custom Data Event Notification Selection Window

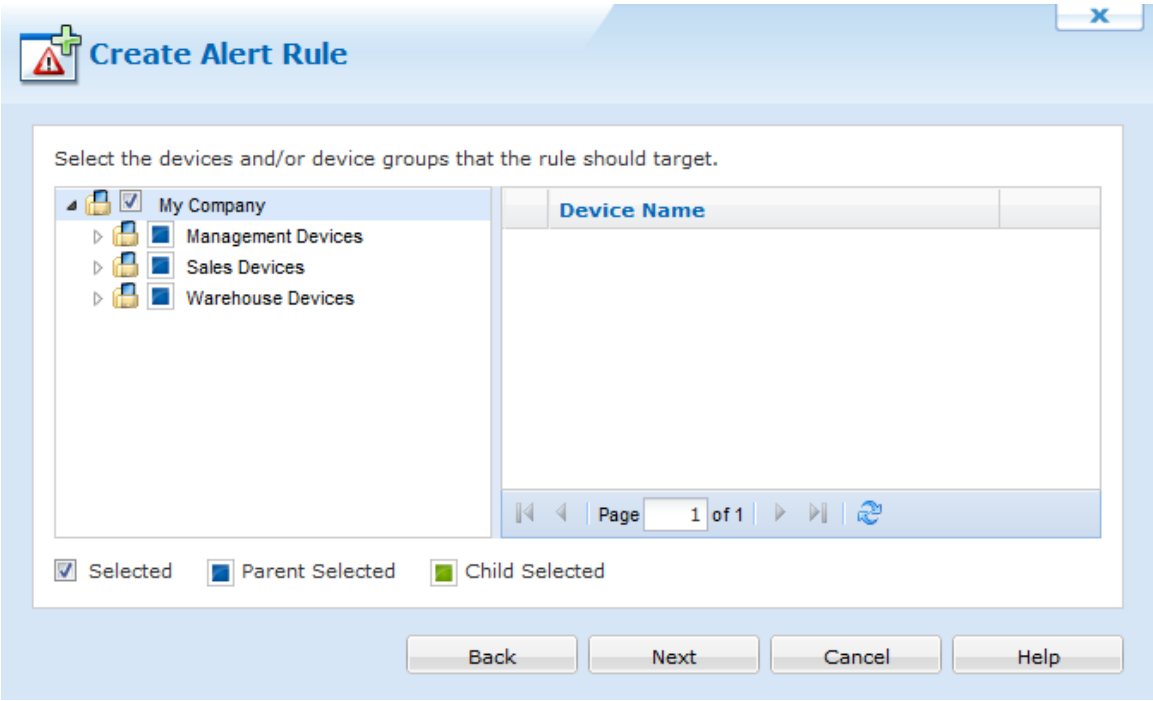
The Operation and Value fields allows to filter out Alerts based on specific values or value ranges. The Operation field specifies at which point an alert will be created for the data value you have specified. Severity is set to Minor by default and can be altered.

The below table shows all available default Device Status and Custom Data Event events:

Log Event	Description
Available Memory	Triggers an alert based on available memory
Battery Status	Triggers an alert based on battery status

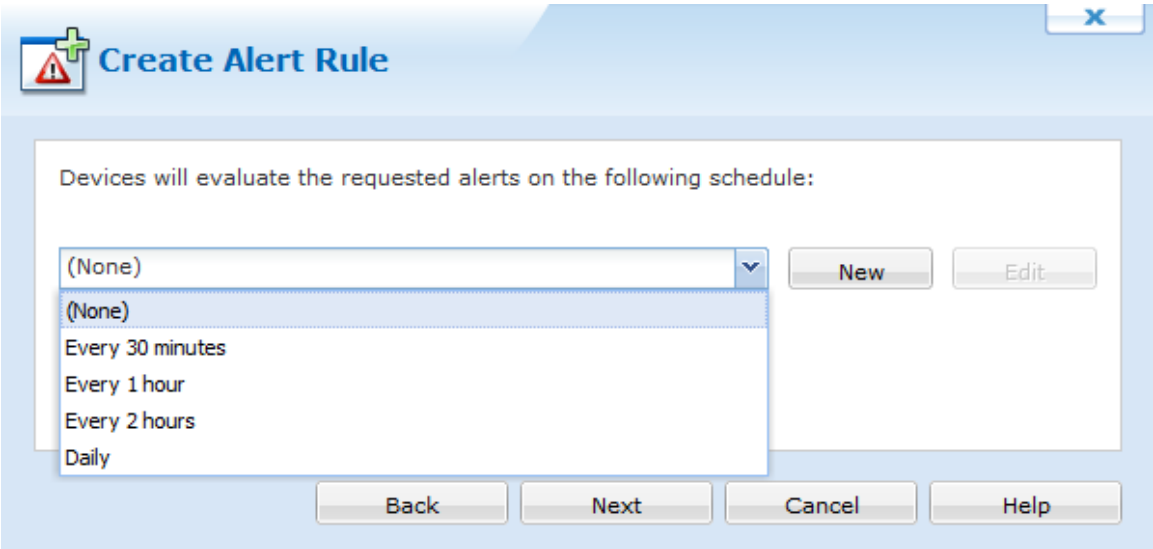
Select devices.

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



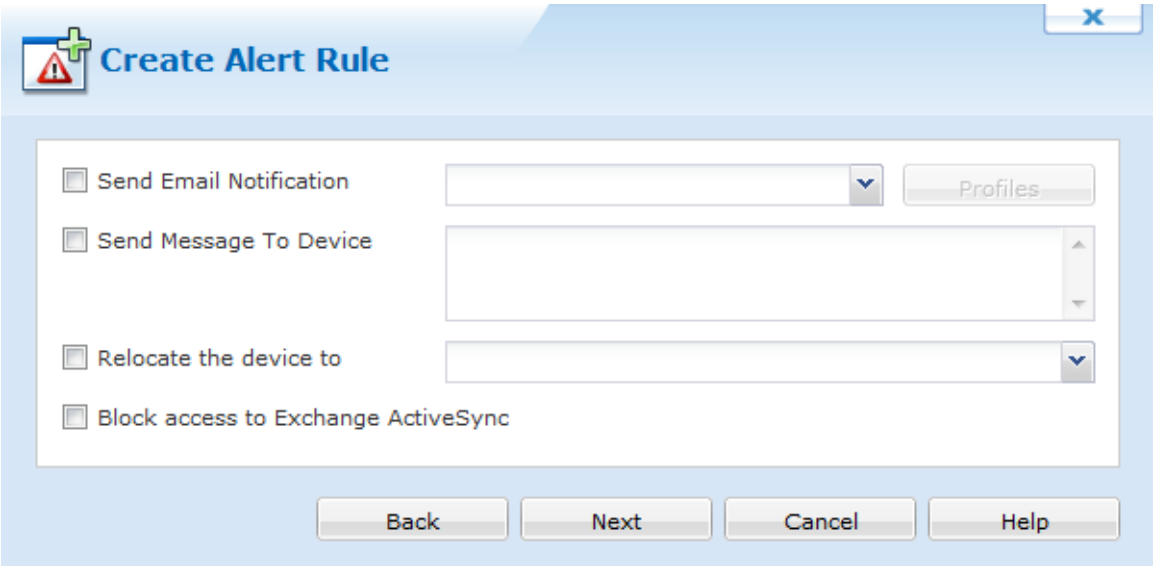
Select Schedule.

Select how frequently the devices should be checked for the requested Alert information. Once you have completed this section, click the **Next** button.



Select Actions.

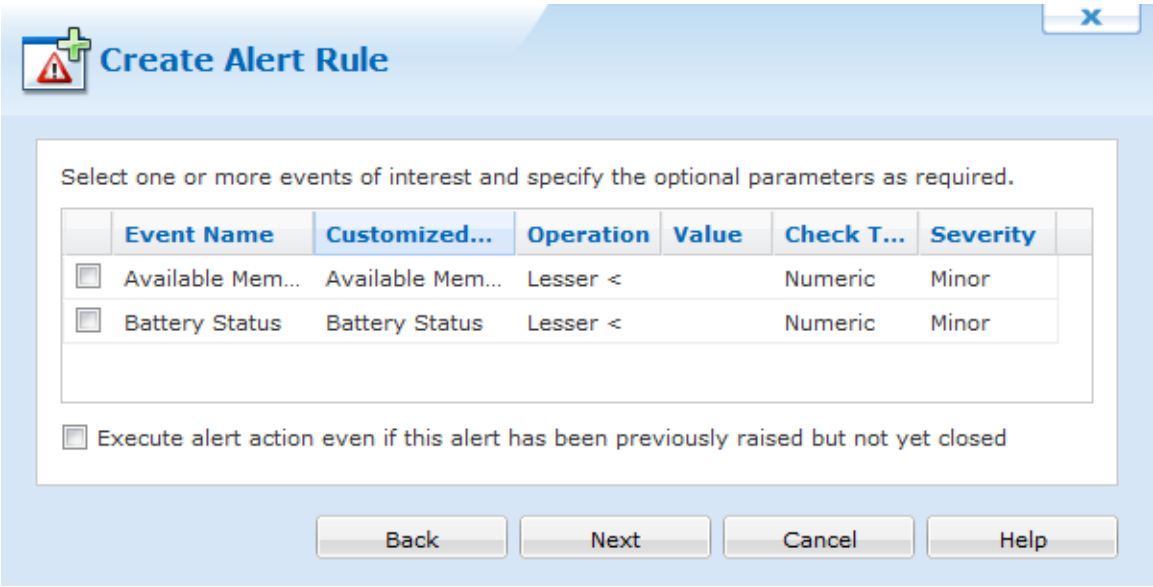
Select any action to be done when the alert has been triggered. MobiControl gives the option to send an email to administrator groups, send a message to the device, relocated the device to a different group, or block access to Exchange Active Sync. One or many of these options can be selected.



After selecting your Profile and Actions, click Next and continue the Alert Rule Wizard here.

Android Plus Devices

The Device Status and Custom Data Events listen below are specific to Android Plus Devices.



Device Status and Custom Data Event Notification Selection Window

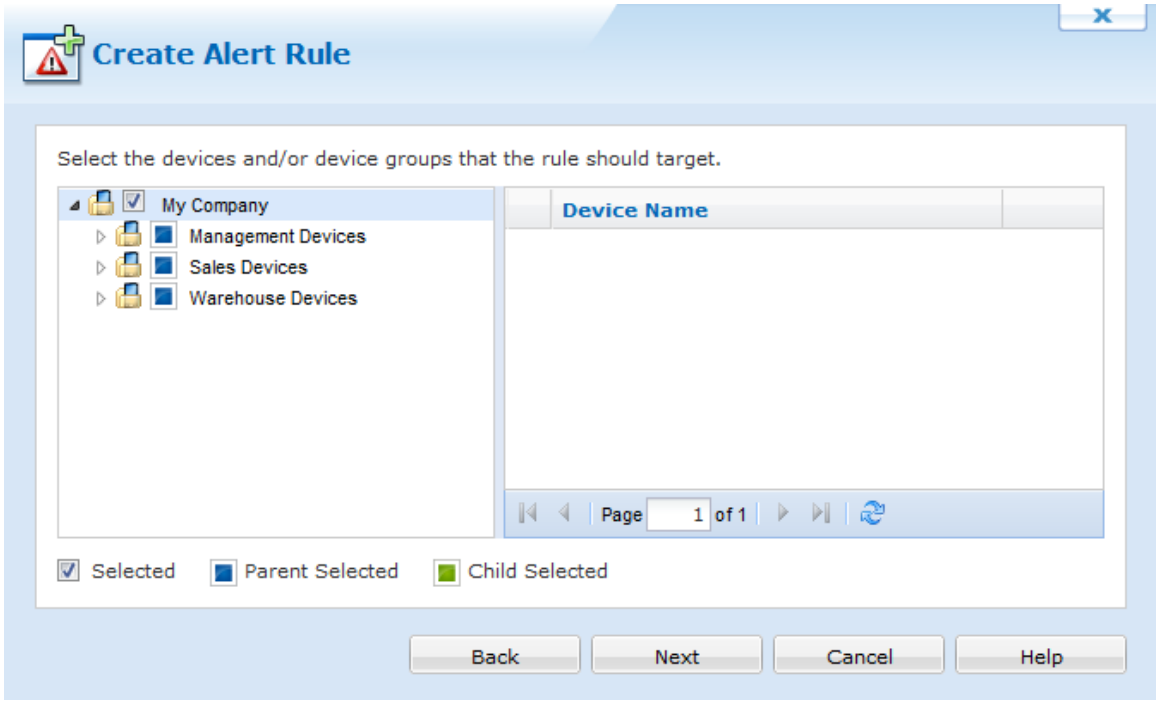
The Operation and Value fields allows to filter out Alerts based on specific values or value ranges. The Operation field specifies at which point an alert will be created for the data value you have specified. Severity is set to Minor by default and can be altered.

The below table shows all available default Device Status and Custom Data Event events:

Log Event	Description
Available Memory	Triggers an alert based on available memory
Battery Status	Triggers an alert based on battery status

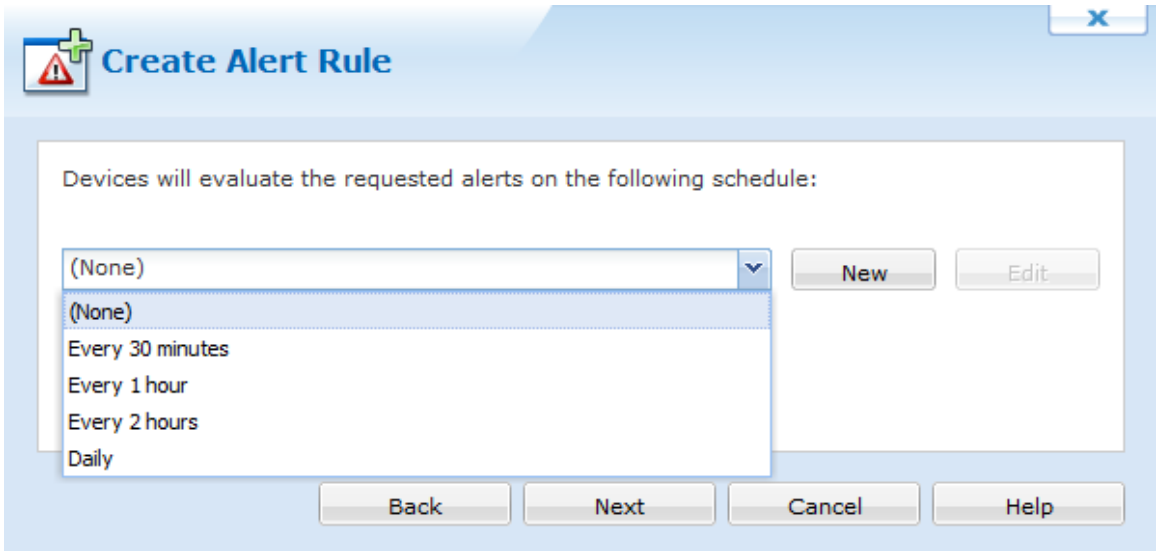
Select devices.

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



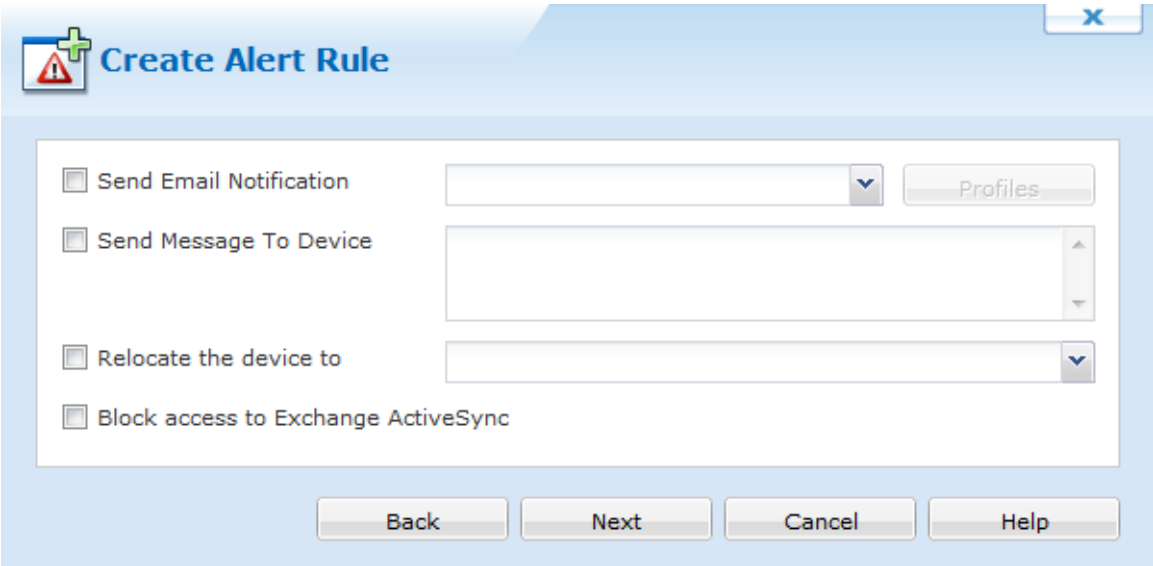
Select Schedule.

Select how frequently the devices should be checked for the requested Alert information. Once you have completed this section, click the **Next** button.



Select Actions.

Select any action to be done when the alert has been triggered. MobiControl gives the option to send an email to administrator groups, send a message to the device, relocated the device to a different group, or block access to Exchange Active Sync. One or many of these options can be selected.



After selecting your Profile and Actions, click Next and continue the Alert Rule Wizard here.

iOS Geofence Event

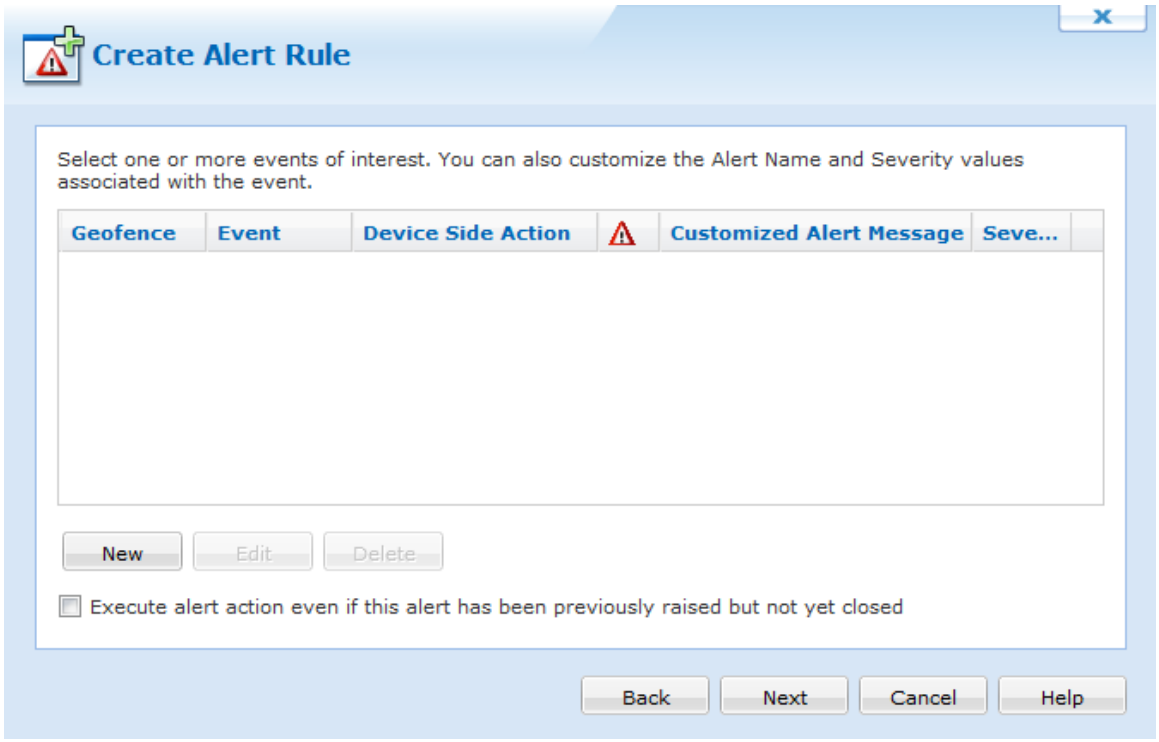
A Geofence Event is an alert trigger based on a GPS enabled device entering or leaving a Geofenced area defined by MobiControl administrators.

EXAMPLE:

If there are devices that should not leave a building complex, a geofence alert rule can be created to ensure that MobiControl administrators are alerted if these devices do leave the complex. Geofence areas can be as small as a house, or a big as a continent.

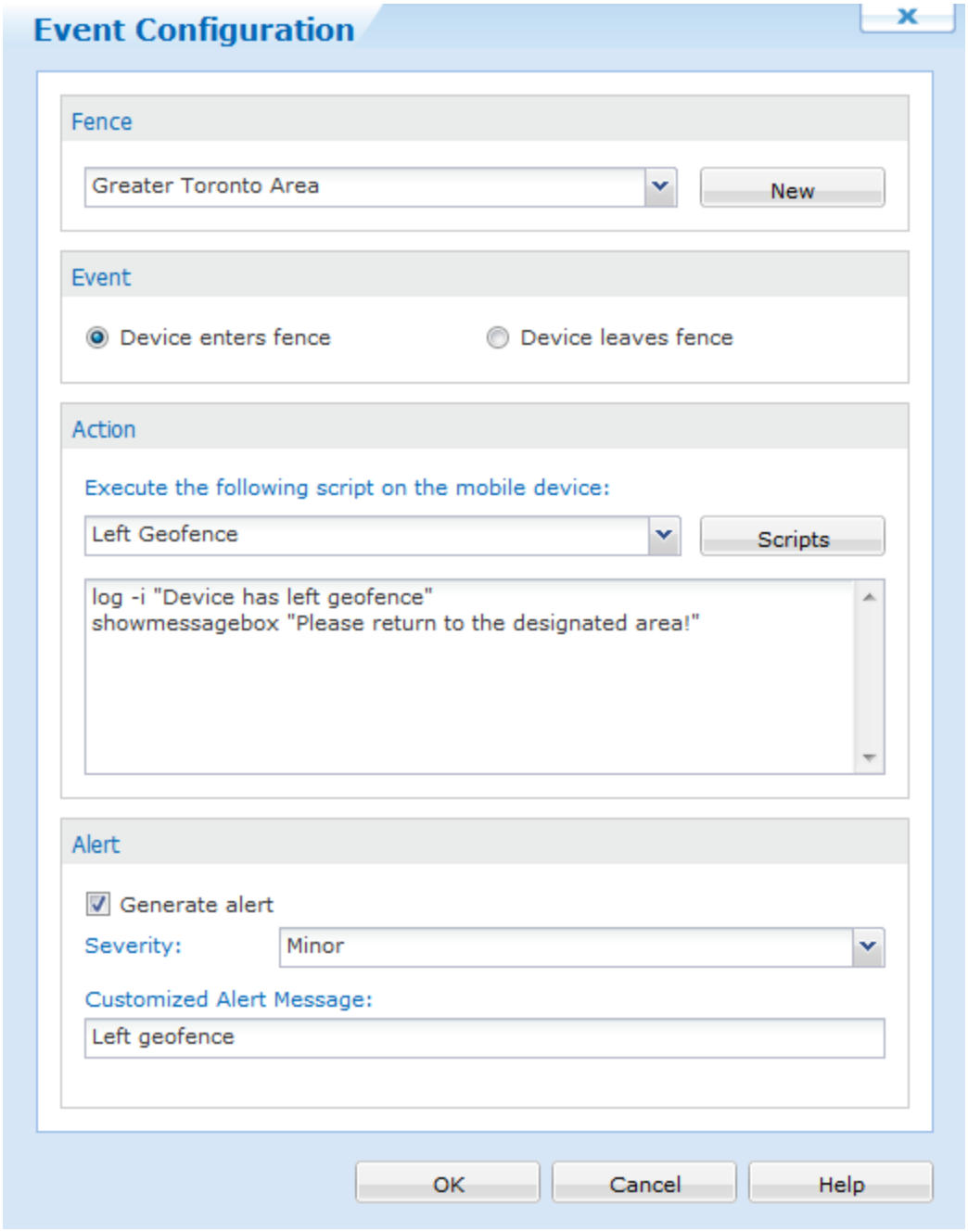
In order to create a Geofence event, an Alert Rule is needed with the Geofence Event type. Please see the "iOS Alerts" topic on page 1068 for assistance with creating an alert rule.

After selecting the Geofence alert type, you will be presented with a window that has all previously created Geofences. If no Geofences have been created click the **New** button.



Geofences

Clicking new brings up the Event Configuration window. Here we can create a new geofence.



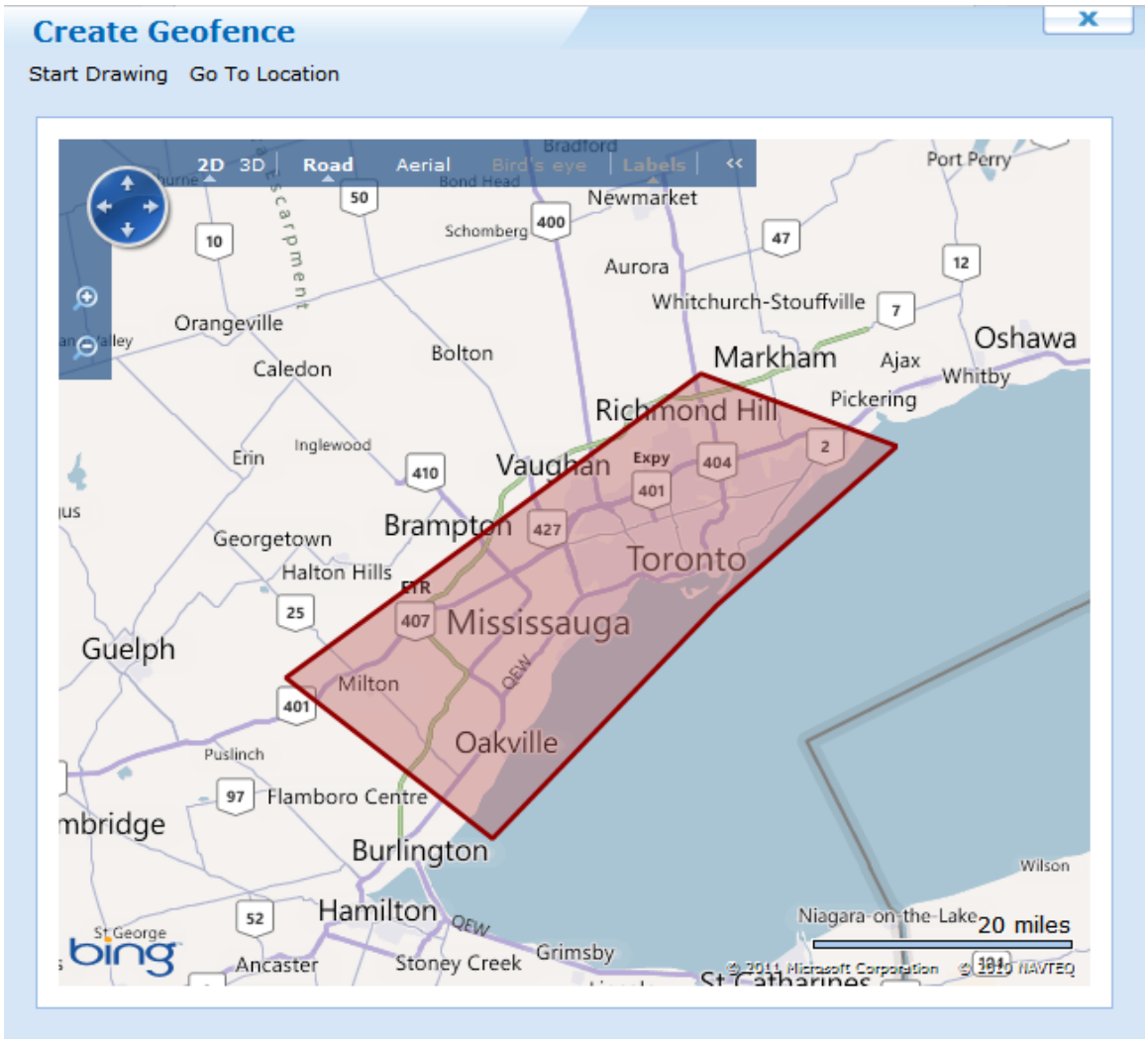
The **Fence** section allows you to create a geofence by clicking on the New button in the dialog box.

The **Event** section allows you to configure if this event should be triggered on entry or exit of a fence.

The **Action** section allows you to configure what script you want to run on the mobile device when the event is triggered. This is optional, but you have for example the ability to run an Activate Connection, Log Event, Show Message or even wipe the device completely.

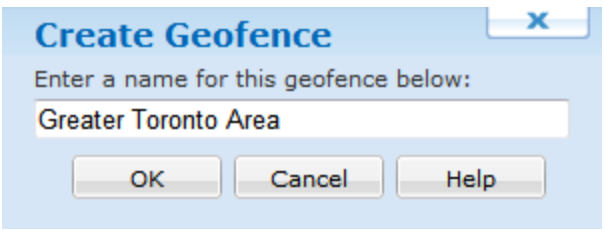
The **Alert** section allows you the option to Generate an alert, configuring its Severity (Minor, Serious and Critical) and add a Customized Alert Message, such as "Left geofence".

When you click on the **New** button in the **Fence** section, the following Geofence Creation dialog box appears:



The two options available are to Start Drawing and Go to Location.

The **Start Drawing** option allows you to begin drawing on the map below the button. The area drawn on the map will be defined as the Geofence. The defined area must be a complete geometric shape, which means the Start Drawing point will be the same as the End Drawing point. When you have completed a proper geometric shape you be asked to name your geofenced area.



Prior to selecting the Start Drawing button, you have the ability to use the view control buttons in the map in order to move to a desired location, zoom in and out, switch to 3D, Road, Aerial and Bird's eye views among the many options. This allows you ease to create an appropriate view for your geofence.

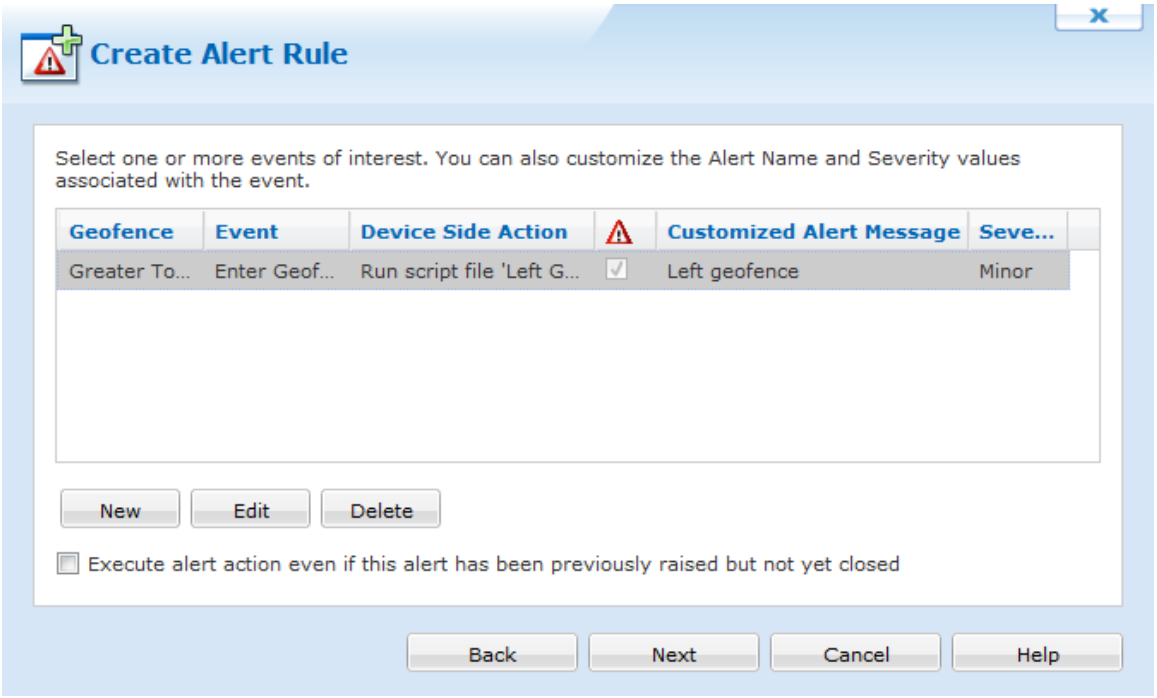
Alternatively to identify the appropriate view of the map, you can click on **Go to Location** which will allow you to specify a street address, location, landmark, or an existing geofence.

EXAMPLE:

- 350 Fifth Avenue, New York City
- Rome
- SFO (San Francisco International Airport)

Once you have the appropriate view displayed, you can click on Start Drawing and you are now able to create a fence. The first click of the mouse is first point of the fence. In order to complete the fence, you must have at least 3 distinct points selected on the map. In order to complete your fence, the last point must end off at the first point so it completes the closure of the fence. Once the last point is selected, a pop-up requesting the name of the geofence is shown. Here you should enter a meaningful name for that specific geofence in case you would like to use it again.

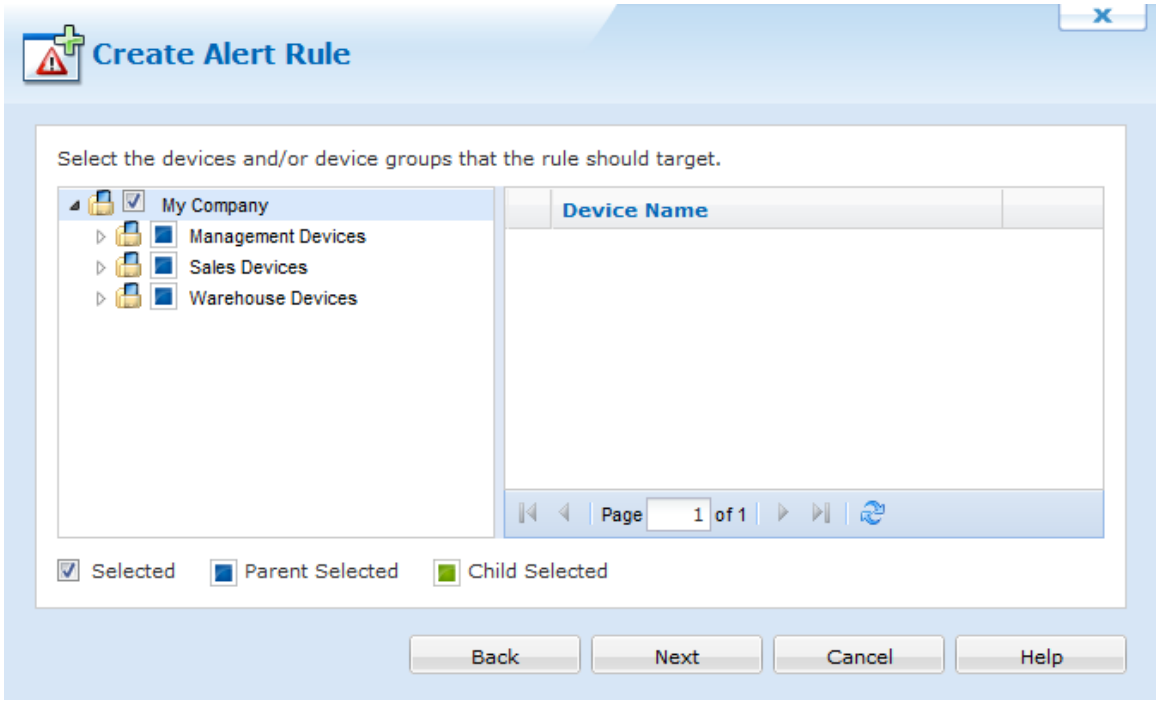
Select Geofence



Once the event is configured it will display as shown in the above diagram. Here you have the ability to create new events, edit existing events or delete events. Also, on this dialog box, there is a checkbox at the bottom allowing you to determine whether or not you want to Execute alert action even if this alert has been previously raised but not yet closed.

Select Devices

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



Select Power Policy

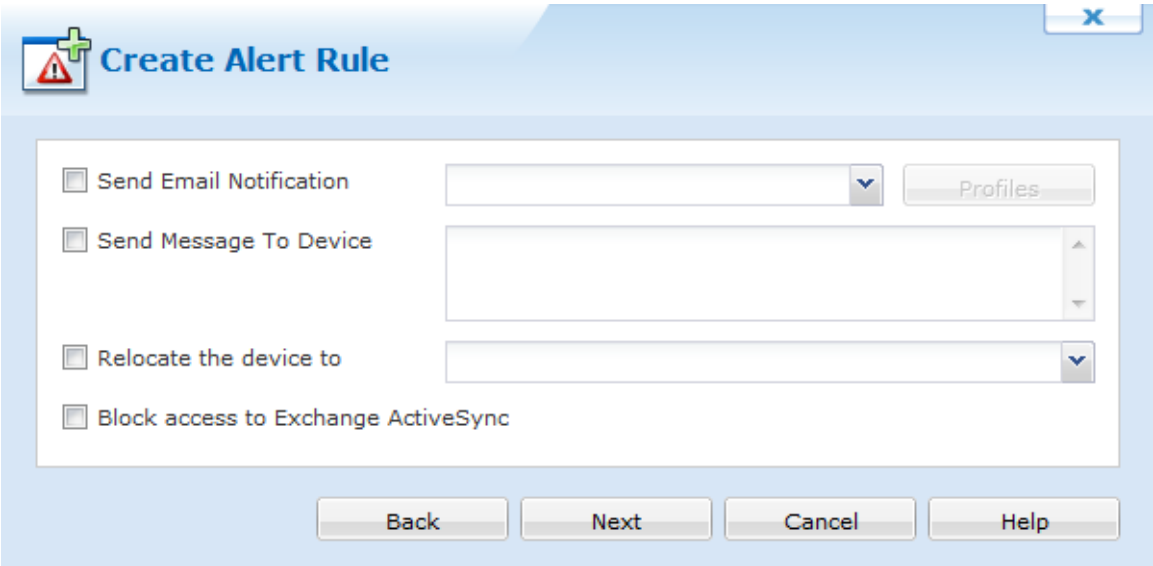
Clicking Next moves you to the Power Policy section as seen below.

The options available for the Power Policy are Optimal Battery Performance and Location Accuracy.

Performance Policy	Description
Optimal Battery Performance	This will report only significant changes in a device's location determined by an active cellular network. This allows for optimal battery while still locating devices
Location Accuracy	This will turn on the radio based on accuracy that you define. Based on your business requirements, location can be as accurate as 10 meters or 3 km. With this, we can also specific when the device will record its location. For example, if **Record location when device moves** is set to 50 meters, the location of the device will be recorded based on the location accuracy.

Action Settings

Once the power policy is selected, you must select your an action to be done.



Select any action to be done when the Geofence alert has been triggered. MobiControl gives the option to send an email to administrator groups, send a message to the device, relocated the device to a different group, or block access to Exchange Active Sync. One or many of these options can be selected.

After selecting your actions, click Next and continue the Alert Rule Wizard here.

iOS Telecom Expense Management

The Telecom Expense alert rule allow MobiControl Administrators to monitor how much data and minutes a group of devices/individual devices use based on a company data plan. This rule allows Administrators to set a soft threshold along with a hard threshold. When data or voice minutes reach either the soft or hard threshold, devices can automatically be relocated to another group and have either data or voice disabled. An email can also be generated and sent to a configured email address when a soft or hard threshold is reached.

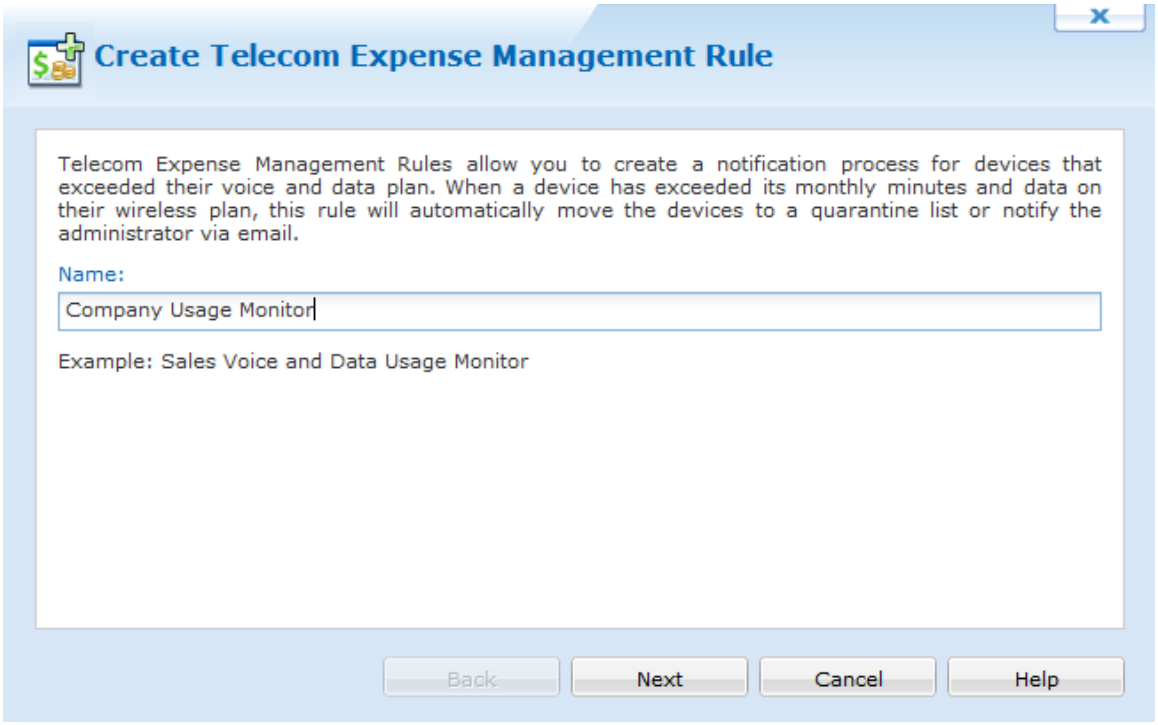
This allows enterprises to better manage company data and voice minutes.

The steps below describe how the Create Telecom Expense Management Wizard can be used to create an Telecom Expense Alert using the MobiControl Web Console:

1. Start the wizard.

   Select the Android+ Tab, then select the Rules tab. After, right click on the **Telecom Expense** folder, and select **Create Telecom Expense Management Rule**. The first page of the Create Telecom Expense Management Wizard will be displayed.

   Enter a descriptive name for the Telecom Expense rule and click **Next.**



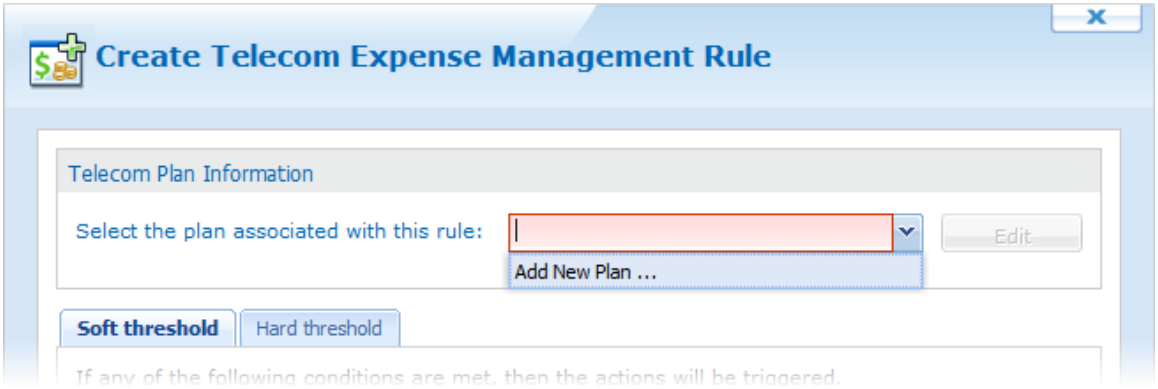
Enter a descriptive name for the Telecom Expense Rule

2. Select the target for the rule.

Here, we can select which group or device will be monitored with the Telecom Expense Management rule. Groups or devices that have ■ means that they are automatically selected because their parent group is selected. Groups that have ■ means that a child of that group is selected. Click **Next** to continue.

3. Telecom Expense Management configuration

On this screen, we are able to create a new data plan that will be associated with this rule, or choose an existing one. To create a new plan, choose the **Add New Plan** from the very top drop down menu.

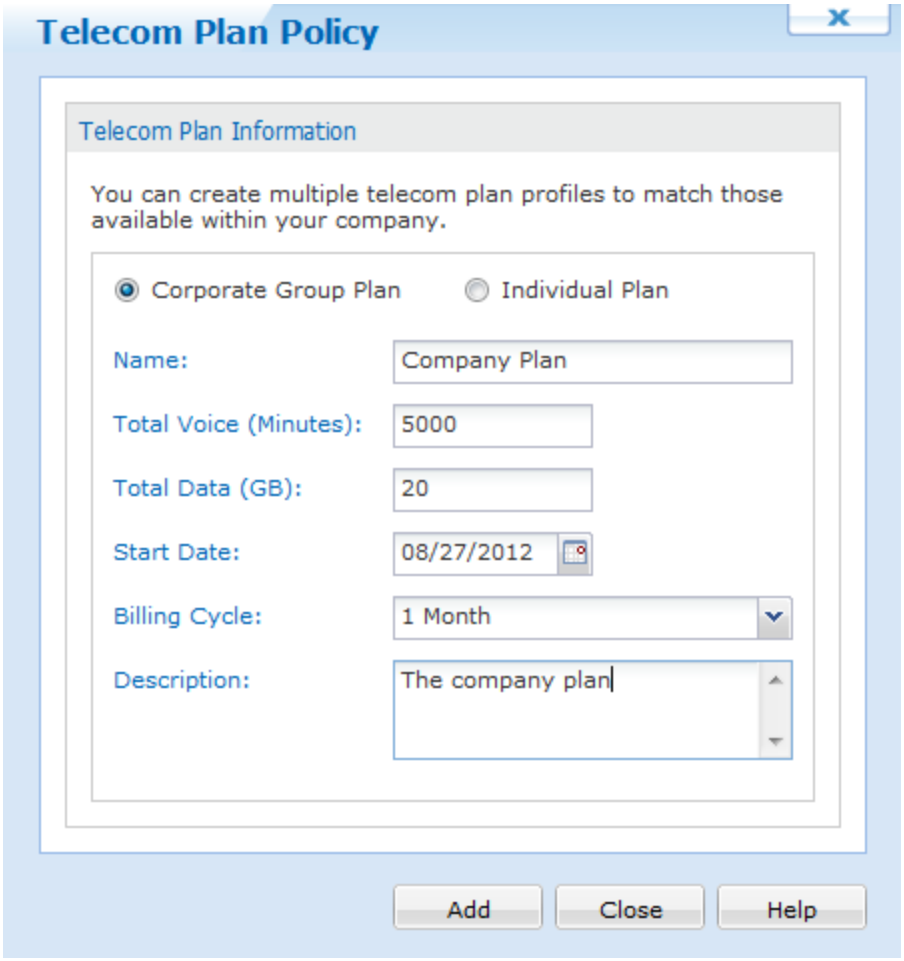


Adding a new Telecom plan

When **Add New Plan** is selected, the Telecom Plan Policy window is shown. Here we can choose whether this plan should be for a Corporate Group plan or an Individual Plan.

It is recommended that Corporate Group Plan is selected if the Telecom Expense Management rule is targeting a group of devices.

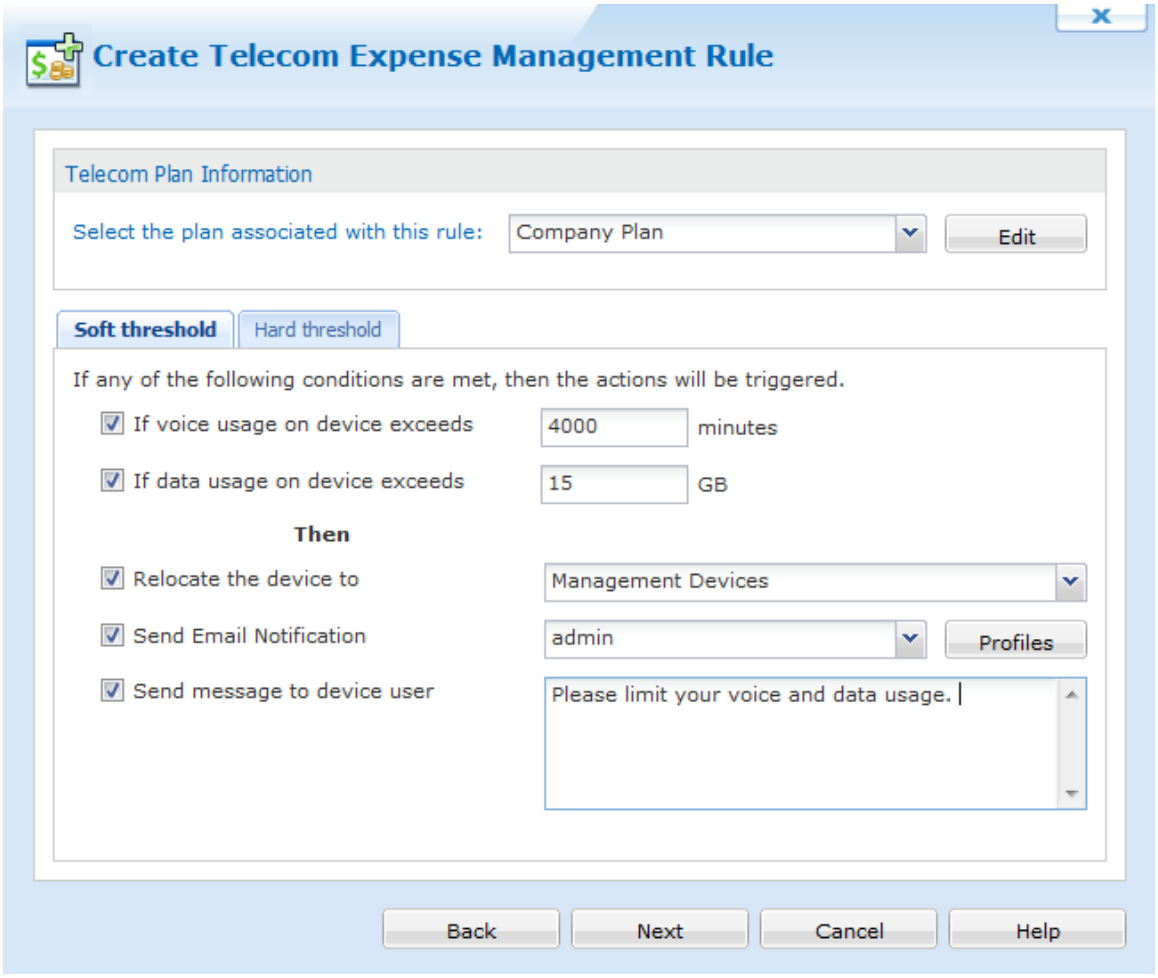
- A name and a billing cycle must be entered to add a plan.
- Voice is calculated in minutes, while data is calculated by gigabytes. If either of these are left blank, then unlimited is automatically listed.



Telecom Plan Policy

When a plan policy is created we can then configure the soft and hard threshold for the rule. Think of the soft threshold as a warning, and the hard threshold as critical. If the "voice usage on device exceeds" check box is selected, MobiControlwill check if a device or devices reach the number specified. The same rule applies for monitoring data usage. If any of the numbers are reached, MobiControl can then move the device to a new group, send an email notification, or send a message to the user.

After setting up the configurations here, click **Next**.



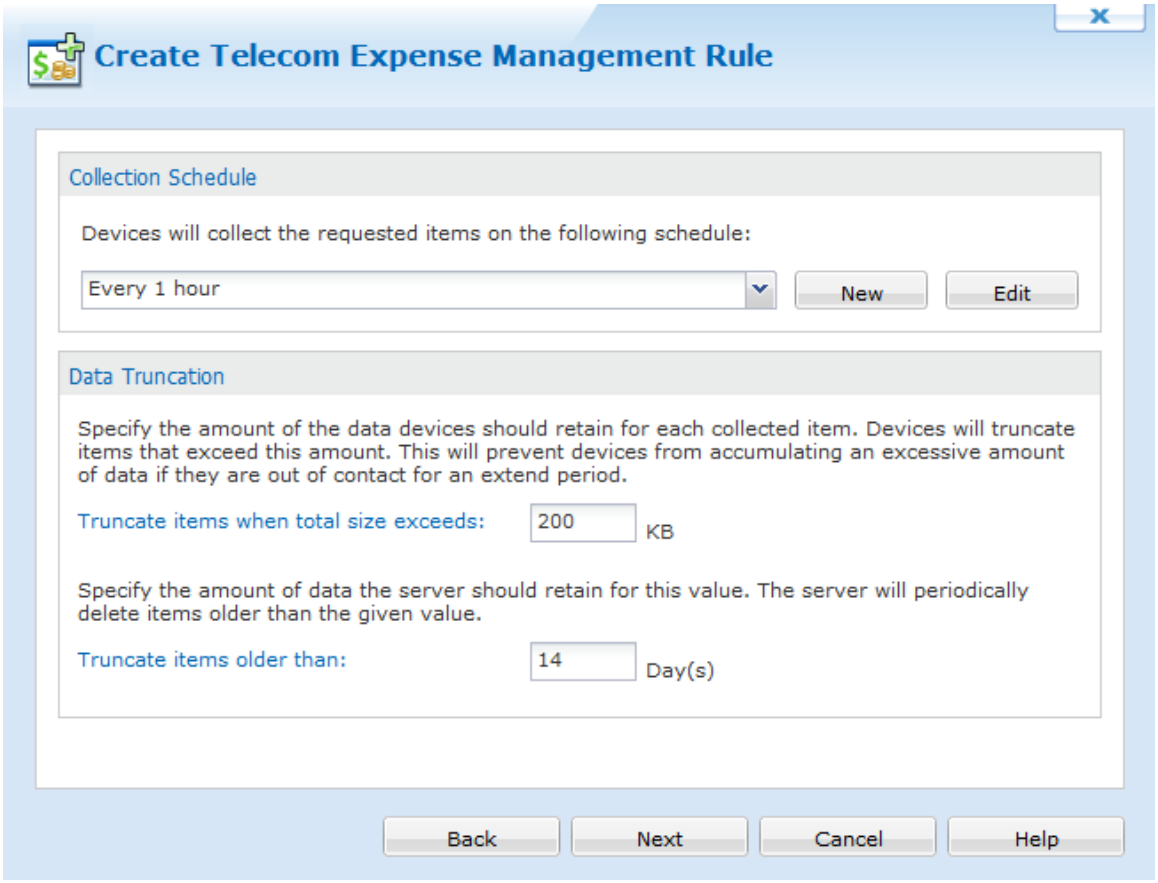
Telecom Expense configuration

4. Configure Data Collection and Optional Settings

Here, we can set how often the data is to be collected. Options include every 30 minutes, every hour, every two hours or daily. We also have the ability to create a custom collect schedule.

Data truncation specifies the amount of data that each device should retain. Any amount of collected data that goes above this number, will be truncated. This can be left as the default value.

After specifying the collection schedule and data truncation settings, click **Next**.

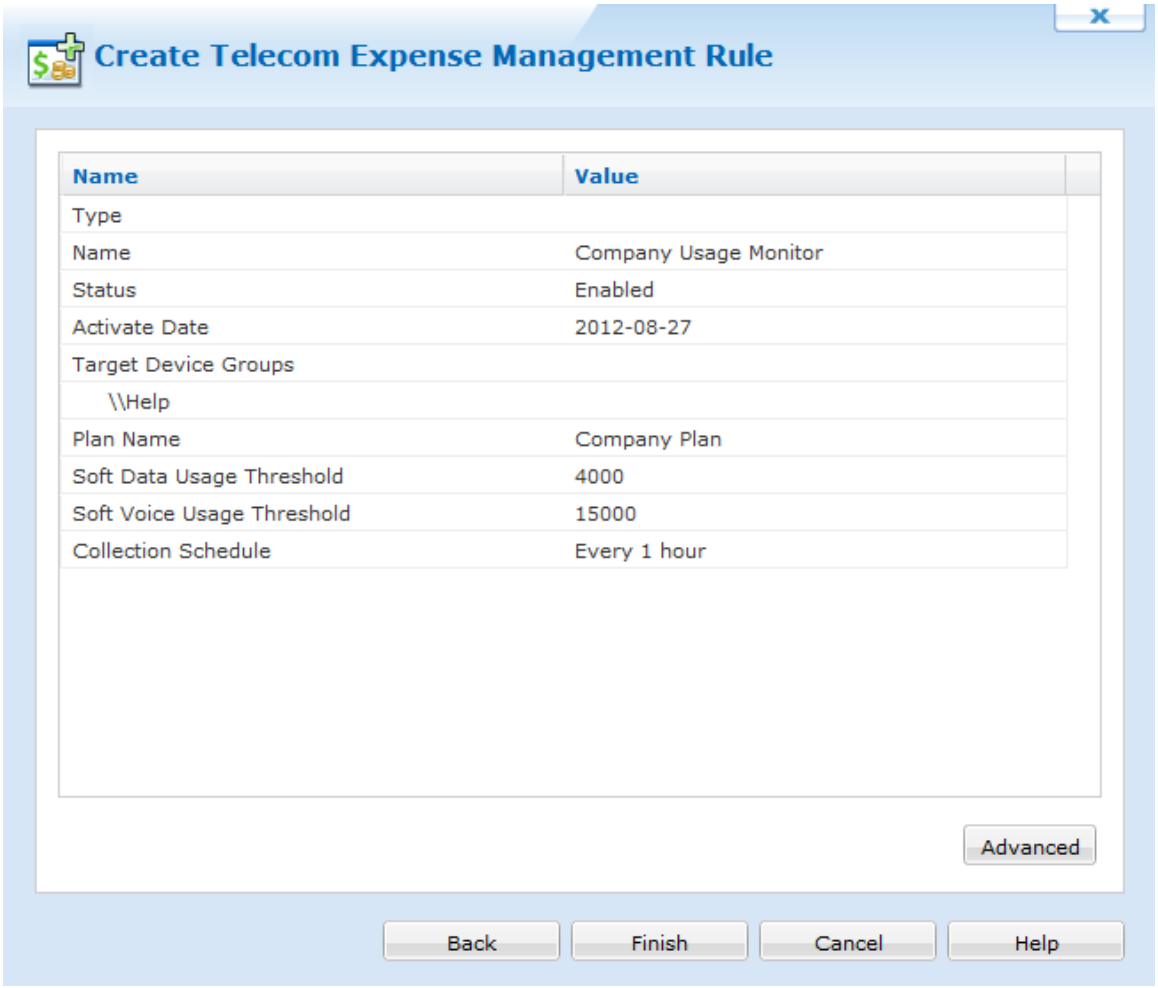


Data collection and optional settings

After specifying the collection schedule and data truncation settings, click **Next**.

5. Review the summarized information.

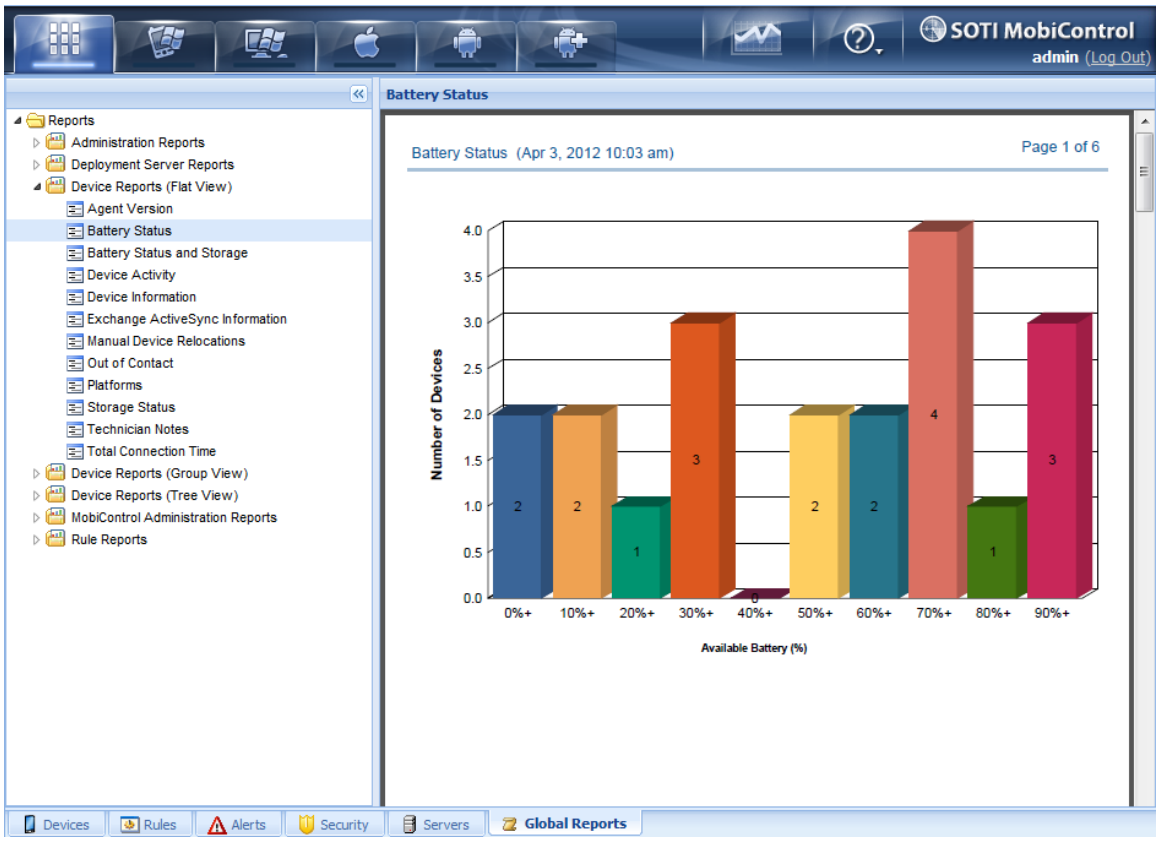
   The summary page will show all options and configurations that was specified in the previous steps. If something is needed to be changed, just click back and change the setting.



   Once everything is confirmed, click **Finish** to complete the wizard.

iOS Reports Tab

MobiControl includes an advanced reporting engine—Crystal Reports—that gives detailed information about all aspects of system operation. The product includes a set of canned reports that provide information about key areas of system operation. Reports can also be customized as well as new reports can be created and added to the system as needed.



MobiControl Manager Reports view (tab)

The MobiControl Web Console allows you to generate Reports based on the Devices Operating System (OS). Some Reports are specific to the OS Tab that has been selected. For detailed information on the Reports available please see the specific Reports that can be created below:

Report Types

The following reports are included with MobiControl:

- A **deployment server activity report** is a detailed report for deployment server activity over a specified time period.
- A **deployment rule report** is a detailed report of deployment rules and all devices.
- A **Battery and Storage Report** is a detailed report of the battery and storage of the selected devices.
- A **Cellular Signal Strength Data Report** is a detailed report of the cellular signal strength of the selected devices.
- A **deployment rule summary report** is about deployment rule exceptions, showing how many devices have executed the rule successfully, are pending, or have encountered an error.
- A **Deployment Server activity report** is a detailed report of Deployment Server activity over a specified time period.
- A **device activity report** provides information about the device activity during a specific time period.
- A **device custom data report** provides information about devices with the custom data values of selected custom data fields.
- A **device note report** provides information about the notes for your devices.
- A **device package report** provides information about packages installed on your device.
- A **device program report** provides information about all the programs installed on your devices.
- A **device relocation rule report** provides information about all the relocation rules for your devices.
- An **out of contact devices report** provides information about devices that have not connected to the system since the specified date.
- A **package deployment report** provides information about package deployment.
- A **Location Collected Data Report** is a detailed report of the location data collected for the devices.
- A **Connectivity Information Report** is a detailed report regarding device's connectivity.
- A **Device Tree Report** provides information about the device tree structure.
- A **Device Tree with Virtual Groups Report** provides information about the device tree structure along with the virtual groups.
- A **Log Information Report** provides information about the device logs.
- A **Phone Number Report** provides information about the phone number of devices.
- A **Alert Summary Report** provides summary of the alerts.
- A **deployment rule report** is a detailed report of deployment rules and all devices.
- A **Geofence Report** provides detailed report based on the Geofence.
- A **Uninstalled Mandatory Applications Report** provides information about the mandatory application not installed on the devices.
- And many more.

Generating a Report

1. In MobiControl Manager, select the Reports view (tab).
2. Select a report in the left pane of the Reports view (tab).
3. Click the **Generate Report** button.

4. For some reports, a window will appear requesting additional parameters (e.g. time period) that may be required.

Saving a Report

1. Generate a report.
2. On the report screen, click the **Export Report** button. (It is the first icon in the toolbar, beside the **Print Report** button.)
3. Select the desired file type. Available file types are:
    - Adobe PDF (`.pdf`)
    - Crystal Reports (`.rpt`)
    - HTML 3.2/4.0 (`.html`)
    - MS Excel 97-2000 (`.xls`) or Data only (`.xls`)
    - MS Word editable RTF (`.rtf`)
    - ODBC
    - Record-style (columns of values with or without spaces) (`.rec`)
    - Report definition (`.txt`)
    - Rich text format (`.rtf`)
    - Comma-separated values (`.csv`)
    - Tab-separated text (`.ttx`)
    - Text (`.txt`)
    - XML (`.xml`).
4. Select the location to which you want to export the report. The options available are:
    - Application
    - Disk file
    - Exchange folder
    - Lotus Domino
    - Lotus Domino Mail
    - MAPI (Messaging Application Programming Interface)

Printing a Report

1. Generate a report.
2. On the report screen, click the **Print Report** button. (It is the second icon in the toolbar, beside the **Export Report** button.)
3. The print menu will pop up. Select the desired printer and the report will be printed there.

Generating Custom Reports

It is possible to create custom report files on any available statistic you desire. The Deployment Server database is a standard SQL database and can be queried by writing a custom query. Also, it is possible to create additional reports that are built into MobiControl. For more details, please contact us.

Other Tools

These other tools are available through the toolbar:

- The **Stop Loading** button stops the report generation process
- **Refresh** regenerates the report. If parameters were required to generate the original report (e.g. time period), a window will appear requesting the additional parameters
- The **Search Text** button searches the body of the report for a specified text string
- The **View Zoom** field allows the user to select view magnification, page width, and whole page views

Secure Content Library

The MobiControl Secure Content Library allows users to upload files through the web console so that it can be distributed to devices.

With the Secure Content Library we are able to specify file properties when it is uploaded. These properties can range from delivery methods to expiry dates.

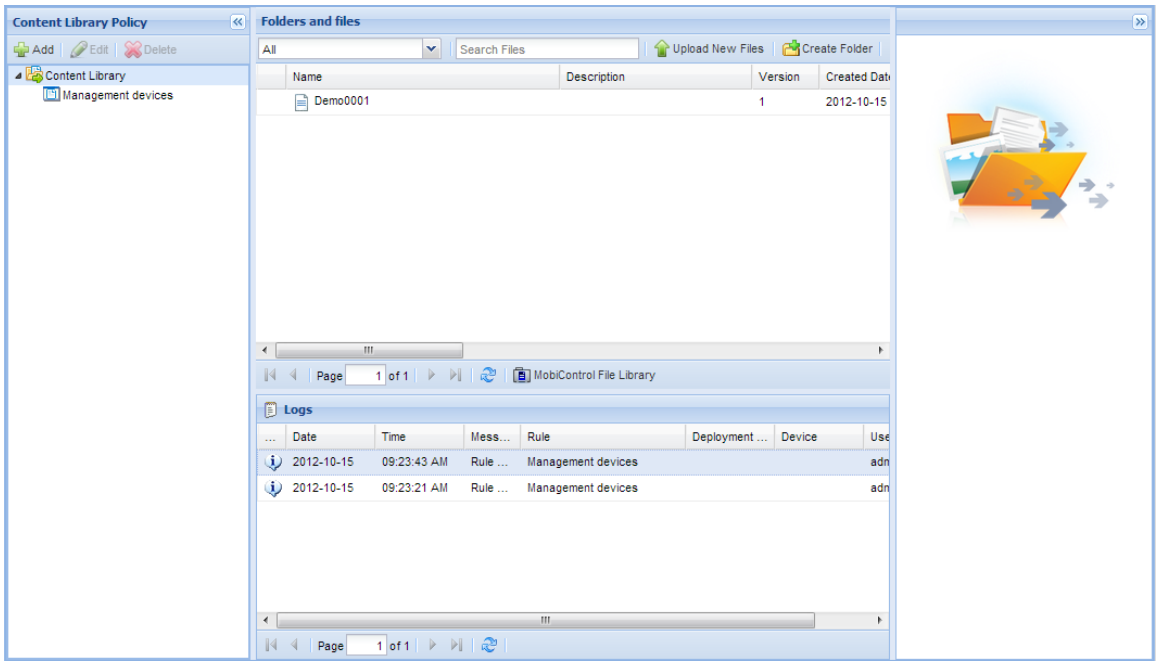
NOTE:

The Secure Content Library is only available for iOS and Android devices.

NOTE:

If the file sync rule is enabled for iOS devices, all those files will appear in the same panel as Content Library files. Files sent by the file sync rule cannot be configured by Content Library settings.

To go to the Secure Content Library, click the Content Library tab at the bottom of the device tab.



Secure Content Library

There are 4 main panels in the Secure Content Library. Starting clockwise, there is the Content Library Policy, Folders and Files, Deployment status, and logs. The Content Library Policy allows us to select which devices get files. Folders and files panel allows us to upload new files and create new folders. The deployment status shows us how many devices downloaded files, and the logs panel shows the logs related to the Secure Content Library.

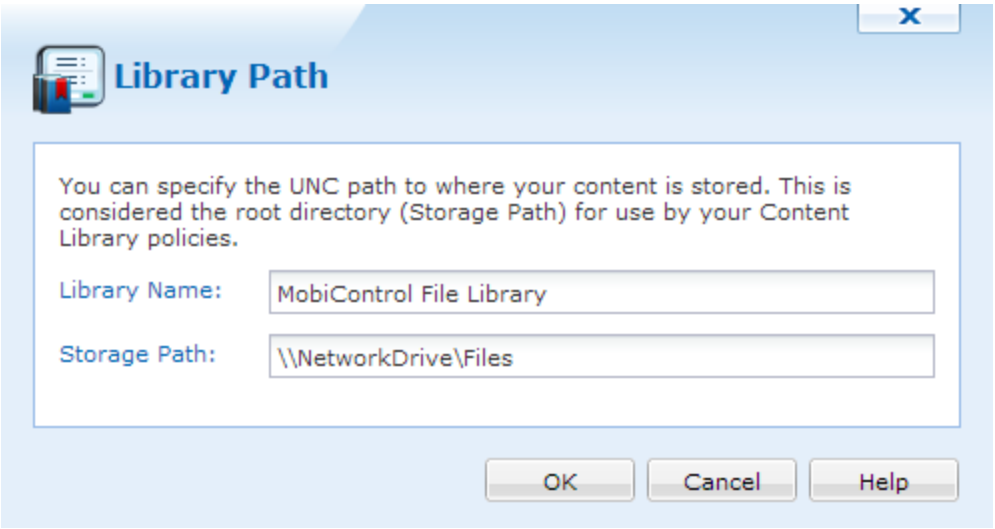
Library Path

When we first open the Secure Content Library tab, we will be prompted with a dialog asking us to name the Content Library and where to store the files.

The Storage Path could be anywhere the deployment has access to. Be it a shared folder on the network, or a folder on the hard drive. All files uploaded will be placed here.

NOTE:

The recommended Storage Path should be a network drive where both the Deployment Service and Management Service have access to.



Library Path

NOTE:

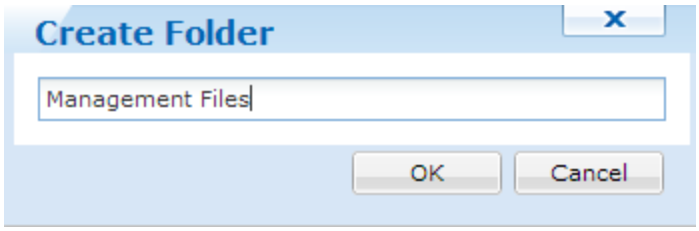
We can change the Library Path at any time. To do this, click the icon at the bottom of the Folders and files panel.

Folders and Files

After choosing the Library name and the Storage Path we are ready to create our folders and upload our first files.

Creating Folders offers a way to organize files. If a folder is wanted to be created, click Create Folder.

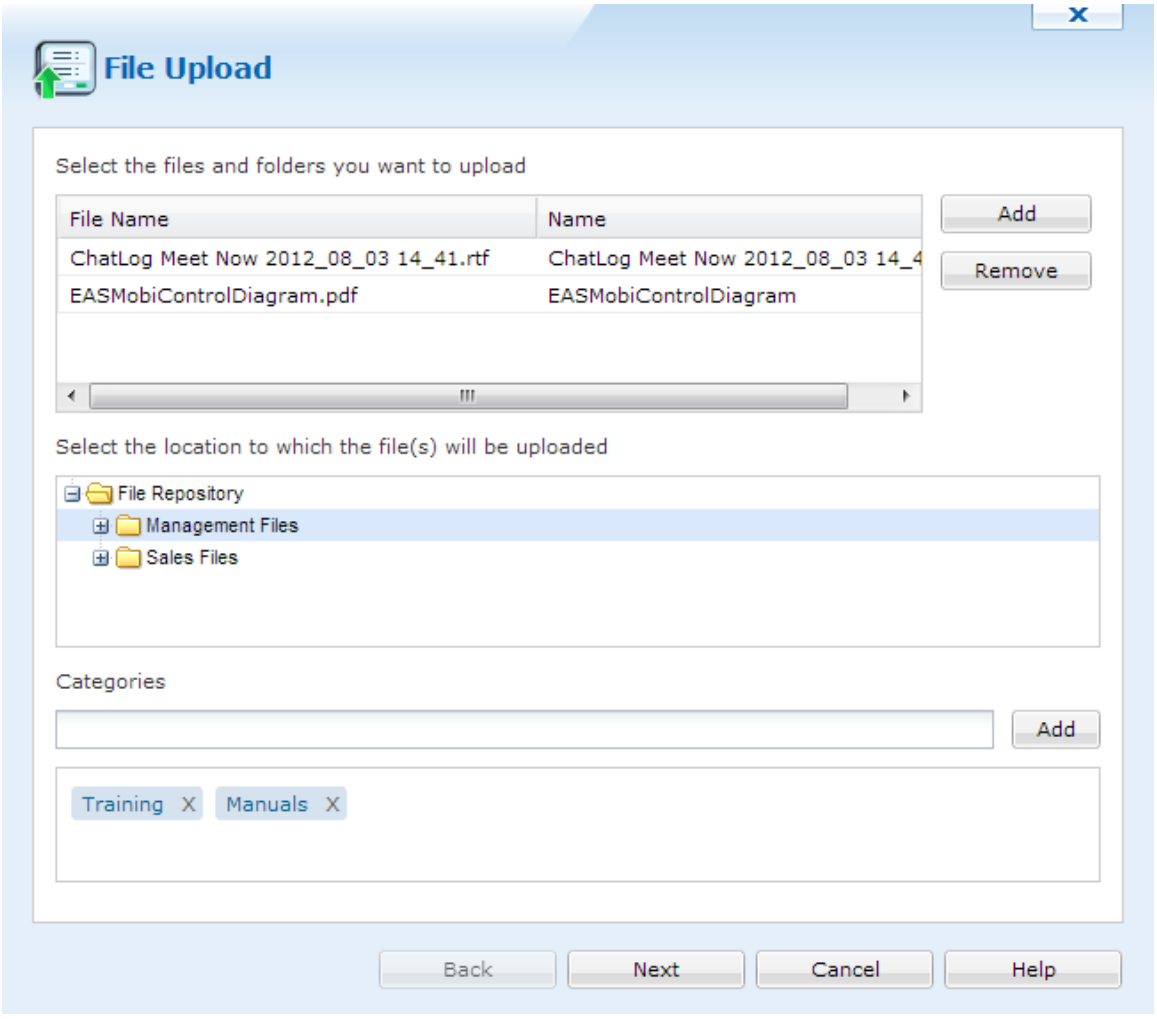
When the Create Folder dialog appears, enter a name and click OK.



Create Folder dialog

File Upload

After creating any folders needed, we can now upload files. To do this, click Upload New Files .



File Upload

Click the Add button to select a file and upload it. We can upload multiple files from here. If a file isn't needed, select it and then click Remove.

After uploading the files, we can select where these files will be placed in the Secure Content Library. File Repository is the root directory, then listing all folders that were created.

When a folder is chosen, we can add categories to these files. Categories are special tags that label each of the files. If we categorize these files for training, we can filter them based on these tags.

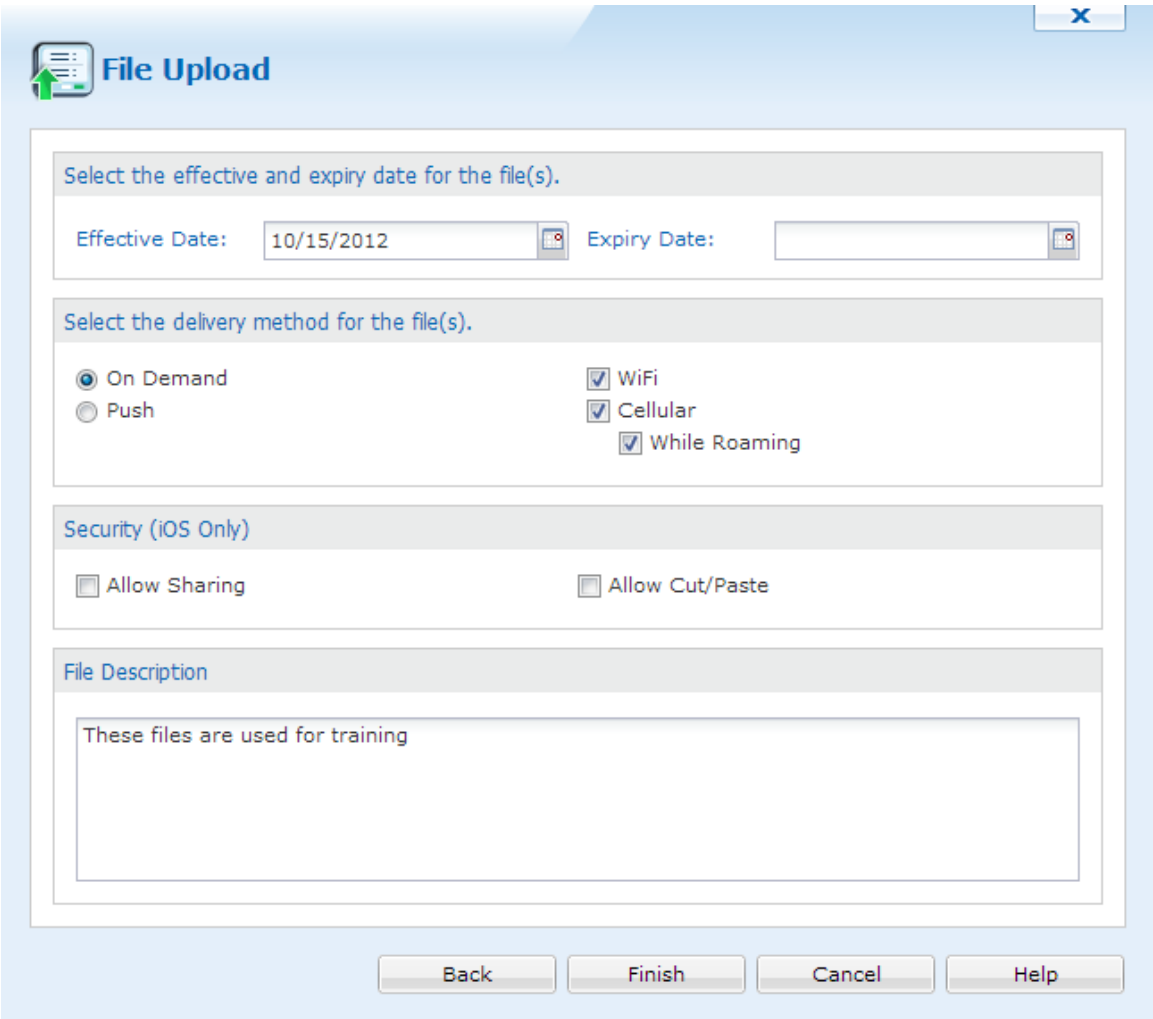
To add a category, just type it into the text field. If categories were created before, MobiControl will find them and we will be able to select them. If a category wasn't created, click Add to create this category.

When everything is configured and set, we can click Next to go to the next page.

File Upload Properties

This panel will allow us to modify the properties of the uploaded files.

We can select the dates the files are effective for, the delivery method, security and description.



File Upload Properties

NOTE:

If the Expiry Date is not needed, please do not click the field. This will ensure that the files will never expire.

If we select On Demand as the delivery method, then files will not be automatically pushed to the devices. Selecting Push will allow the files to be automatically downloaded to the devices.

We can also restrict the way the files are downloaded.

iOS devices offer additional security where these files cannot be shared or cut and pasted.

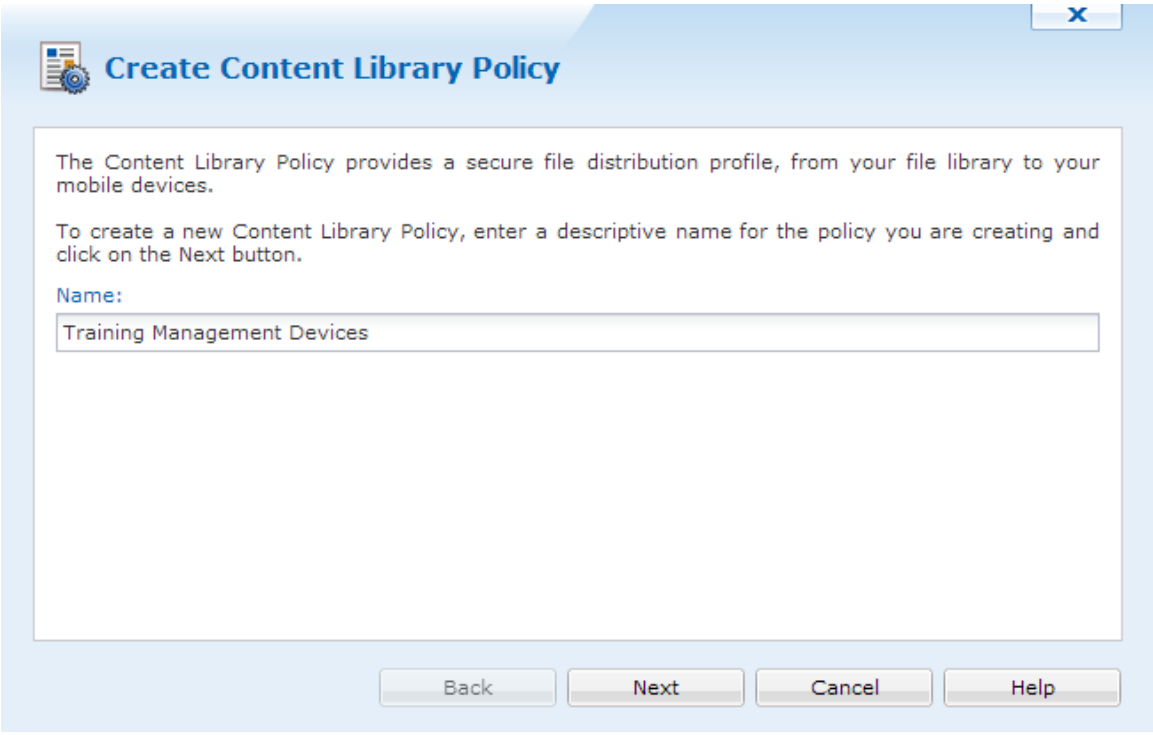
After all properties have been set, click Finish. The files are now uploaded to the MobiControlDeployment Server.

Content Library Policy

The Content Library Policy provides a secure file distribution profile, from the file library to mobile devices.. We can create as many policies as needed. To create a new Content Library Policy, click Add.

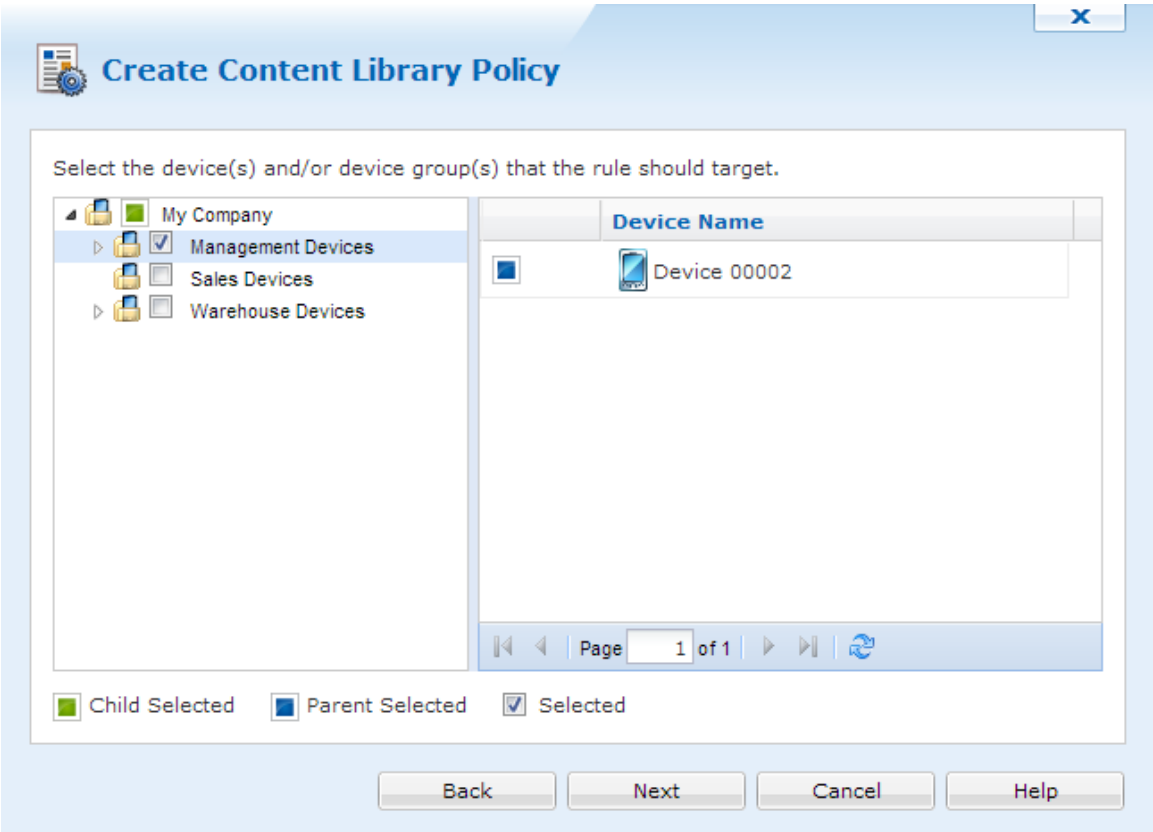
Create Content Library Policy

When we clicked Add, the Create Content Library Policy dialog appeared. In the first panel, enter a name, then click Next.

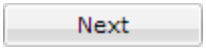


Create Content Library Policy

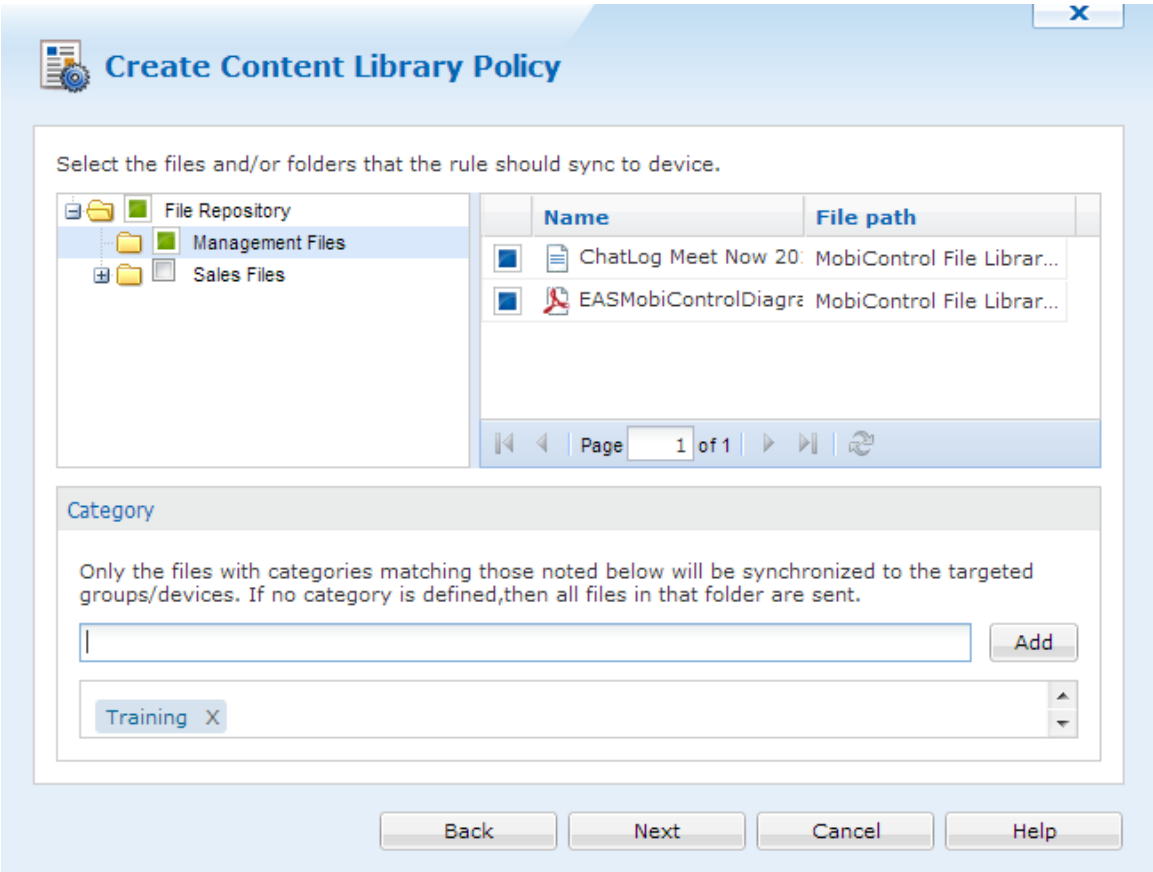
On the next panel, we can select which devices or groups will receive these files.



Select devices and groups

Click  to advanced to the next panel.

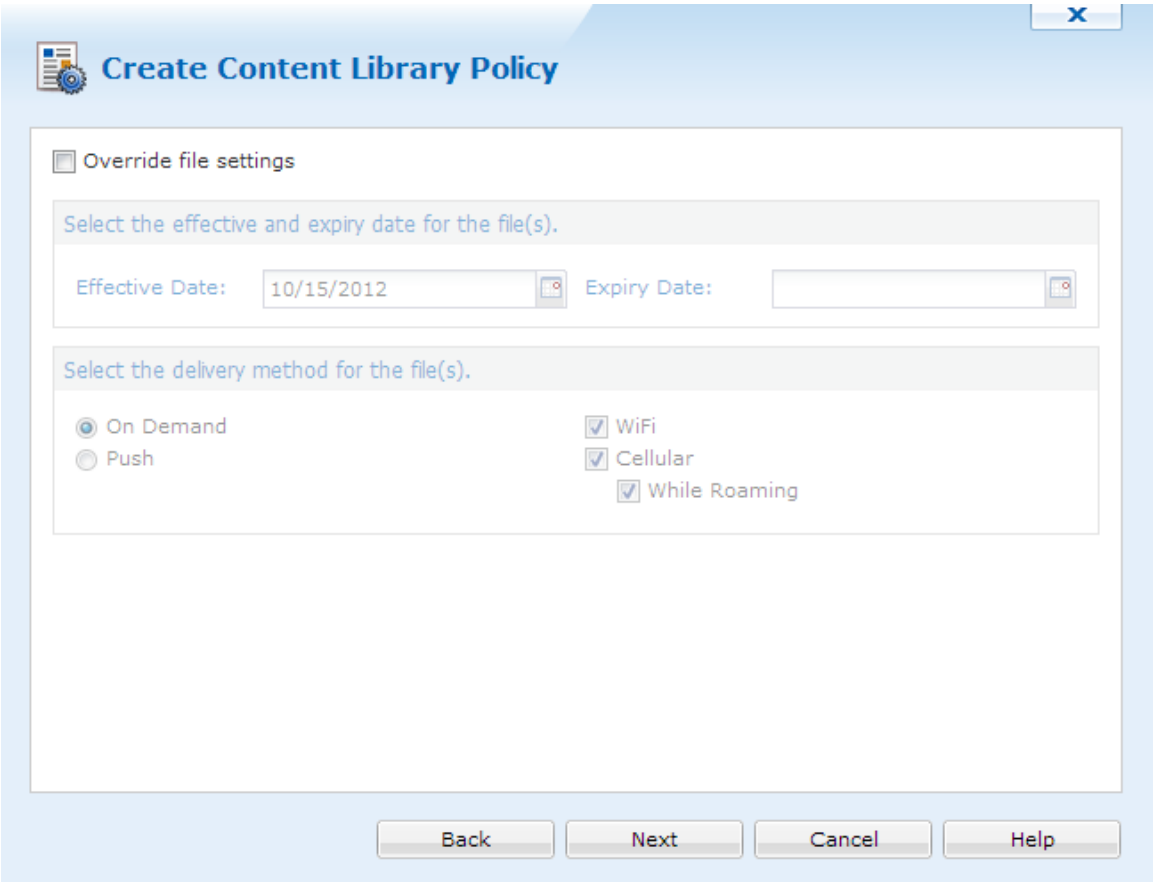
On this panel we are able to select which files are going to be accessible on the devices. If categories were made before, we can just type a category and all files with that tag will be selected.



Source Files

After the files are selected, click Next.

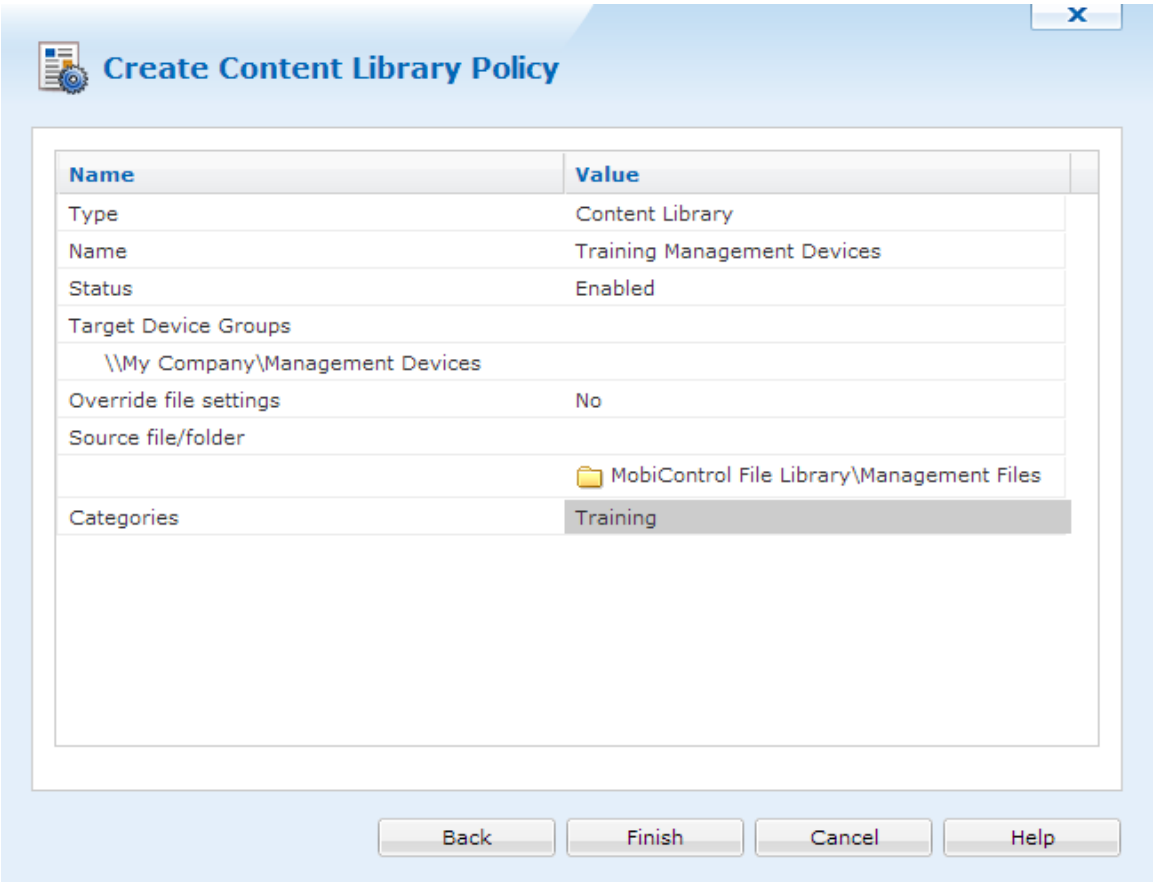
The next panel will allow us to override the file settings. If these settings need to be set, click the Override file settings checkbox.



Override File settings

Once the settings have been set, click Next.

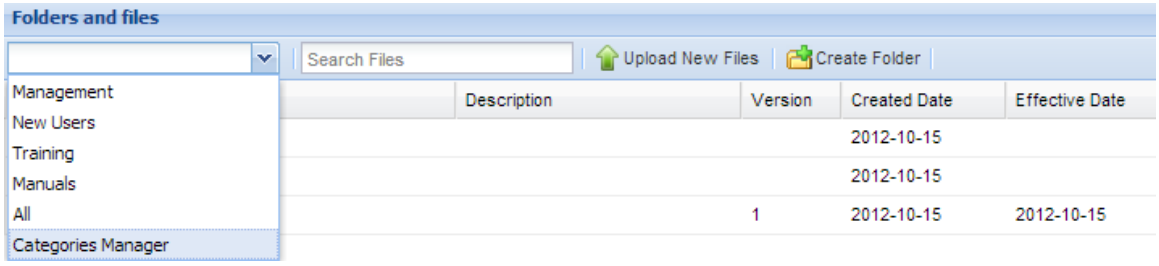
The final panel will show us a summary, click Finish to save and create this policy.



Content Library Policy summary

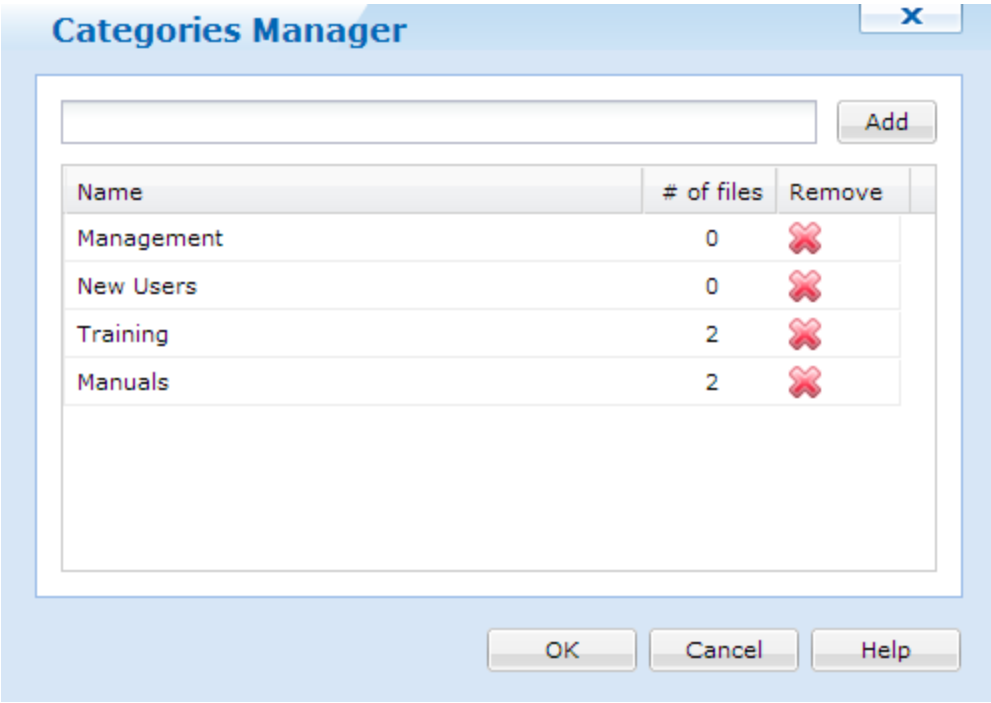
Categories Manager

To gain access to the category manager, click the drop box and select Categories Manager. This drop down list is located in the Folders and Files panel.



Categories Manager selection

Once selected, the Categories Manager dialog will open. Here we can delete previously created categories, and create new ones. We can also see how many files a category was tagged in.



Categories Manager

File Context Menu

When files have been uploaded to the Secure Content Library we are given additional options when we right click a file. Please see the "Secure Content Library - File Context" topic on page 1465 for more information.

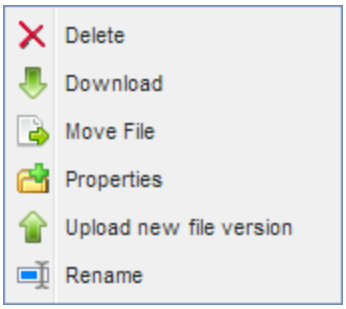
Secure Content Library

File Context Menu

When files have been uploaded to the Secure Content Library we are given additional options when we right click a file.

These options include:

- Delete
- Download
- Move File
- Properties
- Upload a new file version
- Rename

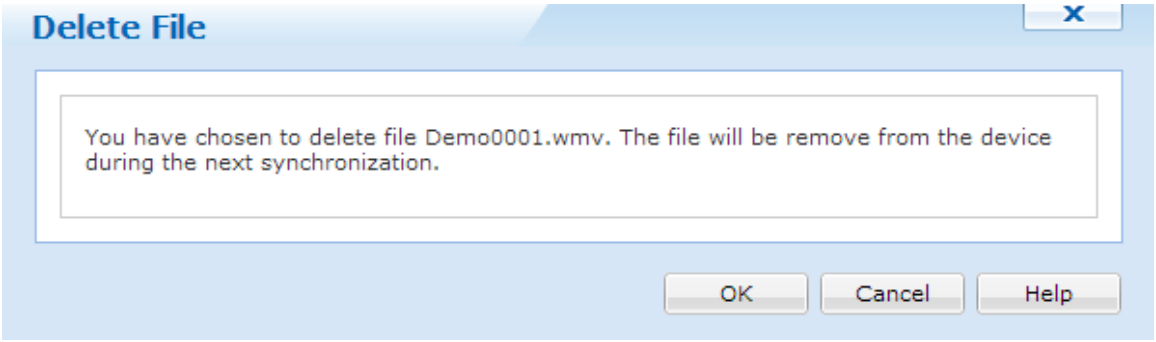


File Context Menu

Delete

Selecting delete will delete the file from the Secure Content Library. A confirmation dialog will appear asking for confirmation.

When a file is deleted from the Secure Content Library and it was already pushed to devices, the file will be removed from devices on the next synchronization.



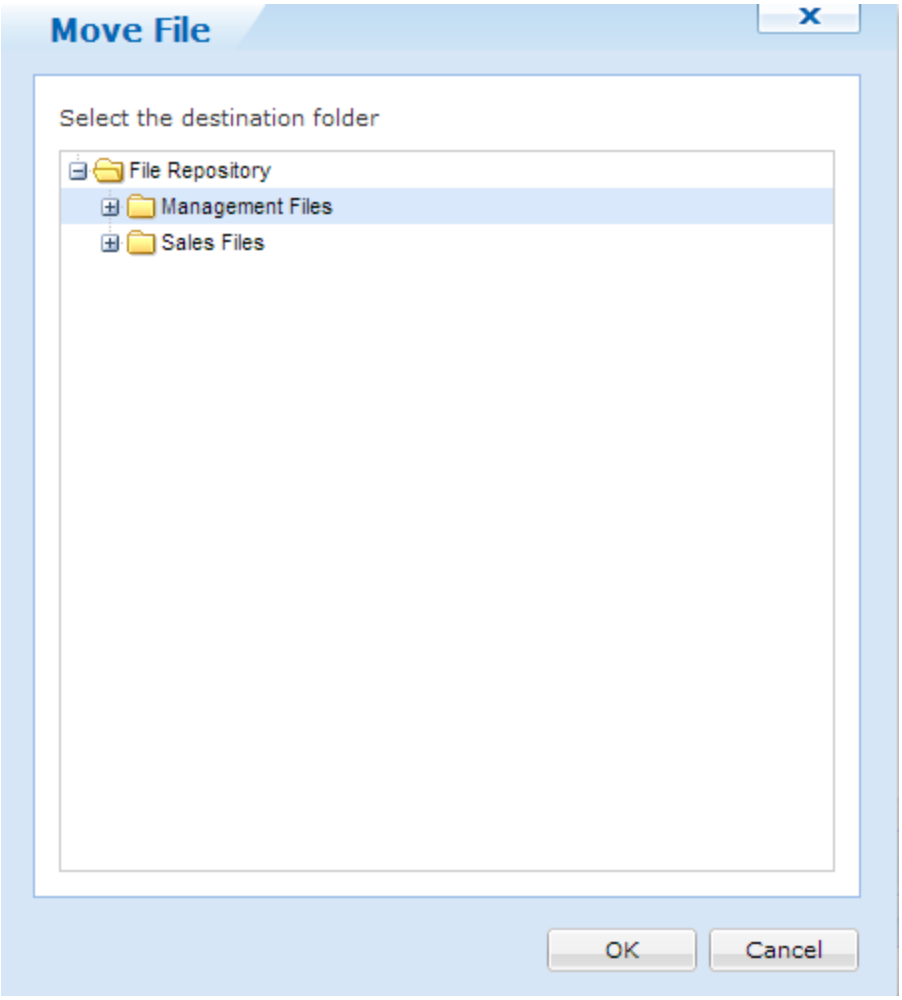
Delete dialog box

Download

Selecting download will download the selected file into the default download directory for your browser.

Move File

Selecting Move File will allow us to move the selected file to a different folder in the content library.



Move File dialog

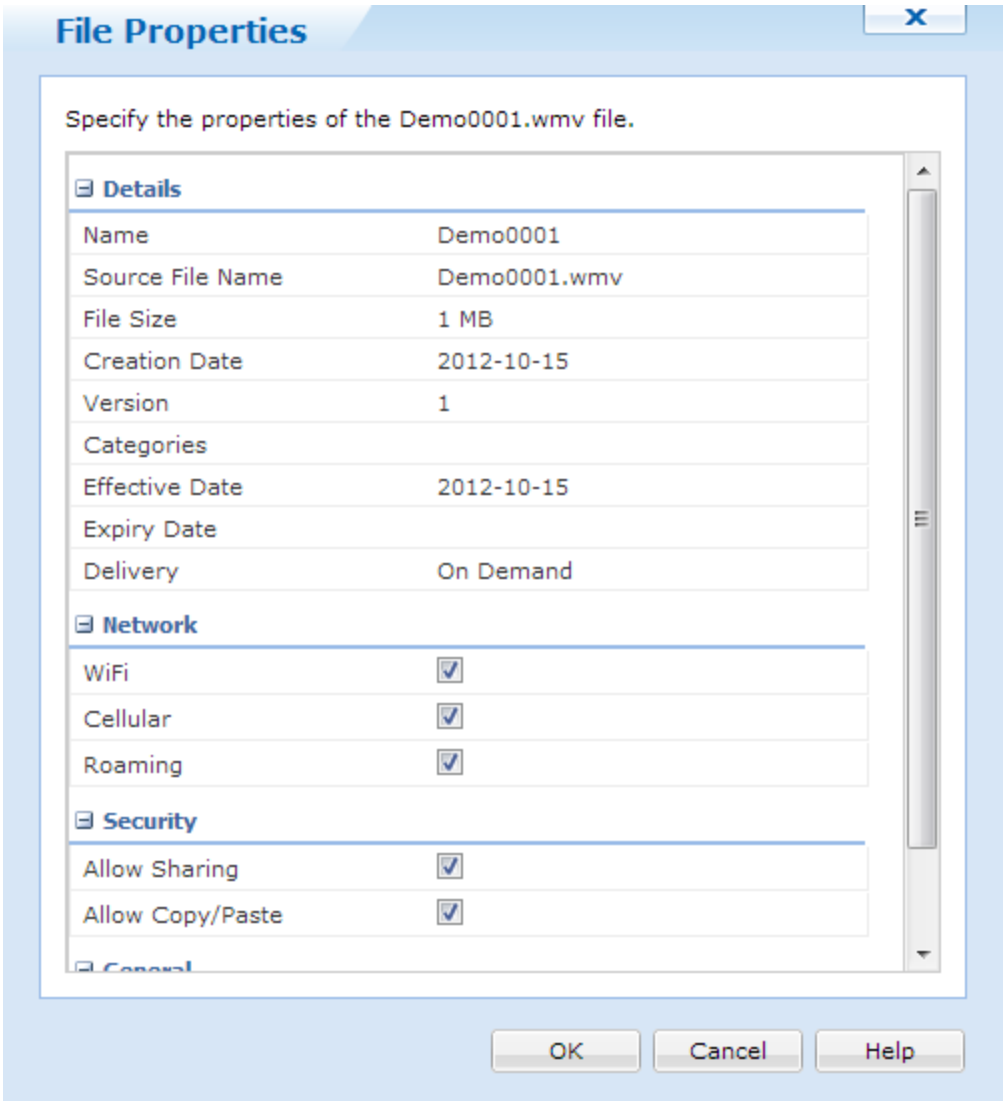
Properties

Clicking Properties will bring up the File Properties dialog. Here we can see all properties that is associated with this file.

Most of the settings here can be configured or edited.

NOTE:

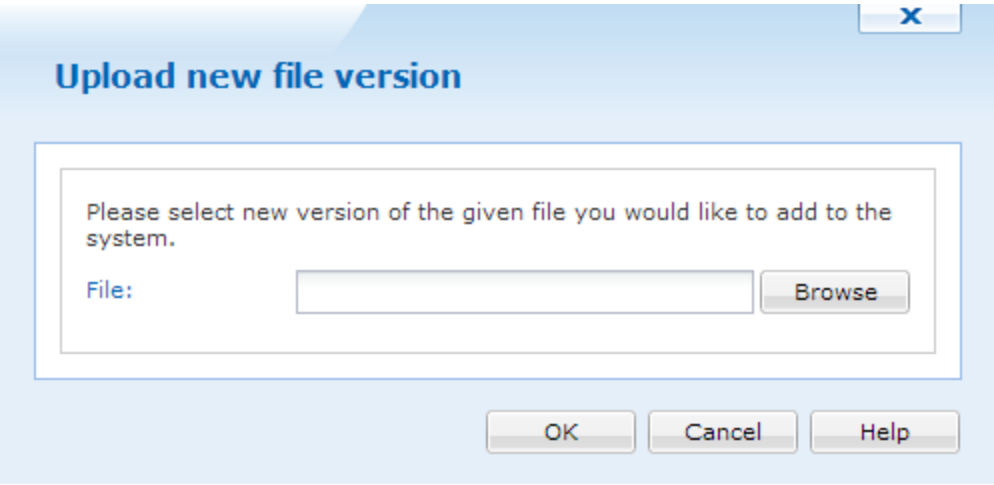
Security settings are only available for iOS devices.



File Properties

Upload new File Version

When we select the upload button, we are given the option to upload a new version of the specified file. When a new file version is uploaded, devices will be able to download the latest version.



Upload New File Version

Rename

Renaming allows us to change the display for the file type. This will not change the actual file name.

Configure Android Devices

The **Android** tab enables you to access the devices connected to the deployment running the Google Android operating system. All functions that can be performed on this OS are:

- Location Services
- Device Security
- Device Configuration
- Adding a Device
- Distributing software to a device
- Data collection functions
- Alerts

There are three views available for Android within the MobiControl web console. The views can be selected using the tabs at the bottom of the MobiControl Web Console user interface.

- The **Devices view (tab)** allows users to view information about configured devices, for instance packages installed, device ID, and IP address. The Devices view (tab) also allows users to control and configure devices, for example, to remote control a device or to change a device's name. For more information on the Device View, or Configuring your iOS device, please See "Android Advanced Settings" on page 1177 page.
- The **Rules view (tab)** allows users to view information about the configured rules. The Rules view (tab) also allows users to configure rules, for instance, create an add devices rule. For more information on the Rules view (tab) please See "Android Rules Tab" on page 1213 page.

- The **Reports view (tab)** provides users with a set of reports containing detailed information about the operation of the system. Provided reports include: deployment rule execution summary report, device configuration rule execution summary report, and device activity report. For more information on the Reports view (tab) please See "Android Reports Tab" on page 1264page.

Android Device Agent

Android Device Agent Installation Methods

The MobiControl Device Agent is the MobiControl software that is installed onto mobile devices. The Device Agent communicates with MobiControl Deployment Server(s) and carries out the instructions it receives from servers. Device Agents also provide reporting and real-time information to Deployment Servers.

Android Device Agent Installation from Google Play

1. Install the MobiControl Device Agent from Google Play by searching for MobiControl.

2. Once the Device Agent has been installed, enter the Enrollment ID provided when you create an add devices rule.

For More information on creating an add devices rule, please See "Adding Android Devices" on page 1216.

Android Device Agent Installation from Internal/External SD Card

1. Create an Add Devices Rule. For more information on creating an Add Devices rule, please See "Adding Android Devices" on page 1216

2. Download the .APK by right clicking on the Add Device Rule that was created and select **Download Device Agent**.

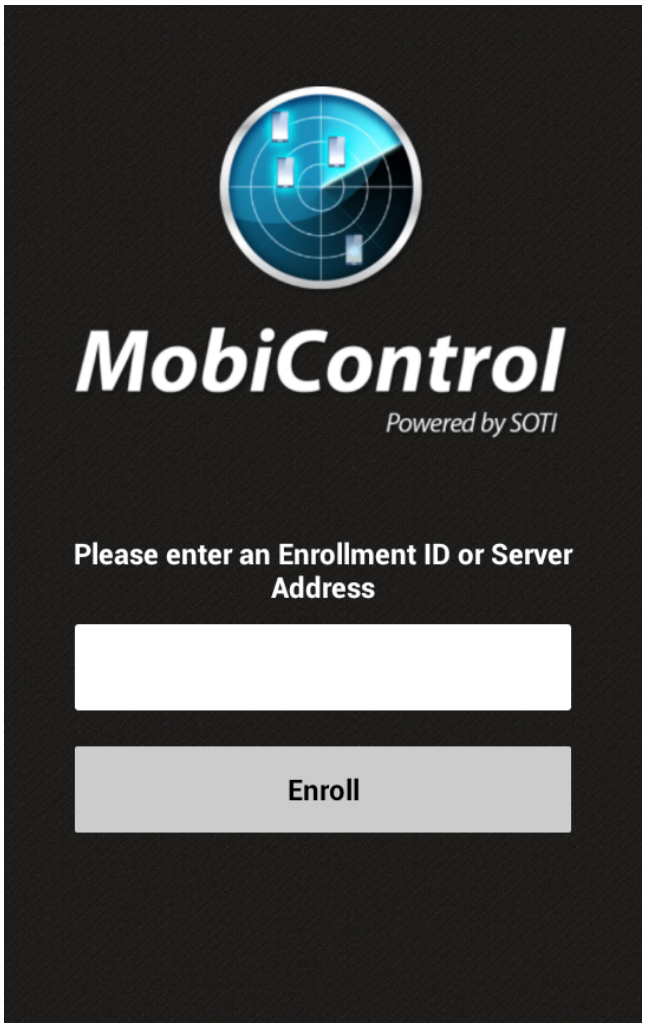
3. Download the .APK file and the MCSetup.ini and place them both in the root of the SD Card or in the Downloads folder.

4. Ensure that your device can install applications that did not come from Google Play. To do this, go to your device settings, select security and check off **Unknown Sources**.

5. From the device, using a file browser, navigate to the SD Card and select the APK to install it.

When using the MCSetup.ini the user will not be required to enter an enrollment ID as this information is stored within the .ini file. For more information on creating an Add Devices Rule please See "Adding Android Devices" on page 1216

Device Agent Configuration Applet



Once installed on the Android Device the Device Agent enables the user to connect or disconnect from the Deployment Server Server, as well as view the Application Catalog among other things. Please see the "Android Device Agent" topic below for more information.

Android Device Agent Uninstallation

The MobiControl Device Agent is installed on the device as a "Device Administrator", first step in uninstalling the Device Agent is to remove the agent as the "Device Administrator".

To remove the Device Agent as the "Device Administrator" and to uninstall the app, please follow these steps:

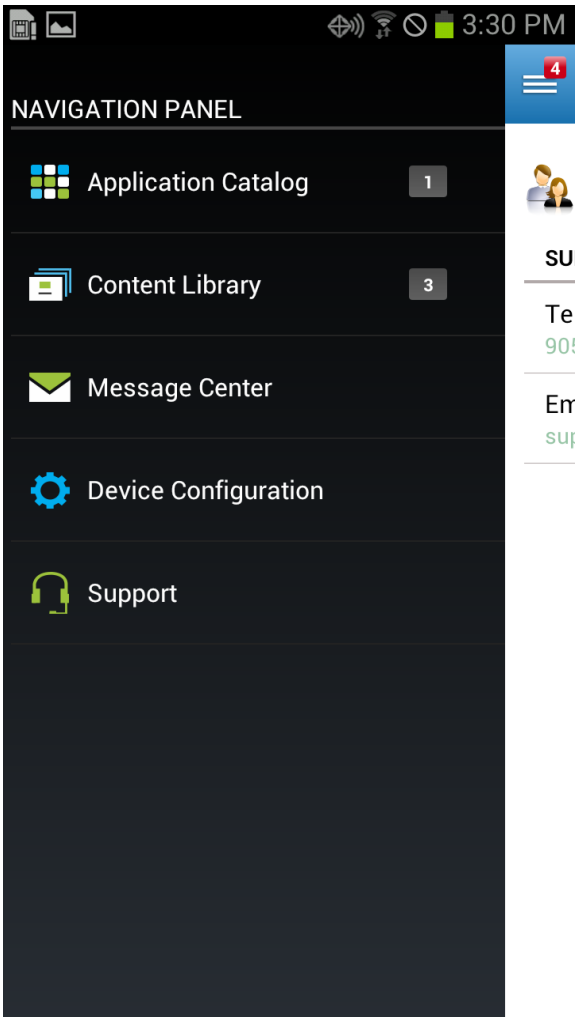
1. Go to your device settings and select **Security**.
2. Once in the Security settings, select **Device administrators**.
3. **Uncheck MobiControl**, this deactivates MobiControl as being a device administrator.
4. Once MobiControl has been deactivated , the app can be uninstalled like every Android app.
5. Go back to Settings and select **Applications**, select MobiControl and uninstall the application.

Android Device Agent

Opening the Device Agent will allow us to gain access to specific components of MobiControl. For the AndroidDevice Agent these components will be:

- Application Catalog
- Content Library
- Message Center
- Device Configuration
- Support

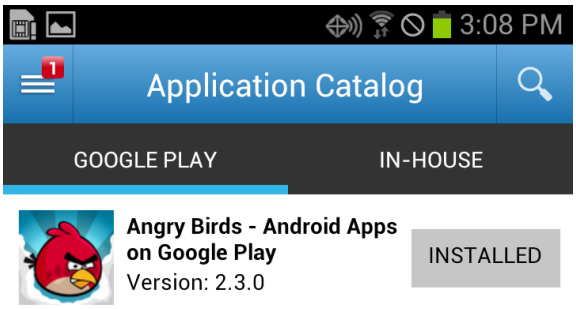
Tapping the menu button will show all these components on the left hand side.



Device Menu

Application Catalog

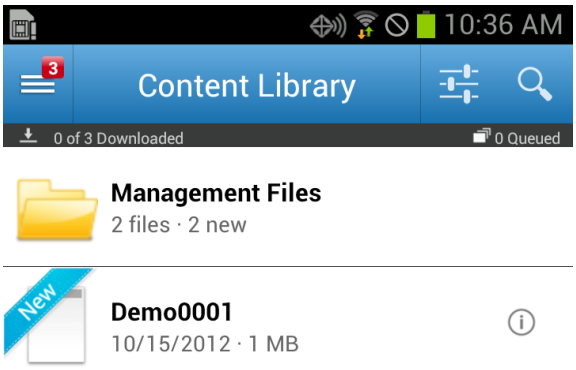
The application catalog menu will show the available applications, (App Store and Enterprise), that the device is able to download. Please see the "Android Application Catalog" topic on page 1222 for more information.



Application Catalog

Content Library

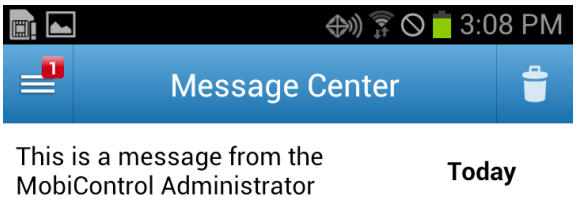
The content library tab will show all files that are available for download from MobiControl. Please see the "Secure Content Library Tab" topic on page 1456 for more information.



Content Library

Message Center

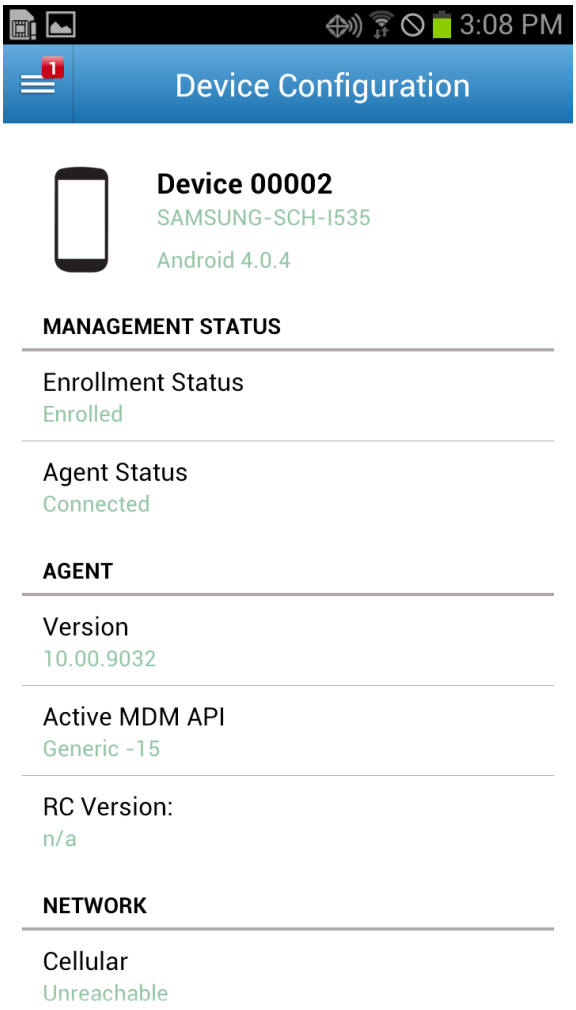
The message center will store all messages that were sent from MobiControl administrators. Users can tap each message to see the whole message.



Message Center

Device Configuration

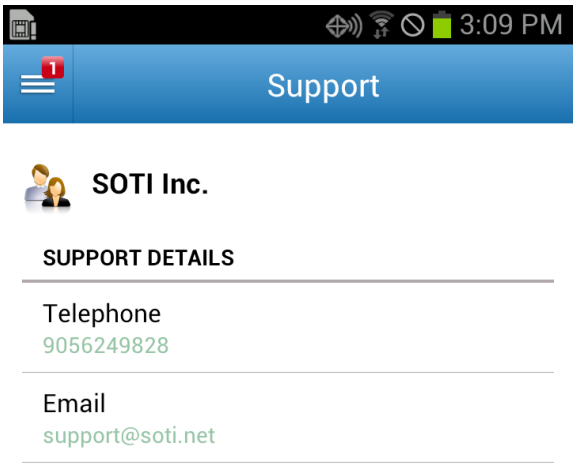
The device configuration menu shows all available information for the device. This includes the model type, Android version, enrollment status and other bits of information.



Device Configuration

Support

The support menu will show the items that were configured from the MobiControl web console. When a user taps either the phone or email items, it will open the respective application to complete the action. For example, tapping the phone item will open up the phone application. Please see the "Android Support Contacts Info" topic on page 1185 for more information.



Support

Android Devices Tab

The Devices view (tab) is the main view into the status of the devices in the MobiControl system.

Device Tree

The device tree provides a structured view of the devices in the system. The group structure is easily defined by the user by creating new groups and dragging and dropping devices between groups.

Commonly-reported device information can be easily referenced in the device tree window by right-clicking in any open space in the device tree window and selecting the information that you would like to see displayed.

Devices are added to the system by defining an add device rule and creating a MobiControl Device Agent that is installed on the device. Please see the "Adding Android devices" topic on page 1216 for a detailed explanation of how to add devices to MobiControl.

Info Panel

The Info panel provides detailed status information about the group or device that is selected in the device tree. When a group is selected, the displayed information includes the number of subgroups and how many unique, online, offline, or disabled devices are in the group. For devices, the displayed information includes device ID, IP address, battery and memory status.

The content displayed in this panel is stored in the MobiControl database. This information is refreshed when a device establishes a new connection to the MobiControl Deployment Server, and when you click **Refresh** or press F5 on this tab.

Logs Panel

The Logs panel provides a listing of the events occurring in the MobiControl system. This listing is filtered based on the group or device that is selected in the device tree. If only one device is selected, only the events related to that device are displayed. If a group is selected, events for the group and all the devices that belong to that group are displayed.

You have the option to show or hide logging, adjust the maximum number of logs displayed, and the frequency with which the Manager should refresh the log view.

Update Schedule Panel

The Update Schedule panel lists the dates and times when the device is programmed to query the MobiControl system to check for updates. By default, a device will also check for updates whenever it connects to the MobiControl system. Please see the "Android Device Update Schedule" topic on page 1186 for more information.

Installed Applications Panel

The Programs panel lists the applications that are installed on the device that is selected in the device tree. This is the same listing that is displayed by the **Manage Application** applet provided by the Android operating system. You can also remove the installed app through this panel; if a app is removed this way, a pop up will show on the device asking to uninstall the app.

Rules Assigned Panel

The Rules Assigned panel lists the file sync rule and Application catalog rules assigned to the group or device that is selected in the device tree. Rules are inherited from parent groups; a rule will apply to a device if it belongs to group to which the rule has been assigned.

The assignment of rules to groups provides a flexible and convenient means for easily configuring devices. For example, once you have set up your rules for software or data distribution, you can automatically provision your devices by simply adding them to the appropriate group within the device tree. Please see the "Android Rules" topic on page 1213 for information on creating deployment rules and file sync rules.

Notes Panel

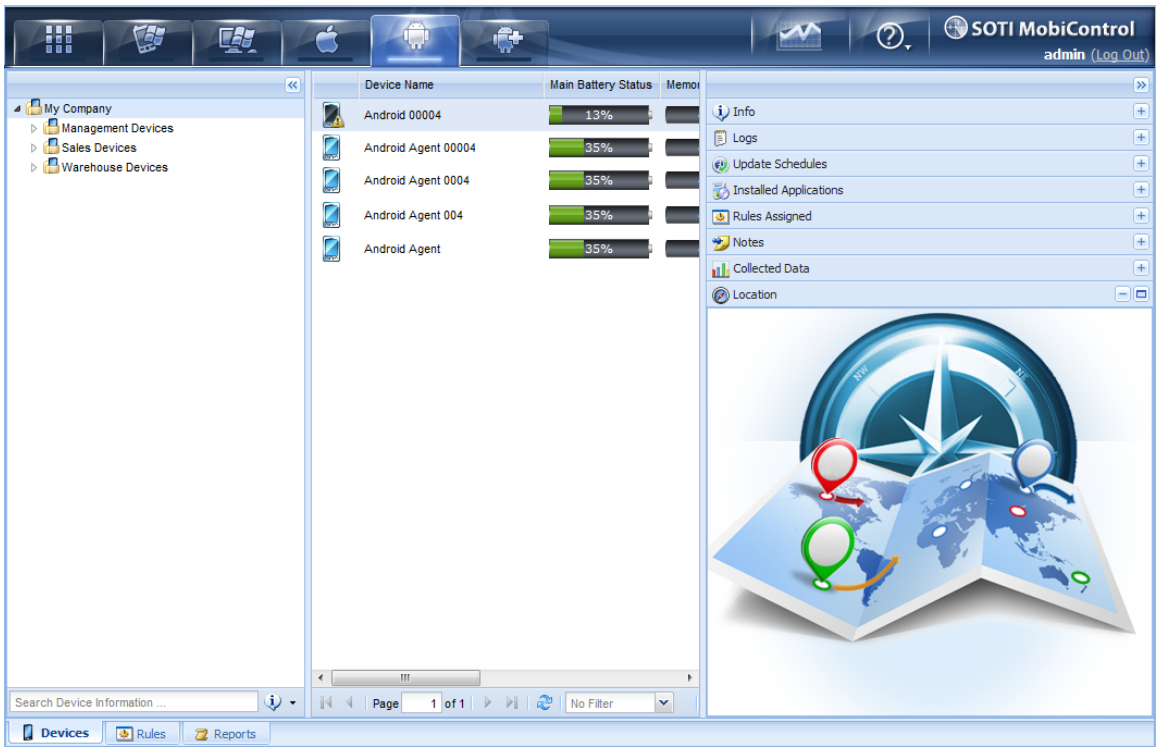
The Notes panel lists the notes that are associated with the selected device. If a group is selected in the device tree, all the notes for the devices that belong to the group are listed. Notes are a convenient way to maintain information about the device such as trouble tickets. Please see the "Device Notes" topic on page 1384 for information on creating device notes.

Collected Data Panel

The Data Collection Panel allows you to view the collected historical data for a set of devices. By creating a Data Collection Rule you will be able to specify which items to collect data from, how often to collect them, and when to upload the collected data to the server. Please see the Creating Data Collection Rules page for information on creating Data Collection.

Location Panel

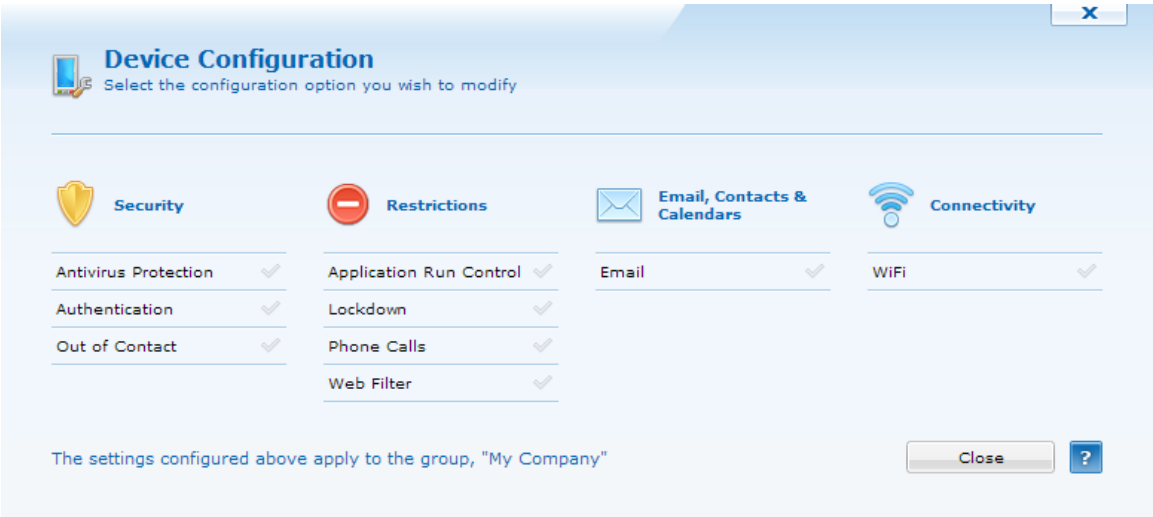
The Location Panel gives the ability to locate, track and gather information on the movement of your GPS enabled devices, no matter where they are in the world which is powered by Microsoft's Bing maps technology. Whether you need to confirm the current location of a particular field-worker, track the progress of an important shipment or collect historical information on the movement of a group of devices or vehicles in order to analyze performance, MobiControl's Location Services can help. Please see the Location Services page for more information.



Android Devices Tab - Devices view (tab)

Android Device Configuration

MobiControl offers several device configuration options ranging from password authentication, user interface lockdown (also known as "kiosk"), and the ability to configure the device to automatically react to security threats such as repeated failed login attempts, even if the device is out-of-contact or in an offline state.



Android Device Configuration dialog box

MobiControl's security provides powerful features for configuring devices and mobile data, while maximizing usability and making configuration implementation easy, efficient and cost-effective. Salient features of MobiControl's security include:

- Over-the-Air (OTA) security policy distribution
- Policies can be assigned at the individual device, group or global level
- Configuration managed for both online (connected) and offline (disconnected) devices

To access Android Device Configurations, select the device or group of devices for which you want to configure security and then click **Device,** click **Configure Devices,** and click **Security.**

Security

Restrictions

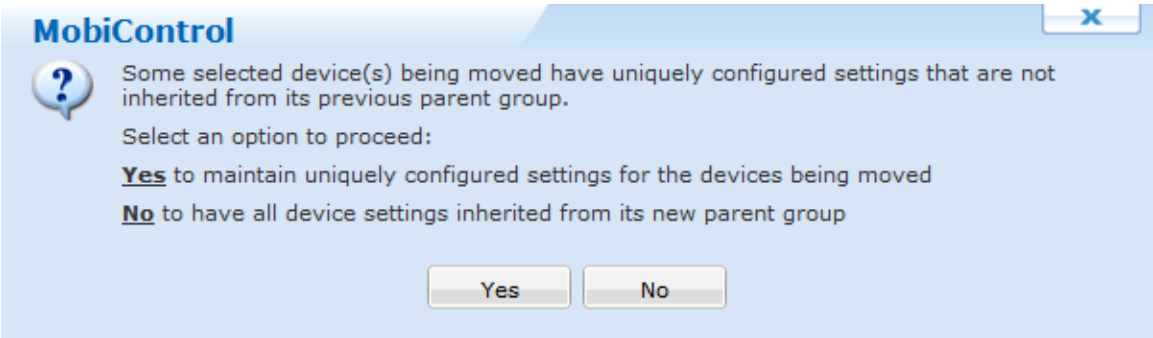
Email, Contacts & Calendars

Connectivity

Configuration Override Settings

Override settings allows you to create unique configuration settings at the current level which you have selected. This will override the settings that the device or group was previously inheriting from the parent group.

If the configuration settings are different at any sublevel (be it device or subgroup) then a confirmation prompt will allow you to choose whether the current setting(s) should be applied to all sub devices and groups or only the level that inherit configurations from this group.



Android Antivirus Protection

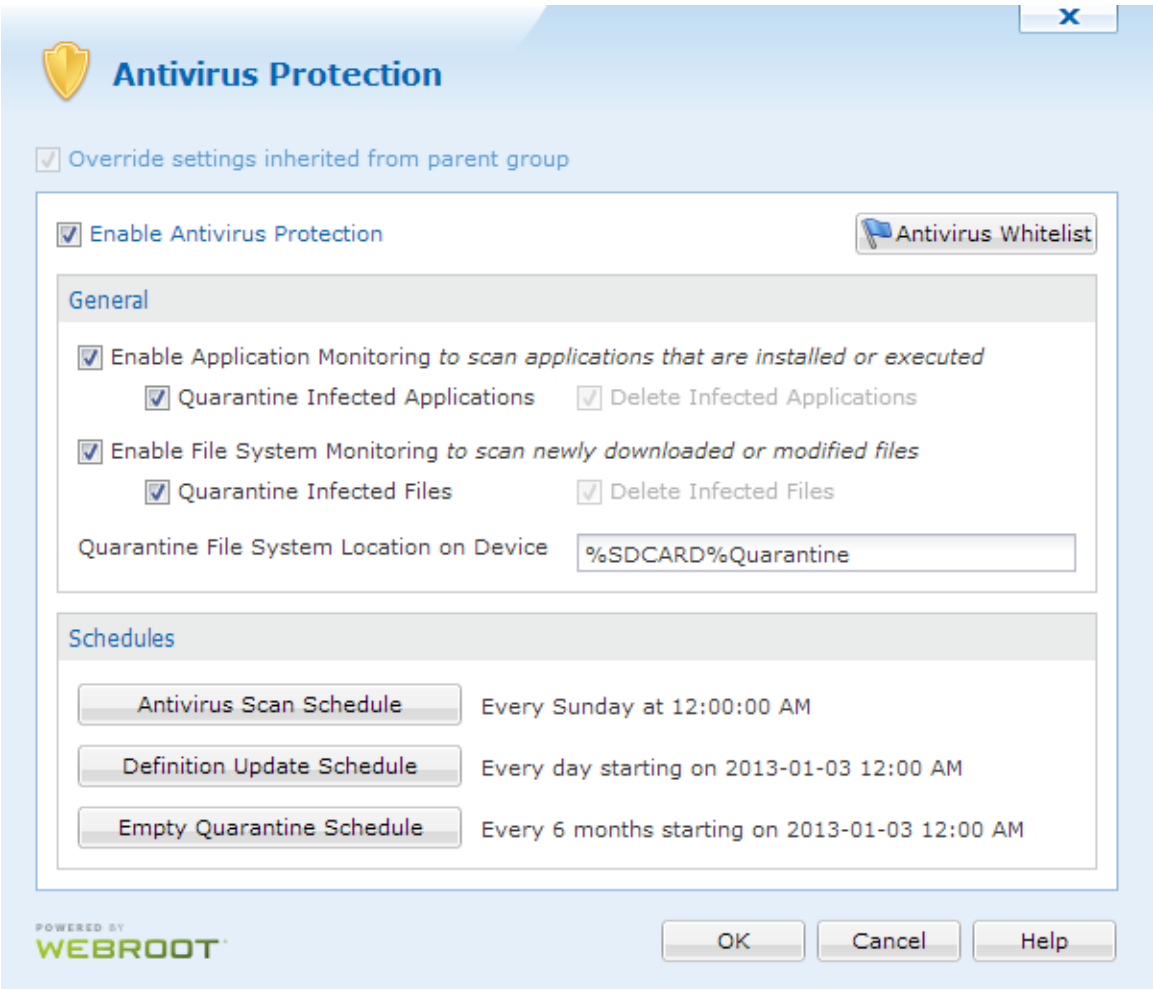
MobiControl's Antivirus protection policy allows us to monitor files and applications on devices. Scans can be configured from every 2 minutes to as much as once a month.

This is done by scanning apps and files against virus definitions, very similar to a Windows desktop antivirus application. Virus definition updates can also be configured to download new definitions based on a schedule.

When an infected file or app is found on the device, MobiControlhas an option to move these files to a special folder on the device's SD card. When it is moved to the folder, it is then deleted from the Android system. This folder can be configured to anywhere that is desired. When infected files or apps are in this folder, we can see a list of all quarantined items in the Web Console.

If a certain application is quarantined by mistake, we can create a whitelist to halt any further quarantines of the application or file.

Click **Enable Antivirus Protection** to enable this feature.



Android Antivirus Protection.

General Settings

If **Enable Application Monitoring to scan applications that are installed or executed** is selected, then MobiControl's Antivirus protection will monitor any applications that are installed. Also, if an application is launched, it will again be scanned. Having **Quarantine Infected Applications** checked will allow MobiControl to move the infected application to the quarantine folder specified.

If **Enable File System Monitoring to scan newly downloaded or modified files** is selected, then any file that is downloaded or modified will be scanned for viruses. If they are infected, they will be moved to the quarantine folder specified.

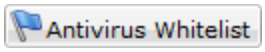
It is recommended to leave the quarantine folder as the default, but it can be changed to any folder needed.

Schedule settings

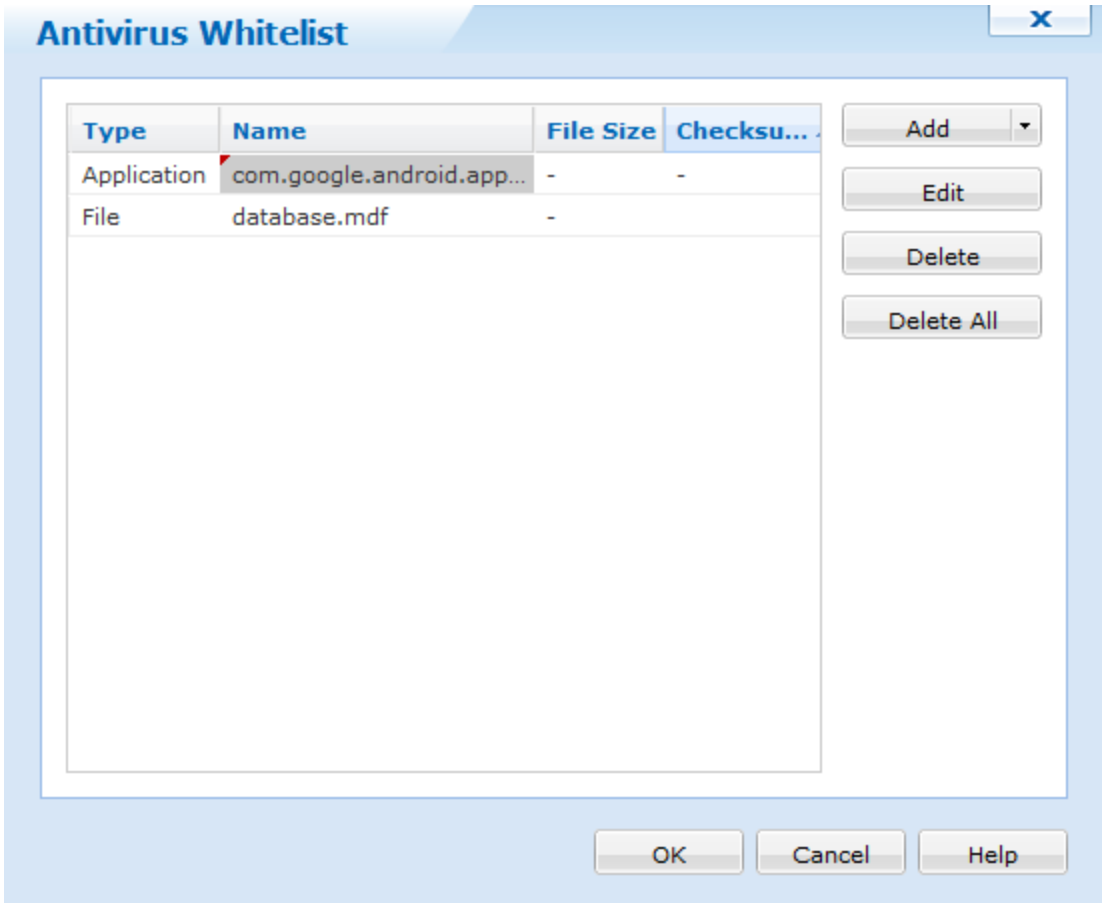
Clicking each of the scheduling buttons allows us to change the frequency of when they are active.

- **Antivirus Scan Schedule**
- **Definition Update Schedule**
- **Empty Quarantine Schedule**

Antivirus Whitelist

The Antivirus Whitelist allows us to exclude certain applications or files from the virus scans. This can be done by clicking the 

button. From here we can specify which applications or files are going to be excluded.



Antivirus Whitelist

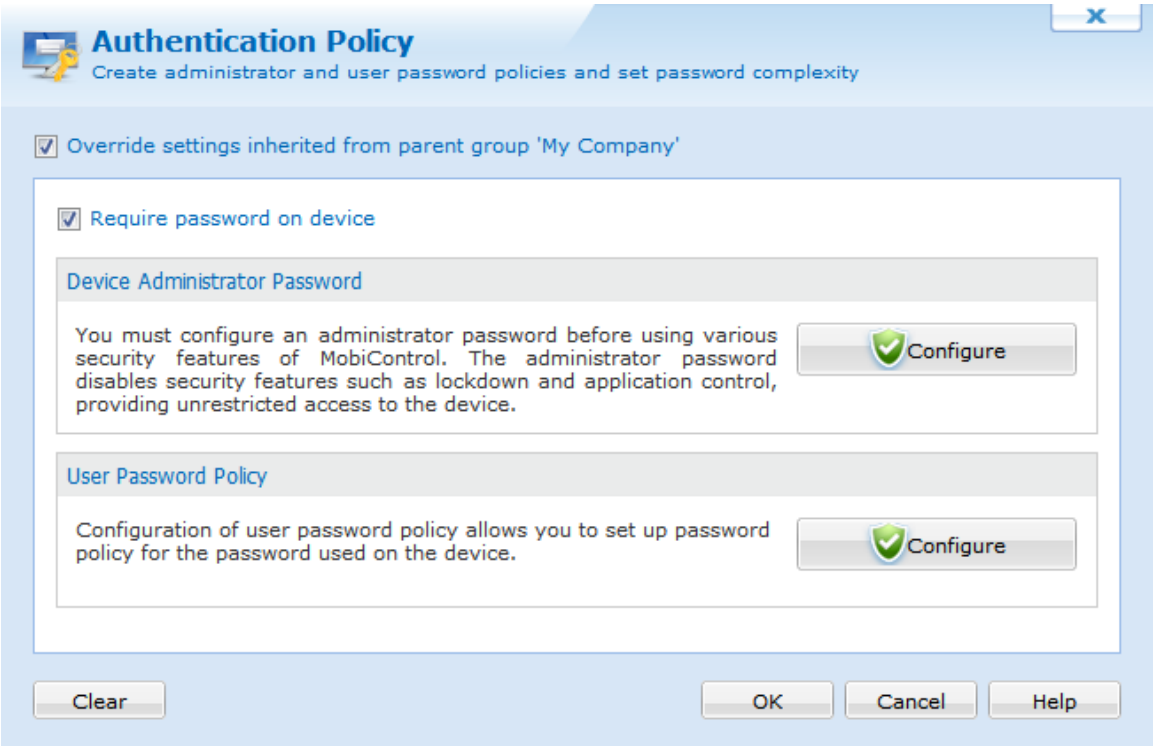
Configuring the Antivirus Whitelist

After all configurations are done, click OK to apply the configurations.

Android Authentication Policy

The Authentication Policy option in the **MobiControl Security Center** dialog box allows administrators to manage device-side, password-based user authentication.

To enable Authentication Security for a device or group of devices, select **Authentication Policy** from the MobiControl Security Center. (Please see the "Android Device Configuration" topic on page 1137.)



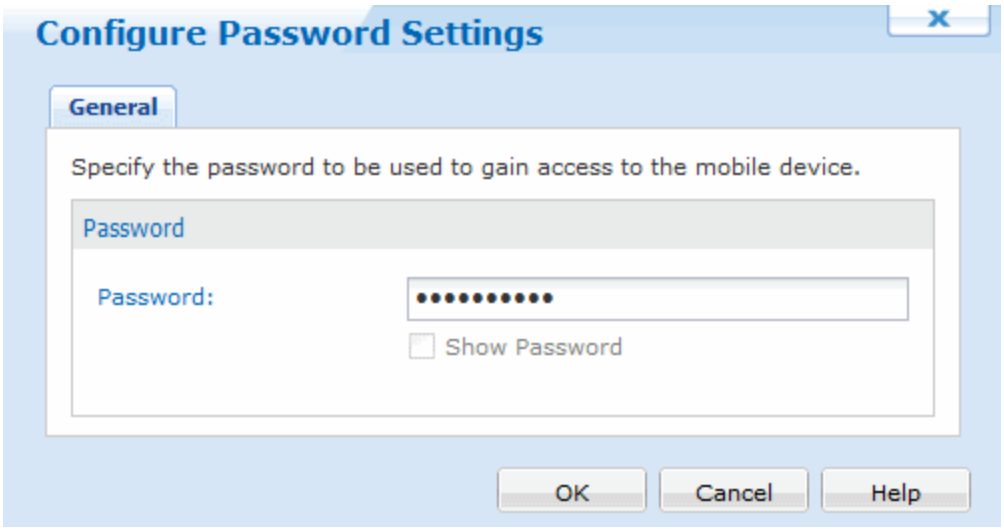
Device Authentication Configuration dialog box

Administrators can configure an administrator password and a user password. When the administrator password is entered, the device is unlocked so that the administrator has complete access to the device. When a user password is entered, the user will have access to only those programs that the administrator has configured. An administrator can allow users to run all programs or only specific programs. Please see the "Android Lockdown" topic on page 1151 for more details.

Field Name	Description
Device Administrator Password	Configures the Administrator password for the Android devices.
User Password Policy	Configures the User password policy for the Android devices.

Device Administrator Password

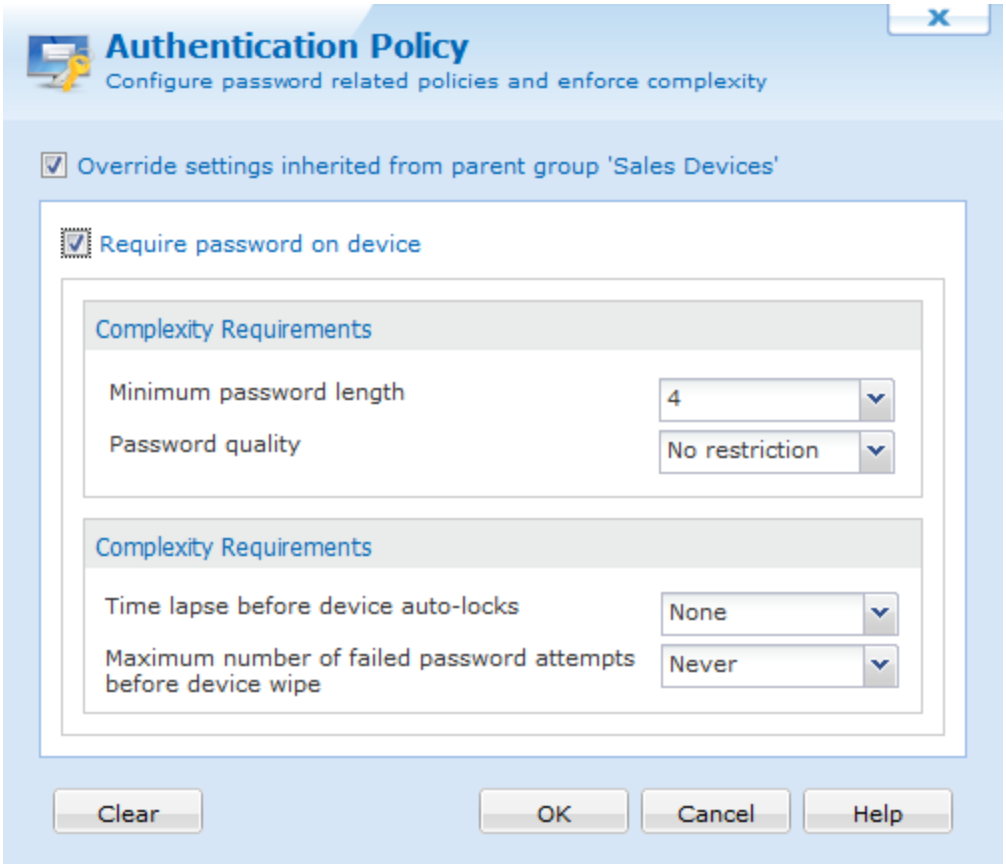
To specify an administrator password, first ensure that the **Require password on device** box is checked, and then click the **Configure** button in the administrator password section. This will bring up the dialog box below. Enter the desired password in the two provided text boxes and click **OK**. The configuration of the Administrator password is a prerequisite for all the other security configurations. To get to this screen you must click on the **Options** button, then select **Administrator** and click **OK.**



Administrator password settings dialog box

Device User Password

To specify a user password, first ensure that a **Device Administrator Password** has been setup, and then click the **Configure** button in the use password policy section. This will bring up the dialog box below. Enter the desired password policy configuration in the provided sections, as displayed below, and then **OK**.



User password policy settings dialog box

Complexity Requirements

To configure a user password, first ensure that the **Enable Password Authentication** box is checked. The **Complexity** dialog box allows you to specify the password complexity requirements for the user password on the Android device.

Field Name	Description
Minimum Password Length	Specify how long the user password must be on the Android Device.
Minimum Password Quality	Specify the password quality by requiring Numbers, Letters, or Number and Letters.
Minimum number of complex characters allowed	Specify how many special characters are required for the user password.

Policy

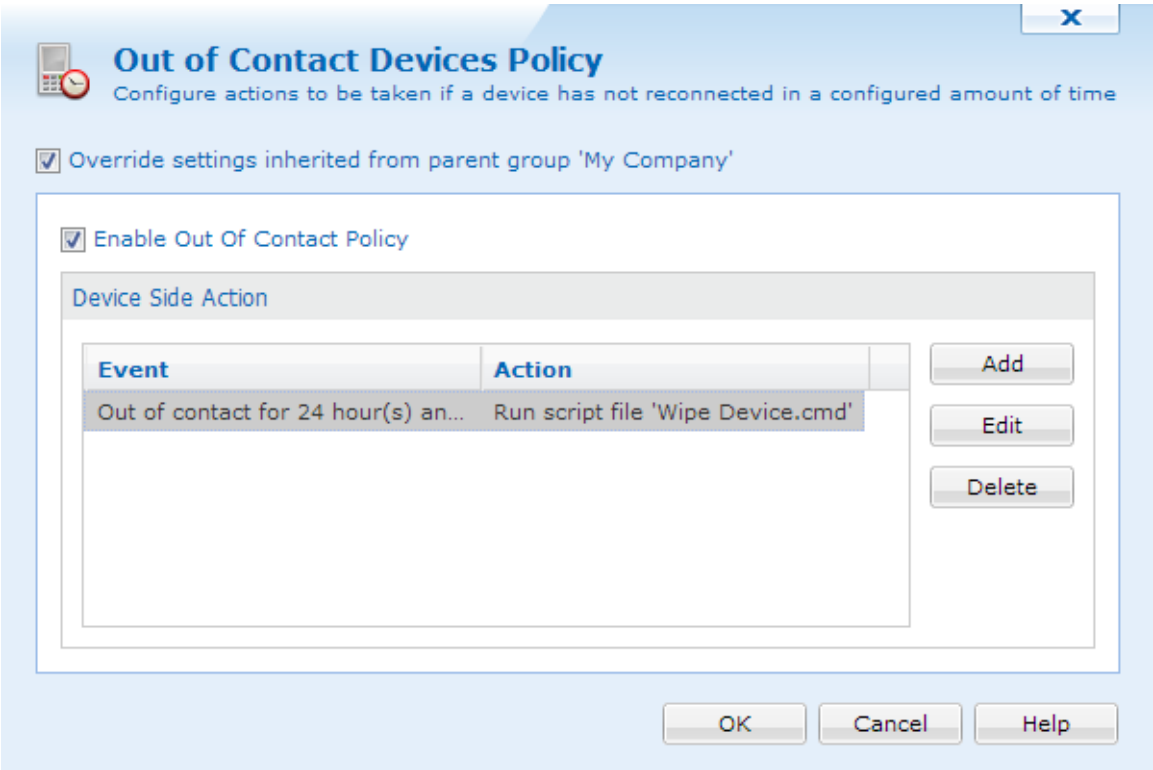
The **Policy** dialog box allows you to specify the password policy requirements for the user password on the Android device.

Field Name	Description
Time lapse before device auto-locks	Specify how long the device will stay unlocked while off. The device will automatically lock again after the expired time.
Maximum number of failed password attempts before device wipe.	Specify how many times an incorrect password can be entered on the device before it automatically wipes itself.

Android Out of Contact Devices

The out-of-contact devices policy dialog box allows you to manage "out-of-contact" devices which are not able to connect to the MobiControl Deployment Server. This feature can be used to define security actions that can be triggered if a device has not contacted the MobiControl server for a specified time interval, or has been lost or stolen and appears as offline in the device tree.

To enable the out-of-contact devices policy for a device or group of devices, select **Out of Contact Devices Policy** from the MobiControl Security Center. (Please see the "Android Device Configuration" topic on page 1137.)



Out of Contact Device Security Policy dialog box

EXAMPLE:

If a device does not contact the server for two days, you can configure it to be wiped to avoid losing any sensitive data on the device. Other actions and standard script commands can also be executed.

To add an event for which security actions can be specified, click the **Add** button. Click on the **Edit** button to modify an existing event or an action. Click on **Delete** to remove an event and its corresponding action from the list.

Action	Description
Add	To add an event for which security actions can be specified.
Edit	To modify an existing event or an action. Clicking this button presents the option to edit an action or the corresponding action.
Delete	To remove an event and its corresponding action from the list.

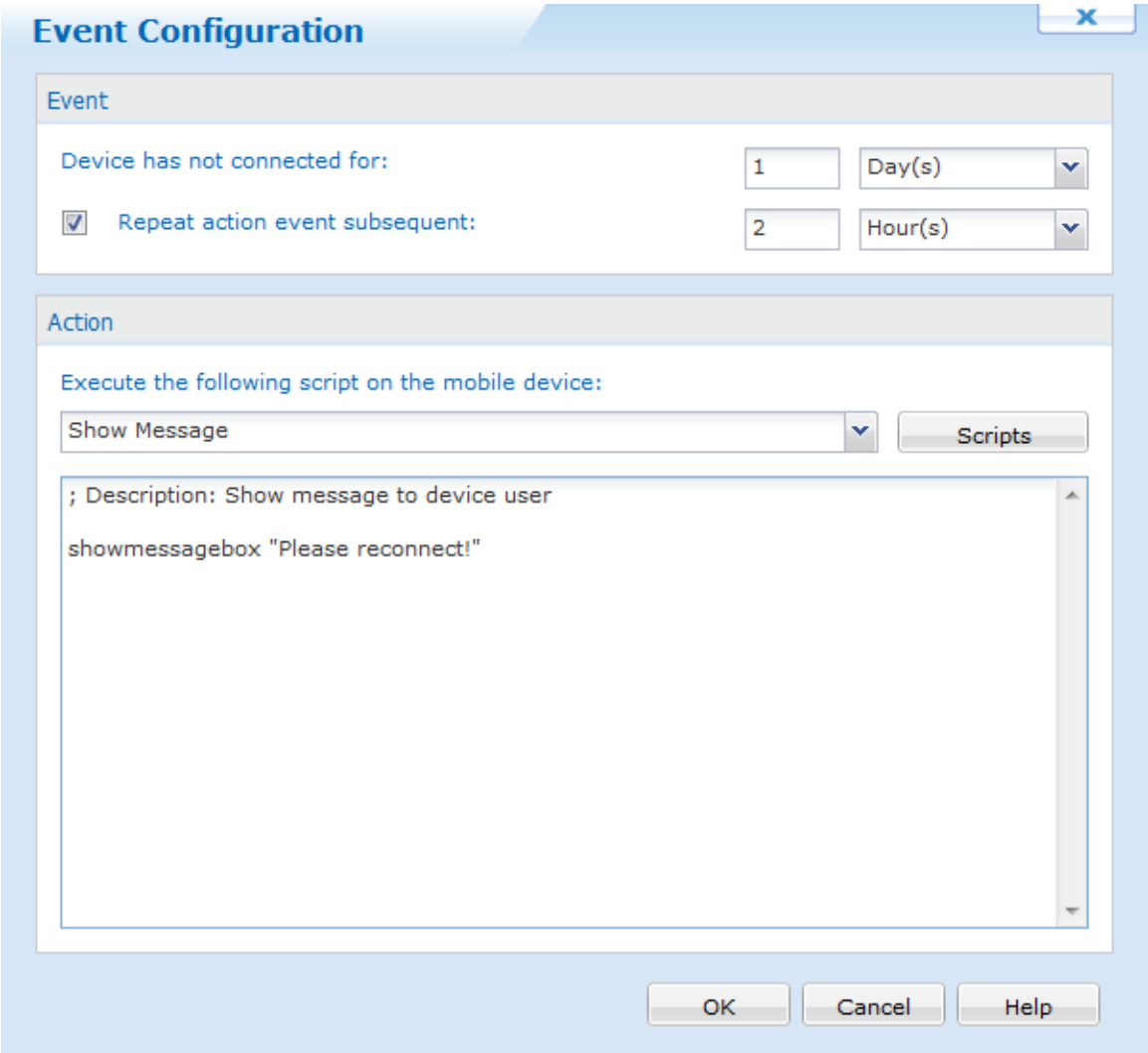
Add Event

To add an event, click the **Add** button to bring up the **Out of Contact Event Configuration** dialog box. Specify the time interval after which an action (or a script) should be triggered if the mobile device has not connected to the MobiControl Deployment Server (which is indicated by the device appearing as online in the device tree). This can be in minutes, hours, days or weeks.

If **repeat action event subsequent** is selected, actions can be repeated after the initial time out.

EXAMPLE:

If the out of contact policy is to be triggered if the device hasn't connected for 1 day, and repeat action event subsequent is configured for 2 hours, the out of contact policy action will be triggered every 2 hours after the initial trigger.



Out of Contact Event Configuration dialog box

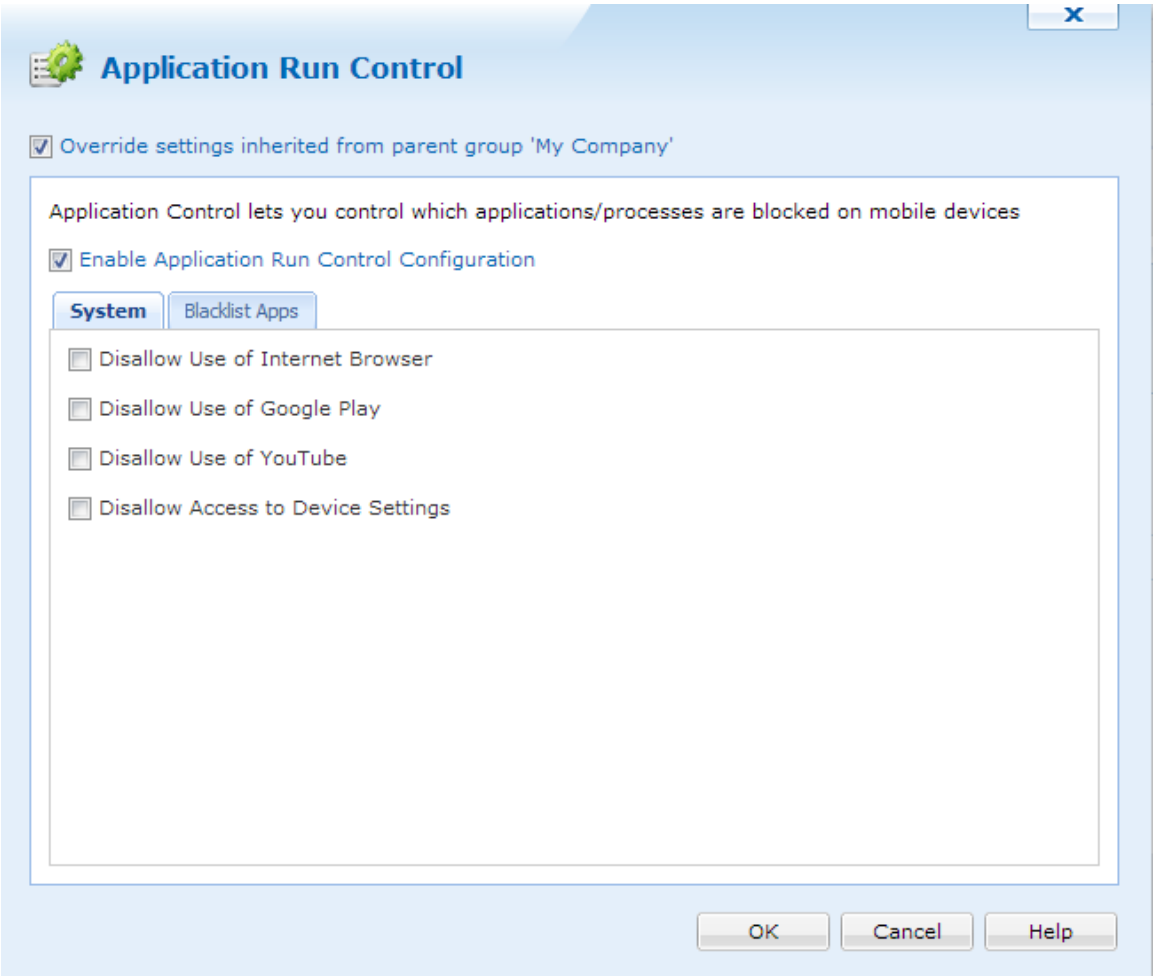
After you have specified the time interval, select a script to execute, or click **Scripts** to bring up the **Manage Scripts** dialog box. Please see the Script Manager page for further details.

Once everything is configured, click **OK**.

Android Application Run Control

The easy availability of applications—games, consumer-oriented utilities and third party tools—for mobile devices results in end users installing and running unauthorized personal programs and recreational software on devices meant for business use. In addition to contributing to memory and battery life overhead, this situation also contributes to productivity losses. The installation of unauthorized and unapproved non-business applications contributes to a significantly higher volume of support calls, increasing the IT help desk's support burden. Most critically, it is imperative for security-conscious users to control and restrict the unauthorized installation of personal applications to ensure compliance with strict mobile data protection requirements.

MobiControl's application run control features reduce the risk of leakage of sensitive data and complement the existing network security model by preventing the introduction of malware and viruses into the network through the mobile devices. Additionally, it also allows memory management on the mobile devices to free up resources taken up by unnecessary processes, and allowing for better device performance. MobiControl integrates tightly with the operating system to prevent restricted applications from running entirely on the mobile device, making it much more efficient than competing white list and black list solutions which use CPU and battery-consuming processes to monitor for and destroy restricted applications.



Application Run Control dialog box

Block System Apps

MobiControl has the ability to block certain system apps. These apps include the default Internet Browser, Google Play, Youtube and accessing the device settings.

If more applications are needed to be blacklisted, please see below.

NOTE:

For all Nexus devices, MobiControl does not recognize Chrome as being the default browser. If Chrome is needed to be blocked, please use the use the blacklist section.

Blacklist Apps

The **black list**, or list of restricted applications, allows IT administrators to ensure that an application will not be allowed to execute on the device. The MobiControl Device Agent prevents any black-listed processes from executing on the device.

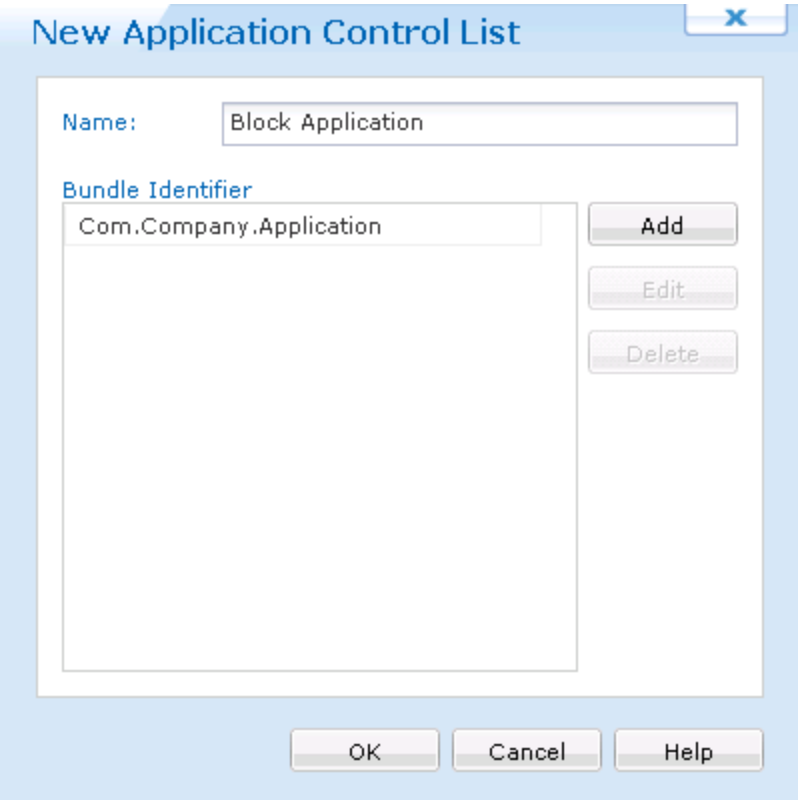
To enable application run control for a device or group of devices, select **Application Run Control Policy** from the MobiControl Security Center.

NOTE:

If an application is being run from the lockdown, and it is blacklisted on the device, the application will still run as the lockdown takes precedence over the blacklist.

Control List Creation Methods

Configuration of application run control begins with the creation of an application control list. An application control list is simply a listing of the names of the Package ID's (Bundle Identifiers) that correlate to the application you wish to disallow on the mobile device. For example, `com.google.android.talk` corresponds to Google Talk, and `com.android.providers.calendar` corresponds to Google Calendar for Google Android.



Application Control list

You can manually create a new application control list by clicking the **New** button in the **Application Run Control** dialog box, and then choosing the **New** option in the **Select Control List Creation Method** dialog box. The **New Application Control List** dialog pops up, allowing you to specify the application that you want to add to the list.

Now the application run control list has been created, you may assign it to various devices and groups.

IMPORTANT:

Application run control can adversely impact the operation of the mobile device if configured incorrectly. After you have developed a control list, apply it to one or two select devices for extended field testing before expanding it to the general deployment. As a general rule, if you don't know what the application or package ID does (e.g. `com.company.application`), allow it to run instead of blocking it as it might be critical for the device's proper operation. You do have the potential to brick the device by blocking incorrect package IDs.

Modifying or Deleting a Control List

An application control list can be edited whether it is currently in use or not.

An application control list can only be deleted if it is currently not selected for any devices or device groups. A control list that is listed in the **Selected** field is considered in-use, even if the application run control is disabled for the given group or device.

NOTE:

If you edit an application control list that is shared among device groups that are not subgroups of the group you are configuring, the changes will not be propagated to the other devices. The modified control list will

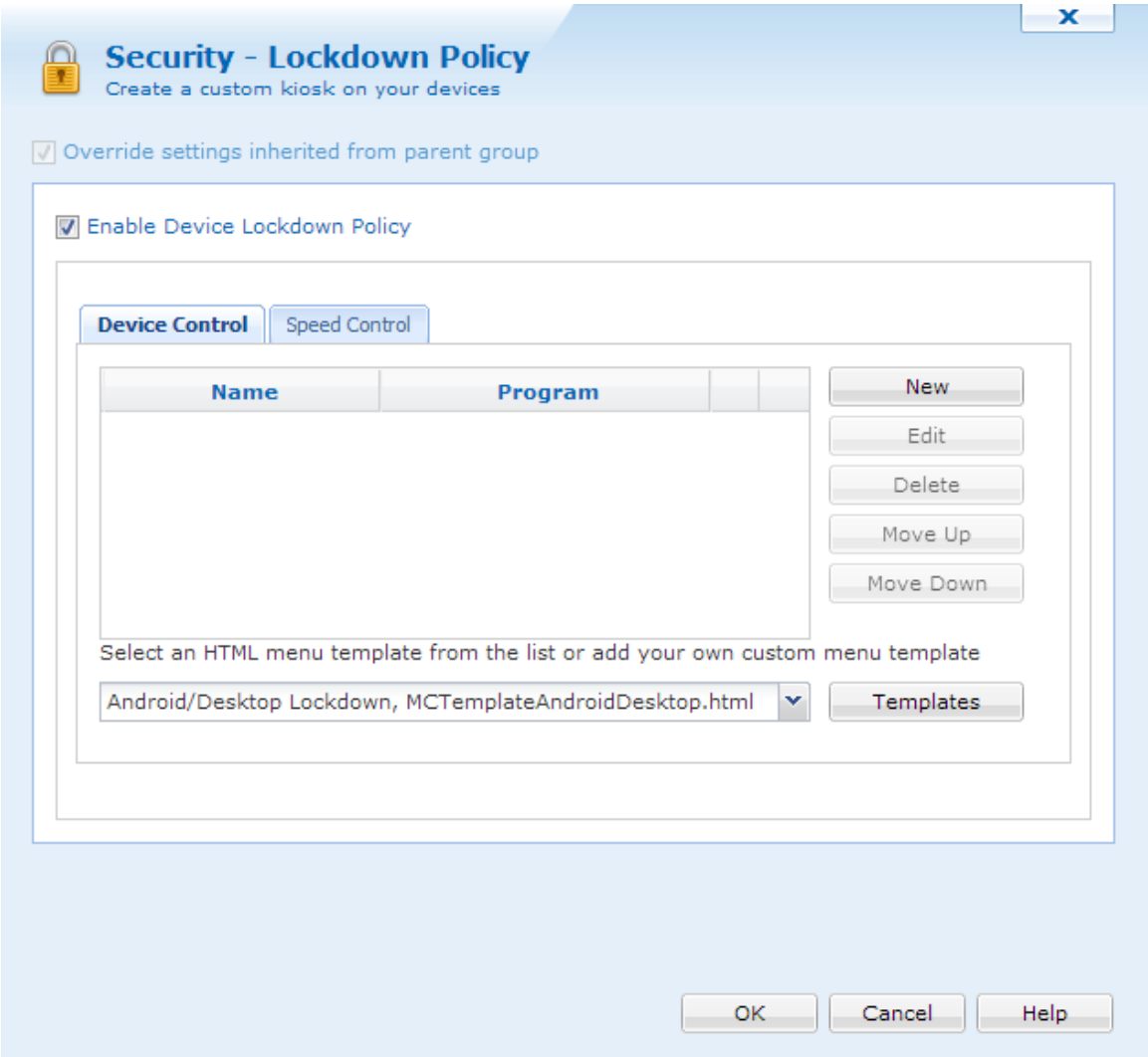
NOTES:

- When logged in as Admin on the mobile device, application control enforcement is suspended.
- Certain processes and applications are critical and necessary for stable device operation and normal execution of the MobiControl Device Agent.
- Applications that are included in a lockdown program menu are automatically on an accept list, and cannot be put on a black list.

Android Device Lockdown

Device lockdown replaces the standard device home screen with a customizable home screen. Users have access only to authorized applications and websites, and are prevented from accessing all other applications and device controls.

Please see the "Android Speed Lockdown" topic on page 1155 for more information about the Speed lockdown.



Lockdown Policy dialog box

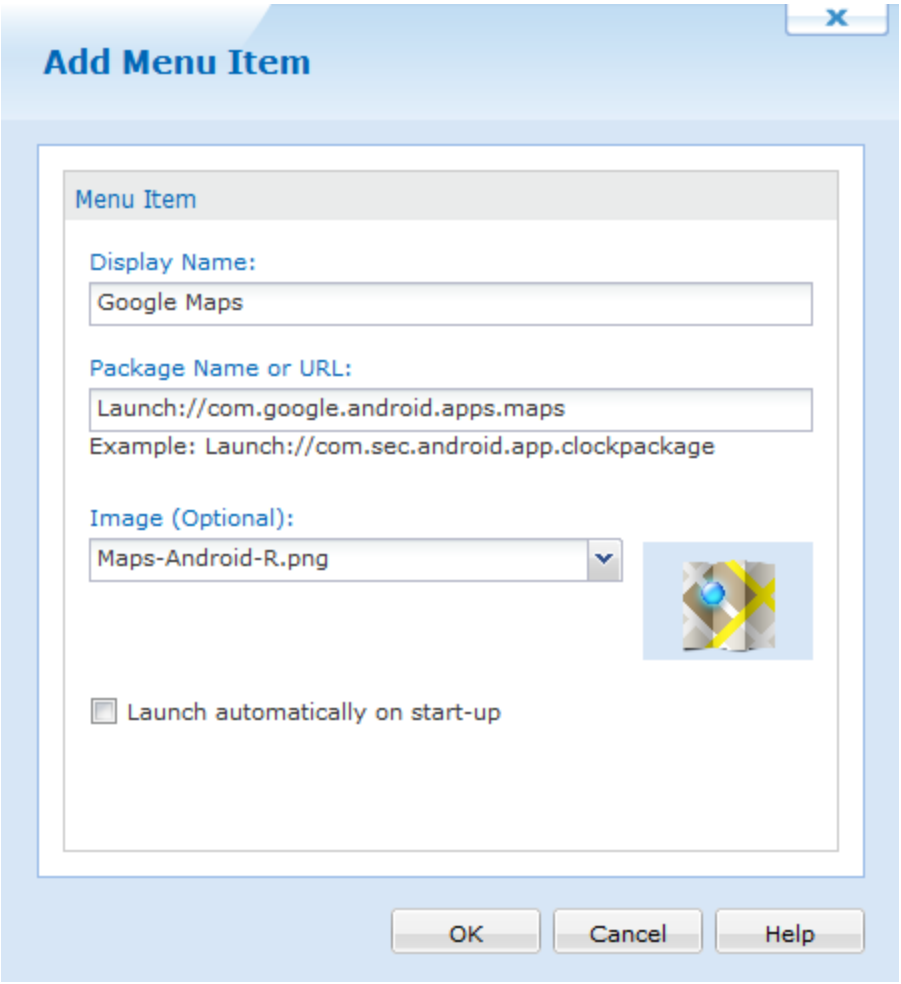
By locking down devices, organizations can minimize the risk of unauthorized persons accessing information on their mobile devices. Administrators can control exactly which programs users are allowed to run, and which websites they are allowed to visit. This decreases the amount of down-time caused by users changing settings that may adversely affect the operation of the device or application software, and also decreases support costs. MobiControl allows running the mobile devices in a kiosk mode with a read-only access to provide critical information to the end users, without giving them access to change the settings.

The lockdown menu can only be dismissed by an administrator. Specification of a user password is optional. If not configured the device user can access the lockdown menu directly after turning on the device. If a user password is defined, then the password must be entered in order to access the lockdown menu.

To configure lockdown settings for a device or group of devices, select the target device or group in the device tree view in the main console window and select **Security** from the **Configure Device(s)** submenu.

Field Name	Description
Enable lockdown menu	Use this checkbox to enable or disable the device lockdown menu.

Field Name	Description
Device Program Menu	The device program menu is a list of programs and websites to which the user has access. There are pre-configured HTML menu templates that can be edited or applied to the menu, and an option to enable or disable the launching of a menu item with keyboard shortcuts. Please see the Device Program Menu section below for details.
HTML menu template	Select a menu template from the drop-down list. Please see the Templates section below or the "Customizing Android Lockdown Menu Templates" topic on page 1158 for more information.



Add New Menu Item dialog box

TIP:

- If you link to a search engine the end user will gain full access to the Internet.

Device Program Menu

Use the **New** button to add menu items. Each entry consists of a user-friendly name and a complete file path to the executable, `.lnk` shortcut file, `.cmd` script file, or website address (URL). To adjust the position of the menu items, use the **Move Up** and **Move Down** buttons.

Field Name	Description
Display Name	This is the displayed name of the menu item which will appear on the device.
Program Path	This is the path for the web address, or Package ID (Bundle Identifier) on the device. For instance, the Package ID (Bundle Identifier) for Google Maps is `com.android.apps.maps`. The Package will automatically be prefixed with the Launch:// URI. If you are attempting to navigate to a web page, simply enter the URL, http://www.Company.com. The list of available URI's for lockdown are as follows: Movie:// - Allows videos to be played on the lockdown. Dial:// - This will open the dialer, with a specified number. (e.g. dial://5555555555) Launch:// - Launch applications based on package ID. File:// - Opens a file on the device (e.g. file:///%sdcard%content/document.pdf) http:// - Opens a webpage from within the lockdown. https:// - Opens a secured webpage from within the lockdown. ftp:// - Opens FTP from within the lockdown. browser:// - Opens a url in browser using the HTTP protocol browsers:// - Opens a url in browser using HTTPS protocol Intent:// - Opens an Android intent (e.g. to open Google Navigation - google.navigation:///?q="2%20Greenway%20Plaza%20Houston%20TX%2077046") action:// - Executes a MobiControl action (e.g. to change device password, action://CHANGE_DEVICE_PASSWORD. To configure WiFi, action://CONFIGURE_WIFI)
Image (optional)	This is the name of the image file that you want to display in the lockdown menu with this menu entry. By selecting the image in this dialog box, it will be automatically delivered to the device along with the lockdown configuration. Select an image from the drop-down list, or click the image to select an image from your desktop computer. In order to display this image in the lockdown menu, it is necessary for the HTML template to have a special `<MCDispImgN>` tag. Please see the "Customizing Android Lockdown Menu Templates" topic on page 1158 for instructions on how to make this image appear in the Lockdown menu. **NOTE:** If you wish to replace an image that had been previously imported, upload the new graphic file, maintaining the same file name as the old one. You will be asked to confirm the overwrite of the old file. Click **Yes,** and the new image will be in effect.
Use Application Icon	Use the application icon in the lockdown. In order to display this image in the lockdown menu, it is necessary for the HTML template to have a special `<MCEXEIconN>` tag. Please see the "Customizing Android Lockdown Menu Templates" topic on page 1158 for instructions on how to make this image appear in the Lockdown menu.
Launch	When this option is checked, the selected program will be automatically executed on

Field Name	Description
automatically on startup	startup (i.e. after a soft reset, or restart of the lockdown process).

Templates

The lockdown program menu is displayed as an HTML web page to the user. The Template drop-down box allows you to select an HTML template from a list of built in templates and your own customized templates.

You can easily create a customized lockdown template by copying an existing template and directly modifying HTML code in the built-in Lockdown Menu Template Editor available in MobiControl. (Please see the "Customizing Android Lockdown Menu Templates" topic on page 1158.) You can also use your favorite HTML editor. When editing the HTML file, be sure to preserve the special MobiControl Menu tags. These special tags are automatically replaced with the appropriate Program Menu entries by MobiControl.

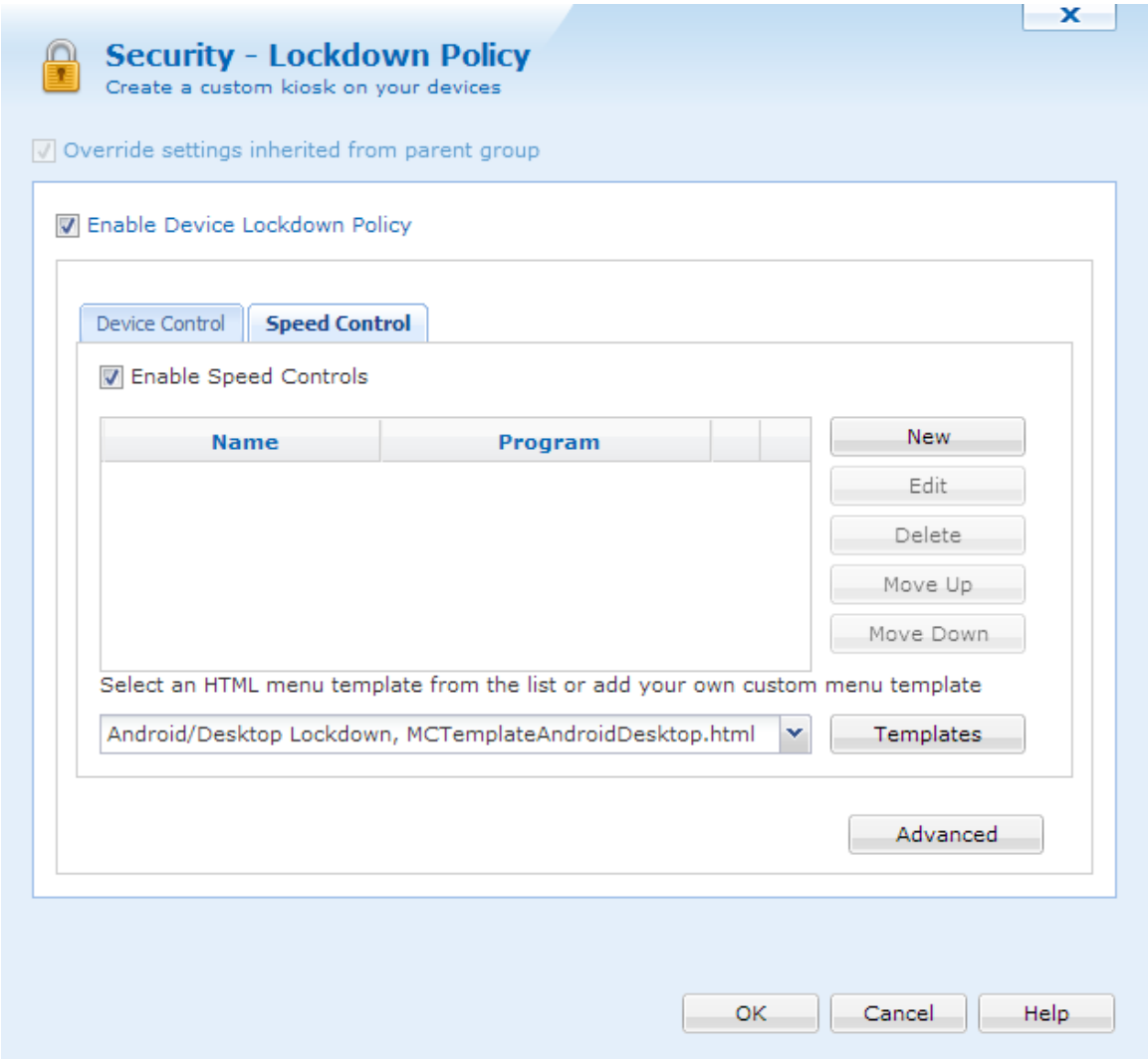
Once you have selected the desired template and clicked the **OK** button, MobiControl will merge the menu items that you have configured with the selected template and generate a custom HTML menu page.

For further assistance, please contact us.

Device lockdown page

Android Speed Lockdown

Device lockdown replaces the standard device home screen and Windows **Start** button with a customizable home screen. Users have access only to authorized applications and websites, and are prevented from accessing all other applications and device controls while on the road. This promotes greater safety by disabling distracting features on a mobile device while workers are on the road.

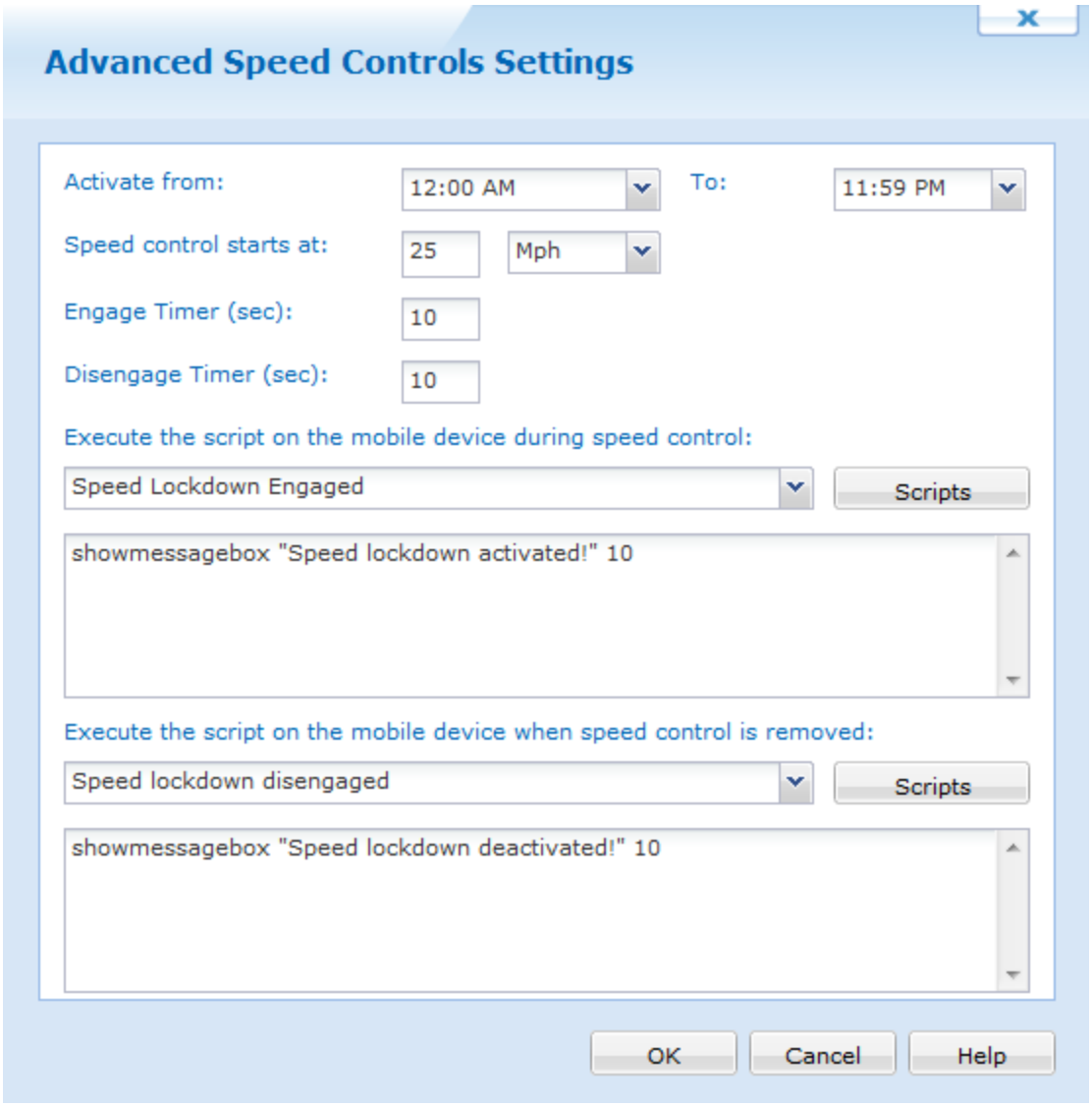


Lockdown Policy dialog box

For information on how to set up menu items and configuring lockdown templates, please click here.

Speed Lockdown triggers when the device is going a certain speed, as set in the Advanced settings. The speed of the device is determined by utilizing the device's GPS unit. Using the device's GPS unit, MobiControl periodically checks the location of the device along with the time. It will then check again and determine the distance between the two points and calculate the device's speed.

Since there are times where there could be traffic, or stop lights, having the speed lockdown disengage and re-engage constantly will cause distraction to a driver. Because of this, the speed lockdown has engage and disengage functionalities. These and other settings can be configured by clicking Advanced.



Advanced Speed Control Settings

Below are brief descriptions of each feature in the Advanced Speed Control settings.

Field	Description
Activate From, to	Here we can set when the speed control should activate. We can set it for the whole day or even 15 minutes.
Speed Control starts at	This is where we decide what speed the device should be travelling before the engage timer starts counting. We can change the speed measurement to either Mph or Km/h.
Engage Timer	The amount of time the device should stay on or above the speed control

Field	Description
	before the lockdown activates.
Disengage Timer	The amount of time the device stays below the specified speed control before disengaging.
Execute script on the mobile device during speed control	When the speed control lockdown is activated, send this script to the device.
Execute script on the mobile when speed control is removed	When the speed control lockdown is deactivated, send this script to the device.

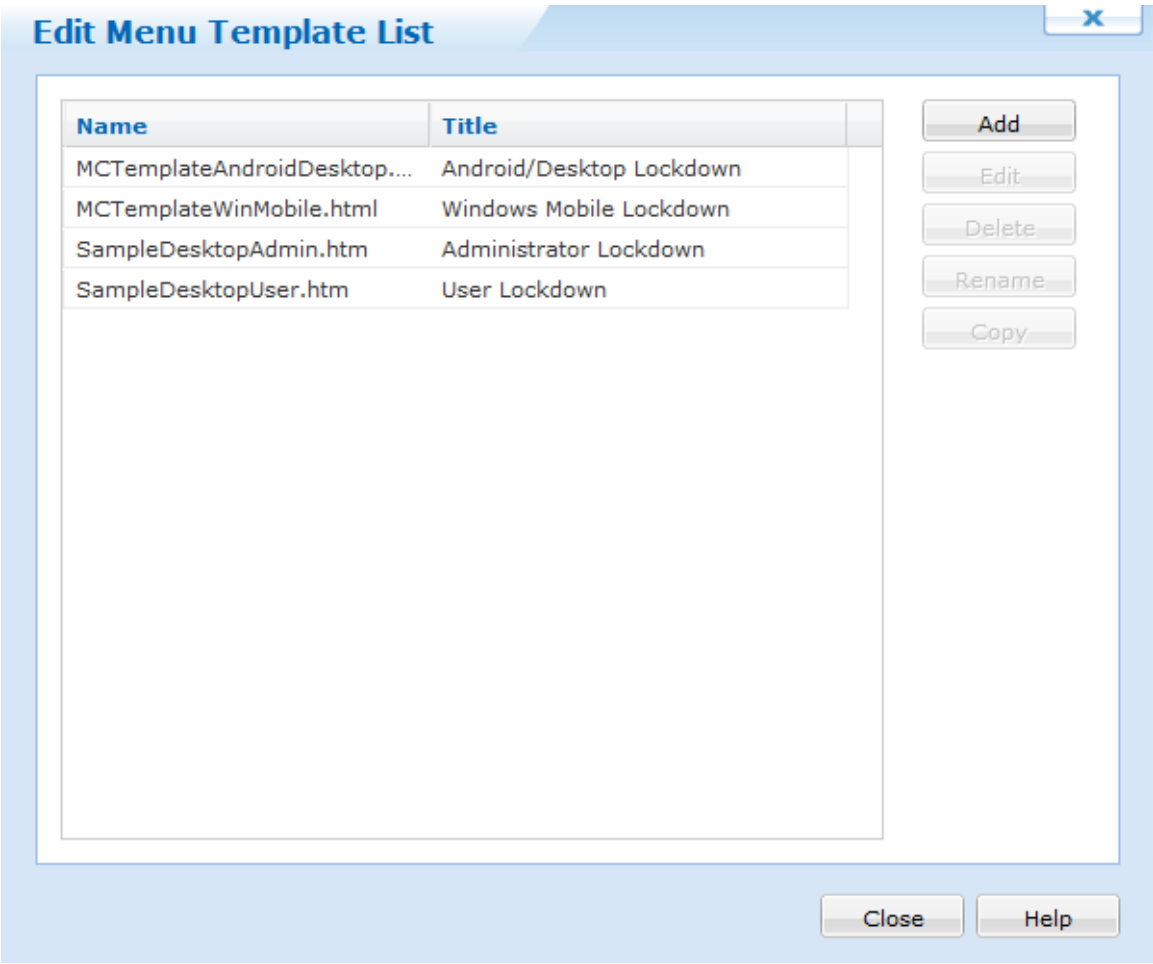
Using the above screen shot, the speed lockdown is activated the whole day, should engage when the device is travelling at 25 Mph or higher for at least 10 seconds. If it falls below the specified speed, wait 10 seconds before disengaging the speed control. When the speed control is activated, send a message box to the device, and when the speed control is removed, send another script.

Android Customizing Lockdown Menu Templates

MobiControl allows you to modify pre-configured HTML menu templates or to build your own HTML menu templates. A menu template is an HTML file with special menu tags that get replaced by MobiControl when it generates the menu. Essentially, the menu tags get replaced by the menu item links that you configure for your program menu. The table below describes the special menu tags that get replaced in the HTML file.

The easiest way to create a custom program menu template is to make a copy of one of the default templates, customize it, and then add it to the list of available templates:

1. Select **Edit** in the **Lockdown Configuration** dialog box.
2. Create a copy of one of the default templates listed in the **Templates** dialog box. (Copy and paste it into another folder, e.g. My Documents.)
3. Edit the copied file according to the guidelines below and name the file appropriately.
4. Add the new template by selecting the **Add** button in the **Templates** dialog box.



Edit Menu Template List dialog box

The following table describes menu tags:

<table>
<tr><th>Tag Name</th><th>Description</th></tr>
<tr><td><MCMenuFull></td><td>This tag gets replaced with the full menu list that the user has configured. The menu items are separated by carriage returns.
Sample Menu Entries:
MobiControl Device Agent(launch://net.soti.mobicontrol)
My Website (http://www.mywebsite.com)
<table>
<tr><th>Template</th><th>Resultant Menu</th></tr>
<tr><td><html>
<body>
<MCMenuFull>
</body>
</html></td><td><html>
<body>
MobiControl Device Agent

My Website

</body>
</html></td></tr>
</table></td></tr>
<tr><td><MCMenuN>
where "N" is the menu item number</td><td>This tag allows you to place each complete menu item where you want it in the HTML.
Sample Menu Entries:
MobiControl Device Agent(launch://net.soti.mobicontrol)
My Website (http://www.mywebsite.com)
<table>
<tr><th>Template</th><th>Resultant Menu</th></tr>
<tr><td><html>
<body>
1. <MCMenu0>

2. <MCMenu1>

<body>
</html></td><td><html>
<body>
1. MobiControl Device Agent

2. My Website

<body>
</html></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Tag Name</th><th>Description</th></tr>
<tr><td><MCLinkN> and <MCDispN>
where "N" is the menu item number</td><td>These tags let you further separate the menu item to be inserted into the "link" and the "display" text and control where in the HTML template they will be inserted.
Sample Menu Entries:
Android Calendar (launch://com.android.calendar)
Browse mywesbite (browse://www.mywebsite.com)
Report.pdf (file://mnt/sdcard/report.pdf)
<table>
<tr><th>Template</th><th>Resultant Menu</th></tr>
<tr><td><html>
<body>
1. <a href="<MCLink0>">
 <MCDisp0>

2. <a href="<MCLink1>">
 <MCDisp1>

3. <a href="<MCLink2>">
 <MCDisp2>

</body>
</html></td><td><html>
<body>
1. <a href=
"
launch://com.android.calendar
"> Calendar

2. <a href=
"browse://www.mywebsite.com">
Browse
mywebsite

3. <a href=
"
file://mnt/sdcard/report.pdf
"> Report.pdf

</body>
</html></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Tag Name</th><th>Description</th></tr>
<tr><td><MCExeIcon N>
where "N" is the menu item number</td><td>This tag lets you display the built-in icon for an application executable that is in the program menu.
Sample Menu Entries:
Android Calendar (launch://com.android.calendar)
Browse mywesbite (browse://www.mywebsite.com)
Report.pdf (file://mnt/sdcard/report.pdf)
<table>
<tr><th>Template</th><th>Resultant Menu</th></tr>
<tr><td><pre>
<html>
 <body>
1. <a
href="<MCLink0>">
<img src="
<MCExeIcon0>">

2. <a
href="<MCLink1>">
<img src="
<MCExeIcon1>">

3. <a
href="<MCLink2>">
<img src="
<MCExeIcon2>">

 </body>
</html>
</pre></td><td><pre>
<html>
 <body>
1. <a href=
"launch://com.android.calendar">
<img src= "
SDCard\Lockdownimage\MCLD_
Calendar.bmp">
2. <a href=
"browse://www.mywebsite.com> <img
src= "
SDCard\Lockdownimage\MCLDBrowse.bmp
">
3. <a href=
"file://mnt/sdcard/report.pdf">
<img src= "
SDCard\Lockdownimage\MCLD_
report.bmp">
 </body>
</html>
</pre></td></tr>
</table></td></tr>
<tr><td><MCDispImg N>
where "N" is the menu item number</td><td>This tag lets you associate a picture with an entry in the lockdown screen.
Sample Menu Entries:
MobiControl Device Agent (launch://net.soti.mobicontrol)
My Website (http://www.mywebsite.com)
<table>
<tr><th>Template</th><th>Resultant Menu</th></tr>
<tr><td><pre>
<html>
 <body>
1. <a href=
"<MCLink0>"> <img
src
="<MCDispImg0>">

2. <a href=
"<MCLink1>"> <img
src=
"
<MCDispImg1>">

</body>
</html>
</pre></td><td><pre>
<html>
 <body>
1. <a href=
"launch://net.soti.mobicontrol">
<img src =
"\SDCard\Lockdownimage\Logo.png">

 2. <a href=
"http://www.MyWebsite.com"> <img
src=
"SDCard\Lockdownimage\website.jpg">

</body>
</html>
</pre></td></tr>
</table></td></tr>
</table>

Including Pictures in Menu Templates

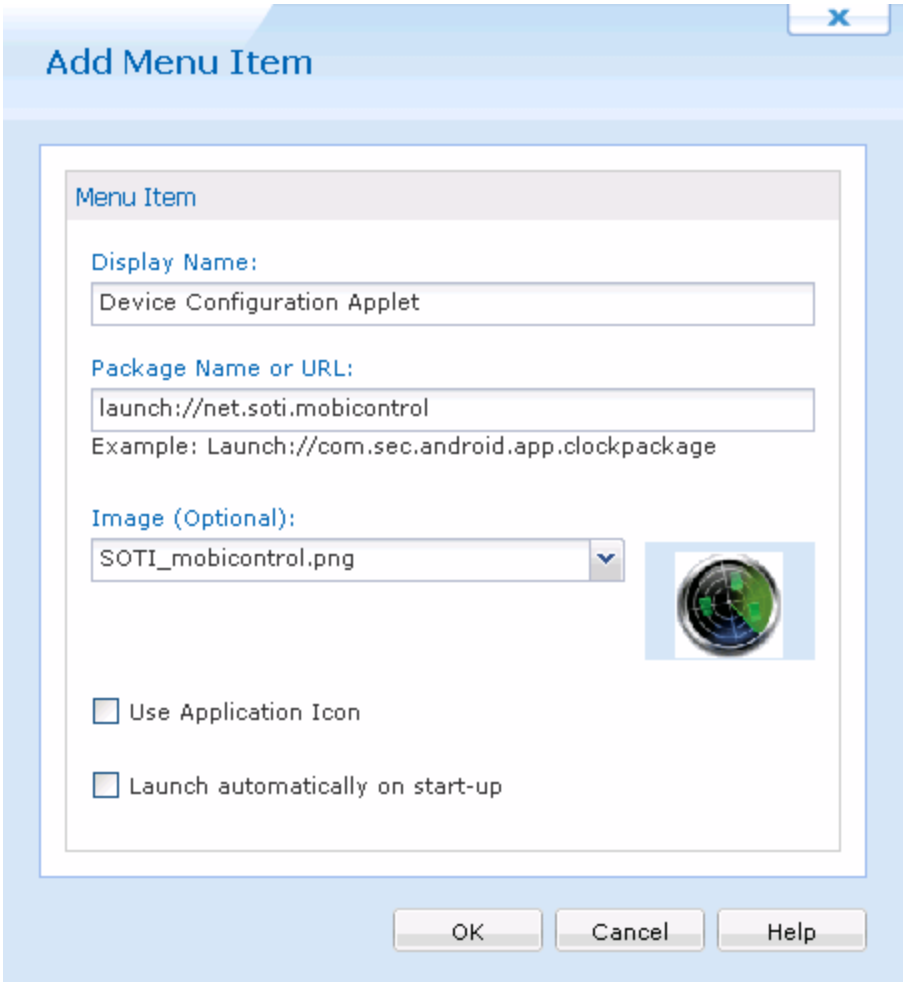
You can insert images into your template by simply using the Insert Image feature in the built-in HTML Template Editor. MobiControl will deliver the image to the device. Alternatively, if you do not want to use MobiControl to deliver the image, you can simply specify in the HTML template the full path to the graphic for where it will be found on the mobile device (e.g. `<img src="file:///SDCard/images/CompanyLogo.jpg">`).

URI's

Uniform Resource Identifier (URI) is a string of characters used to identify a name or a resource on the Android Device. Such identification enables interaction with representations of the resource using specific protocols. Schemes specifying a concrete syntax and associated protocols define each URI. The MobiControl Lockdown on Android devices allows you to use custom URI's. Such URI's include Launch://, Http://, Https://, File:// and Browser://.

Linking to the MobiControl Device Configuration Applet

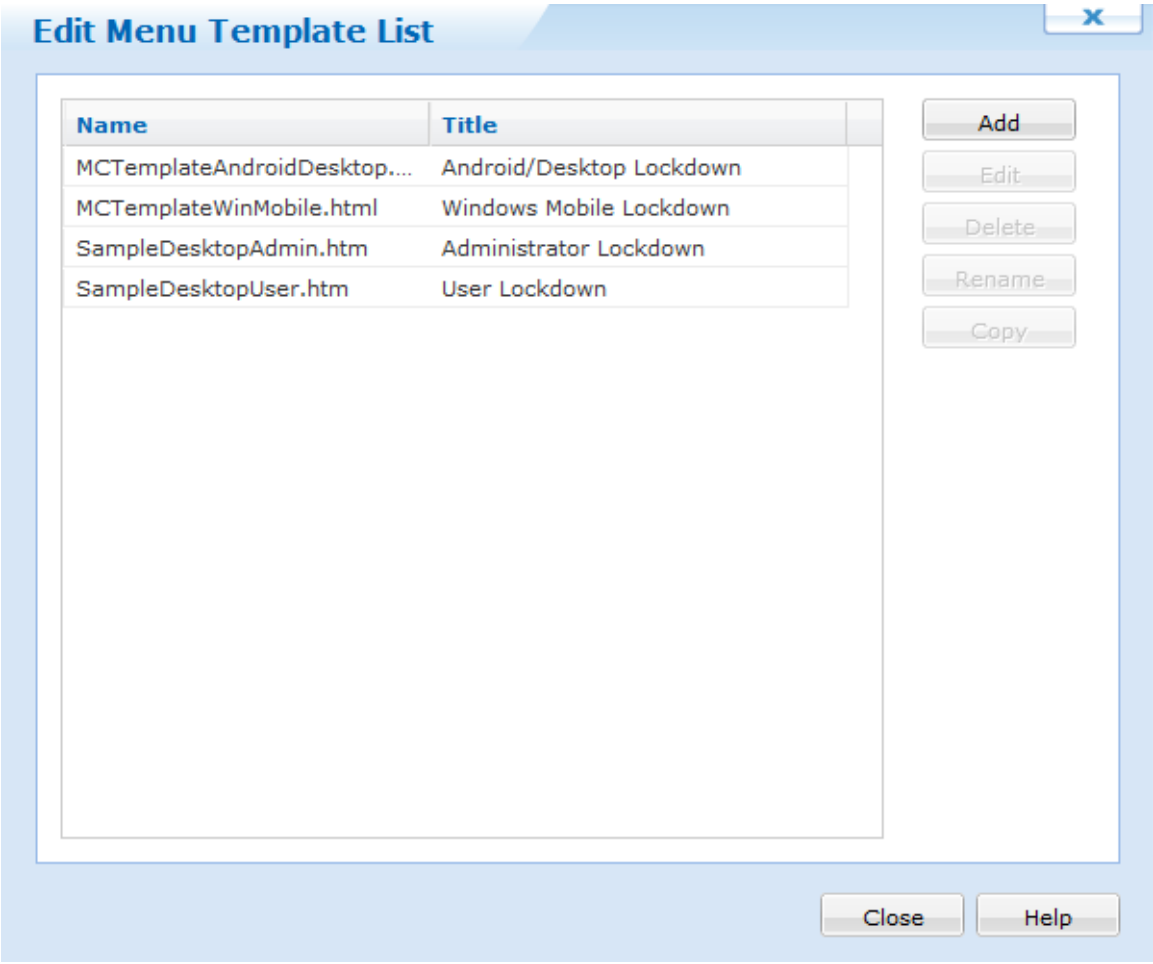
The MobiControl device applet that is normally accessed by tapping on the MobiControl icon on the Today screen or system tray of the device contains a bounty of useful status information. This information can be very useful when trying to troubleshoot a problem in the field, for example resolving connectivity issues between the device and the MobiControl Deployment Server.



Program menu entry for MobiControl Configuration Applet

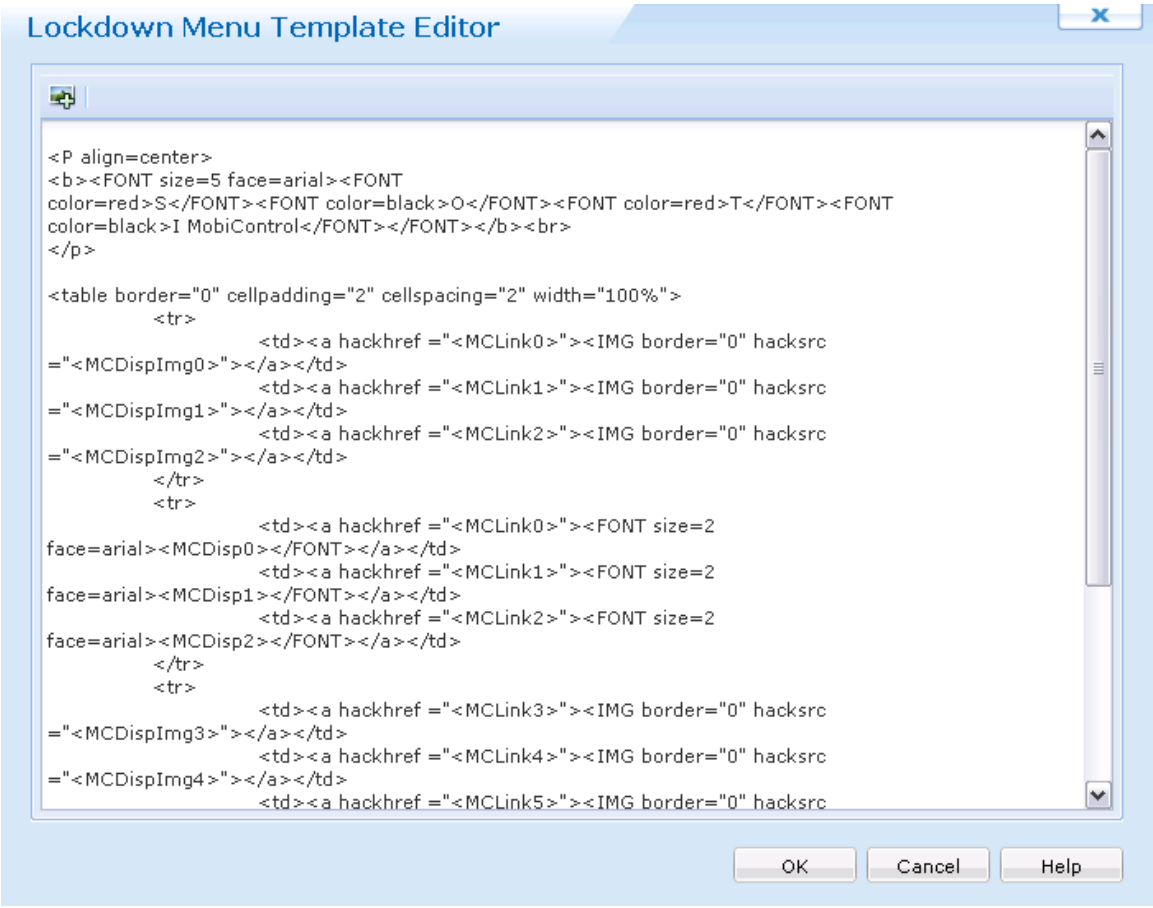
Edit Menu Template List

In the **Edit Template Menu List** dialog box, click **Add** and navigate to the location of your customized lockdown page and select it. You will see the customized menu template in this list now. You can chose to edit this template further by clicking on **Edit** and launching the lockdown menu template editor, or click on **Close** and then select the template from the **Lockdown Menu**.



Edit Menu Template List dialog box

You can edit the lockdown menu templates using the built-in HTML editor. After saving a modified template, be sure to select the template file in the combo selection box on the main **Lockdown Configuration** page. Basic HTML, Java, and Flash are supported in the lockdown.



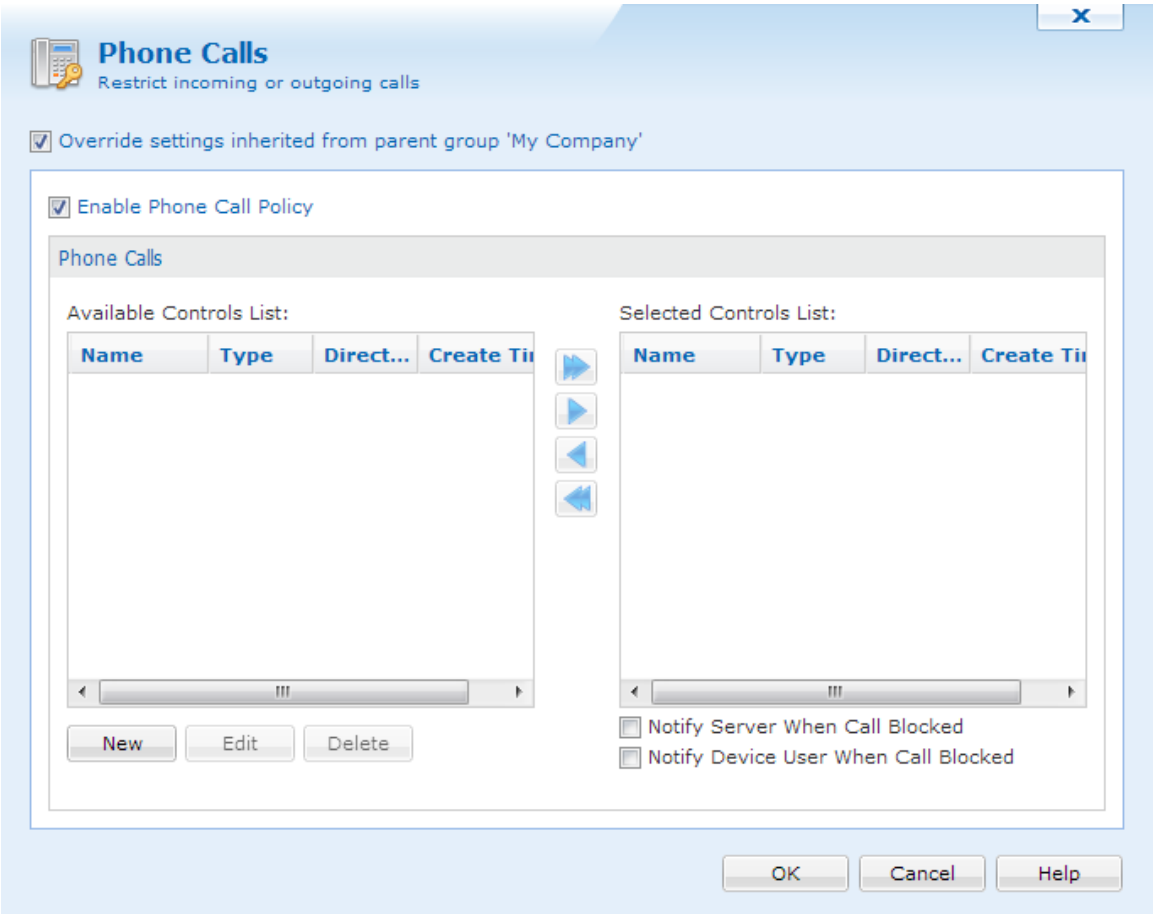
Lockdown menu HTML editor

TIP:

You can easily include a graphic in your HTML template by selecting the **Insert Image** menu option in the HTML Editor.

Android Phone Call Policy

MobiControl provides various on-device feature controls including the capability to block various device communications, including what numbers a device is able to call or receive calls from.



Phone Call Policy dialog box

Phone Call Policy Control Lists

MobiControl allows you to specify the numbers to which users may place calls to and receive calls from:

1. The **Available Control Lists** displays all control lists that have been defined, but currently are not in use. Administrators are able to create several different phone call policies without having them be activated on the devices.
2. The **Selected Control Lists** displays all currently activated control lists. Only the control lists included in the selected control lists are allowed to execute on the device. This provides an added layer of security for organizations concerned about unknown phone calls that may be placed from or received by the device. This can potentially happen without the end user being aware of it, as is frequently the case with viruses, spyware and other malicious applications.

NOTE:

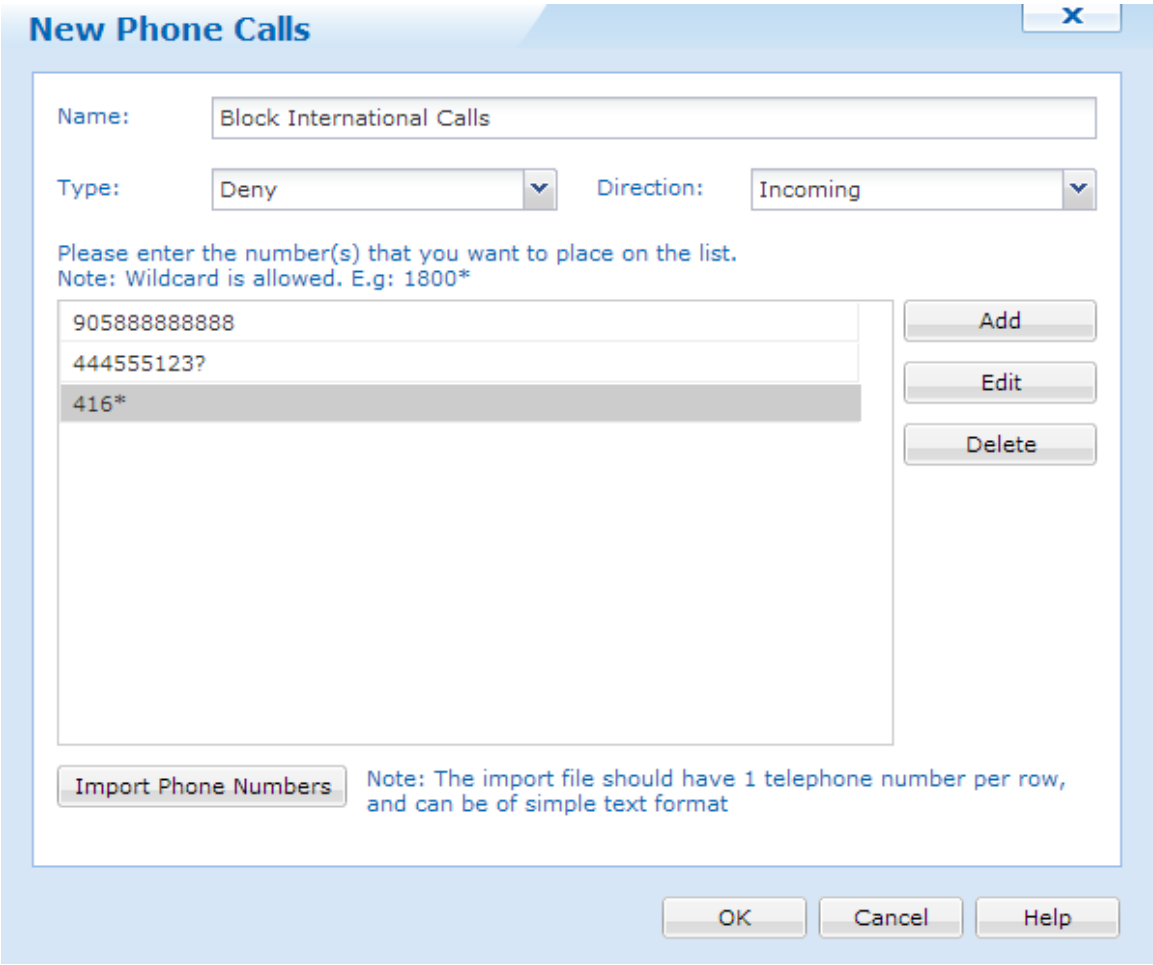
There cannot be both deny and allow control lists activated at the same time. All control lists for a particular direction must be the same type.

IMPORTANT:

If the allowed list is not set up correctly, you may end up blocking or not allowing a potential system critical phone call. Emergency numbers will always be allowed even if they are not part of a whitelist.

3. When the **Notify Server on Call Blocked** check box is checked, the server's log file will output all calls that were blocked, along with the phone number that was trying to call in or out for the particular device.
4. When the **Notify User on Call Blocked** check box is checked, and the user receives an incoming call from a phone number that was blocked, a message box will be displayed

To enable phone call policy control for a device or group of devices, select **Phone Call Policy** from the MobiControl Security Center. (Please see the "Android Device Configuration" topic on page 1137.)



New Phone Call Policy entry dialog box

Field Name	Description
New	Clicking on this button allows you to create a new phone call policy with the dialog box as shown above. Assign a meaningful name to help distinguish between the various phone call policies you may setup.
Type	The available options allowed are either Allow or Deny. The type Allow indicates the phone calls that can either be placed from the phone or received by the phone or both based on Direction set for this policy. The type Deny indicates the phone calls that can not either be placed from the phone or received by the phone or both based on Direction set for this policy. If attempting to block restricted or unknown callers simply add **<unknown>** and/or **<restricted>** to the deny list.
Direction	The available options are Incoming, Outgoing, or Both. Incoming indicates that this policy is for calls received by the device. Outgoing indicates that this policy is for calls placed by the device. Both indicates that the policy is for both incoming and outgoing calls. For example, you may want to allow all communication to and from your device to your IT Support team and hence you would select both in this case with the appropriate phone numbers that can be dialled to work with your support team.

Once you have configured the Name, Type and Direction, click on **Add...** in order to enter in the phone number(s) that the policy monitors.

MobiControl will compare the number either received or placed with the list of numbers mentioned in the policy and compare the exact phone number displayed with the list of numbers you provide. If you have a series of numbers that you would like to enter in, there are a few options available, which can be used in combination with each other:

1. Leverage the wild card character, which is the asterisk, or '*'. The asterisk indicates any number of digits. For example, you may want to only allow calls coming from a particular area code. In this case, you can enter in '<area code>*' as the number.

   EXAMPLE:

   416* would match all calls that start with 416.

2. Leverage the single wild card character, which is the question mark, or '?'. The question mark indicates any single digit.

   EXAMPLE:

   You may want to allow communication to a list of phone numbers that only vary by a single digit. In this case, you can enter in as an example, 444555123?. This indicates the policy applies to the following list of numbers:
   444-555-1230
   444-555-1231
   444-555-1232
   444-555-1233
   444-555-1234
   444-555-1235
   444-555-1236
   444-555-1237
   444-555-1238
   444-555-1239
   Combinations of the two wild card characters can also be used if required. For example, 4??-555-12* would succeed if the phone number is 432-555-1234, but not if the phone number is 432-432-1234

When the **Import CSV** button is selected, a dialog box will appear to import the list of phone numbers using a CSV file. MobiControl assumes that the input file format is **one phone number per line**. To view a sample CSV file, click here.

EXAMPLE:

9058888888
519222*
416*
Upon reading in the file, the individual numbers will be added to the list control, just as though they were individually typed in using the Add button.

IMPORTANT:

The file being imported must not contain more than 2000 lines.

Android Web Filter

The Android Web Filter allows us to block certain types of websites. MobiControl uses a highly sophisticated filter to determine which web pages are safe and which are not. If a user stumbles across a web site that is blocked by the filter, they are then redirected to a predetermined safe site.

To enable the Android Web Filter, right click a group or a single Android device, click **Device Configuration**. After the Device Configuration dialog appears, click **Web Filter**.

IMPORTANT:

Webroot's SecureWeb Browser must be installed on the device for the web filter to function. It is recommended to include the SecureWeb Browser in an Application Catalog so that it can be installed on the device. Click here to access the WebRoot SecureWeb Browser on Google Play. Please see the "Android+ Application Catalog" topic on page 1403 for more information on the Application Catalog.

Android Web Filter dialog box

When the Web Filter is enabled, MobiControl will push down a secured browser to the configured devices. This browser has the advanced web filter technology that allows us to block categorized websites.

The Web Filter has an option to redirect users to a trusted website if they do come across a filtered website.

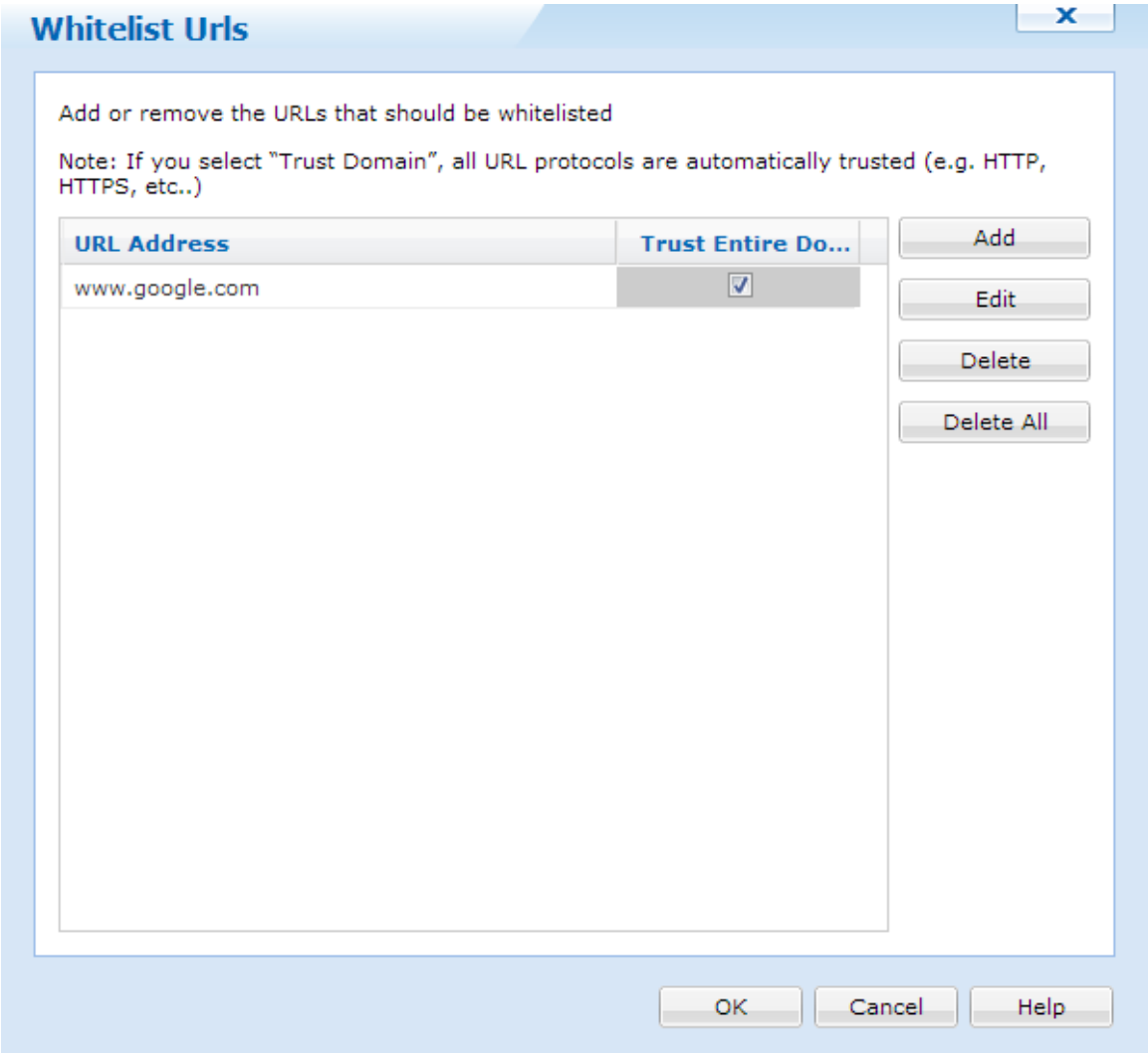
Below, we will go over each of the categories that included with this filter (Click each title to see sub categories):

- **Adult**
- **Business and Economy**
- **Education**
- **Entertainment**
- **Government/Politics**
- **Hacking and Proxy Avoidance**
- **Health**
- **Life Style**
- **Other**
- **Spam**
- **Technology**

Website Whitelist

If certain websites are blocked by the filter, we can enable a Website Whitelist to ensure that these sites do not get blocked. To do this, click the 

button.



Website Whitelist

Clicking Add allows us to enter a URL address. These addresses are the websites that will not be blocked by the filter.

Checking off **Trust Entire Domain** will ensure that all protocols, and sub domains are trusted.

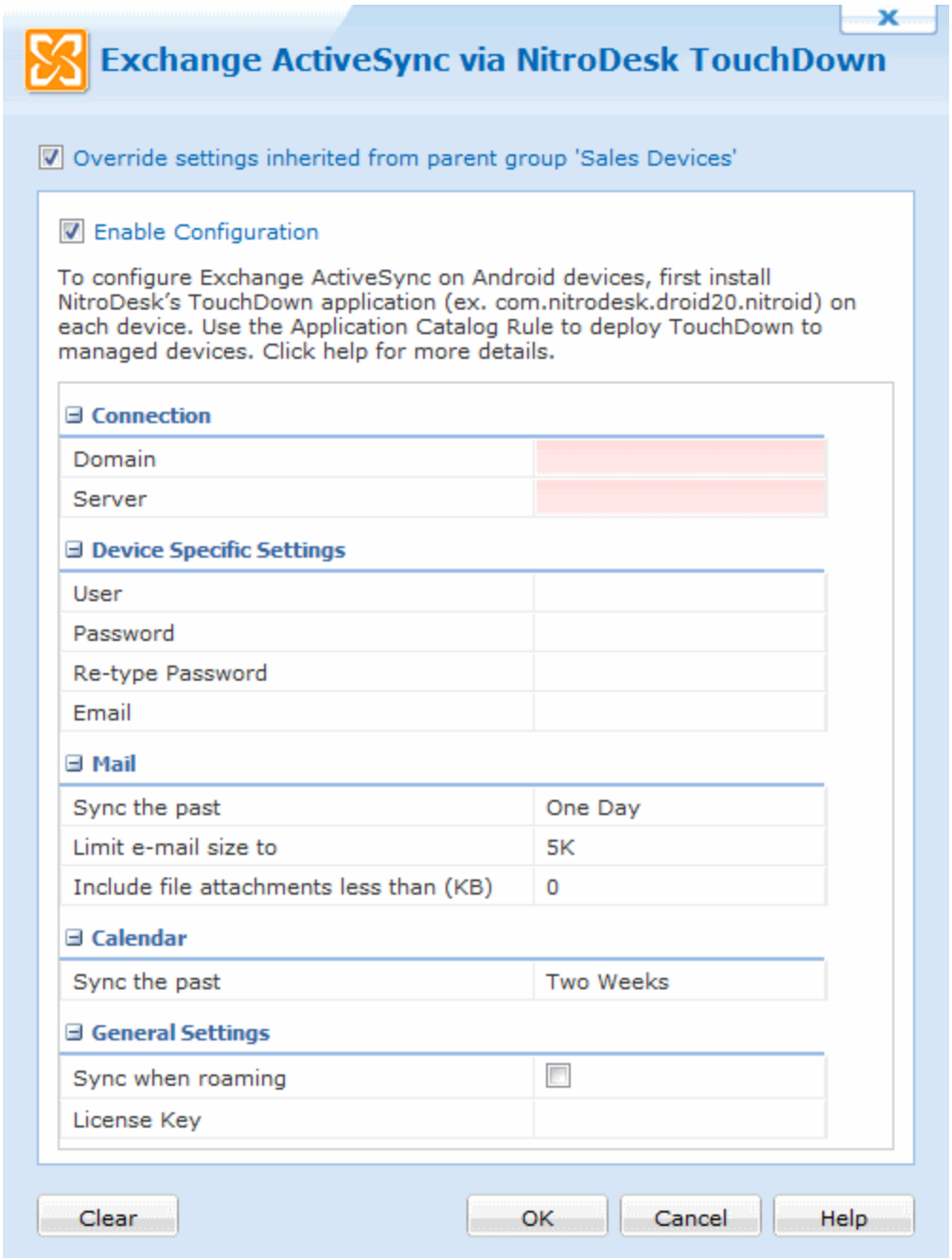
If a URL is not needed anymore, click Delete.

After all configurations are set, click OK to save everything and close.

Android Email Configuration via NitroDesk TouchDown

With MobiControl, you can now configure Microsoft Exchange ActiveSync settings for NitroDesk's TouchDown application for your Android mobile device. NitroDesk TouchDown can be installed from Google Play. MobiControl supports v7.011 and above. To arrive at this configuration menu, select the

device or the group, right-click, select **Configure Device(s)**, and click **Exchange ActiveSync**. In order to be able to setup Exchange ActiveSync via NitroDesk TouchDown, the application must first be installed from Google Play, or an Application Catalog.



Exchange ActiveSync via NitroDesk TouchDown

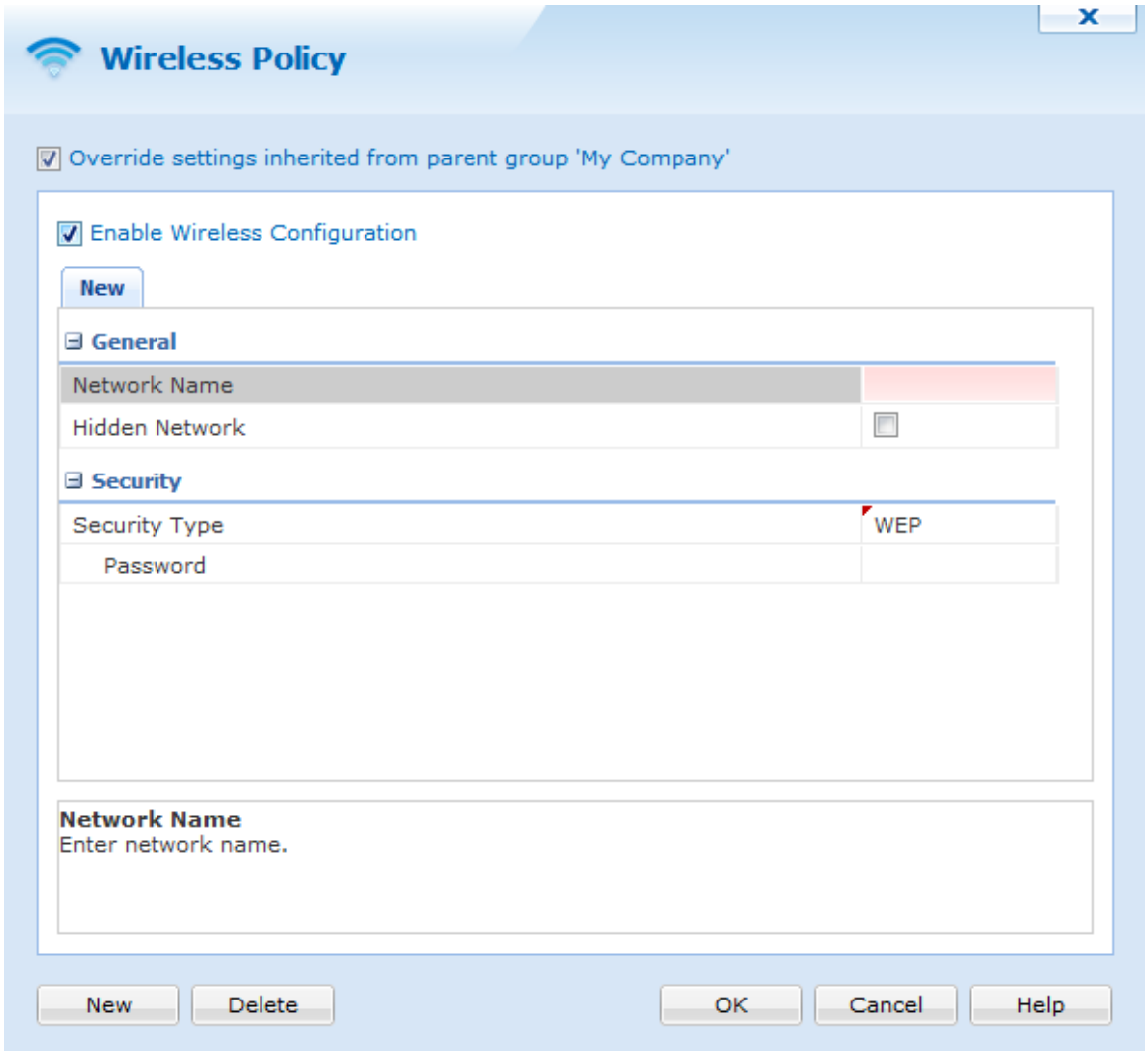
Field Name	Description
Domain	Enter the domain name of your organization.

Field Name	Description
Server Address	Enter the server address of your organization
User	Enter the username for the email address being configured
Password	Enter and Re-Enter the password for the email address being configured
Email	Enter the Email address of the address being configured
Sync the past	Select how far back TouchDown will pull your Exchange Emails and Calendar appointments
Limit Email size	Limits the amount of data used when retrieving emails
Include file attachments less then	Limit retrieval size of attachments.
Sync when roaming	Allow or disallow TouchDown's ability to retrieve emails when roaming
License Key	Enter your NitroDesk TouchDown license key

Android Wireless Policy

With MobiControl's Wireless policy, we are able to configure the WiFi connection on Android devices. This offers a way to safely and quickly configure the wireless connection on one or hundreds of devices.

To enable the Wireless Policy for a device or group of devices, select **Wireless Policy** from the MobiControl Security Center. (Please see the "Android Device Configuration" topic on page 1137.)



Device Feature Control Policy dialog box

If more than one network is needed to be configured, selecting New will create an additional profile.

Field Name	Description
Network Name	The name of the network which the device should connect to. Also is the name of the Wireless Policy.
Hidden Network	Select whether the network is hidden or not.
Security Type	The security protocol currently being used on the network. We can select WEP, WPA, WPA2 or None.
Password	The password to connect to the network.

If a wireless configuration is not needed anymore, just select Delete. After all configurations are done, click OK.

Android Advanced Settings

There are five main aspects to Android Advanced Settings. Each of these settings can be configured for a single device or applied at the device group level thereby configuring a set of devices. When the devices are moved from one device group to another in the device tree, the settings for the new device group are applied automatically to the devices.

Custom Attributes

Custom Attributes allows us to create custom information that appears on the information panel on the right hand side of the web console. Please see the "Custom Attributes" topic on page 1343 for more information.

Connection Settings

This option allows you to configure connection settings for your mobile device(s), via. configure connection security by enabling or disabling SSL, select connection mode between persistent, scheduled and manual, change connection retry interval and set log file management, among other options. Please see the "Android Connection Settings" topic on page 1181.

Deployment Server Priority

This option allows you to specify the Deployment Server preferences for the devices. When a device is configured with more than one Deployment Server, it will try to connect to highest priority one first and if this server is not accessible, then it will try to connect to the next server available. Please see the "Android Deployment Server Priority" topic on page 1184.

Support Contacts Info

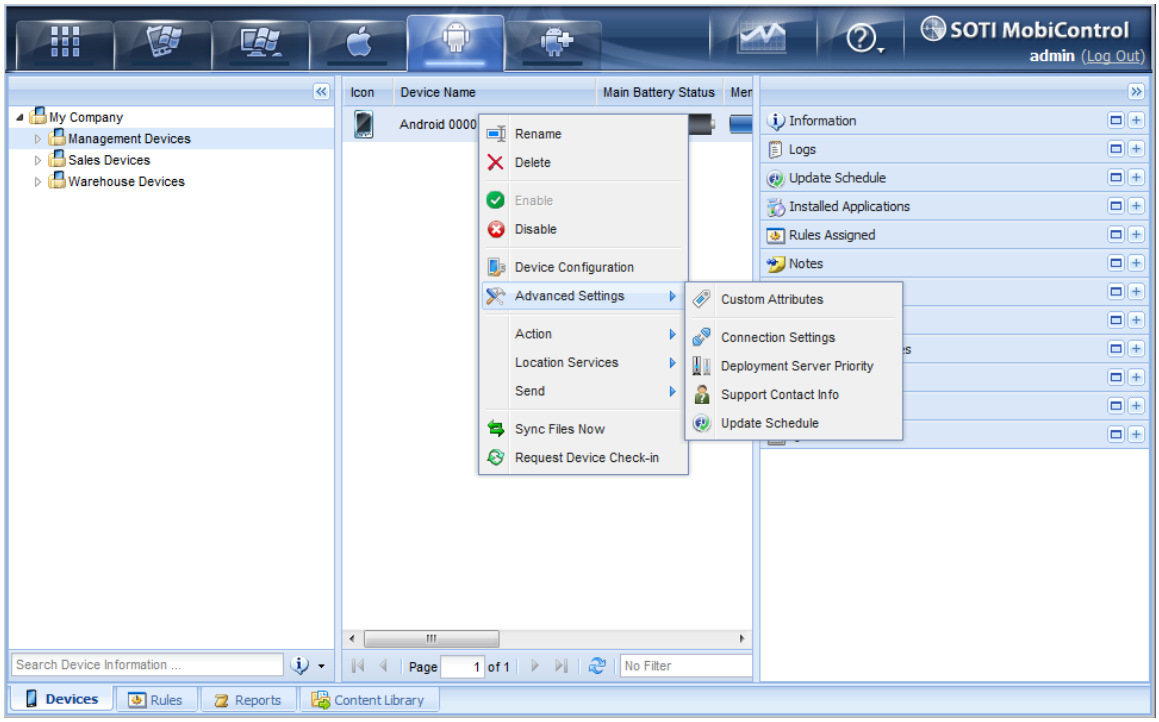
If users call support for their mobile device needs, configuring this option allows them to find the contact information reliably. Since this information is set centrally all information is updated once it's changed. Please see the "Android Support Contacts Info" topic on page 1185 for more information.

Device Time Synchronization

This option allows you to enable time synchronization for a mobile device, allowing the device to update its date and time settings by periodically synchronizing them with an SNTP/NTP time server or the MobiControl Deployment Server. Please see the "Android+ Time Synchronization" topic on page 1357 for more information.

Device Update Schedule

Adjust the interval at which the mobile devices contact the Deployment Server for new updates, configuration changes and packages. Please see the "Android Device Update Schedule" topic on page 1186.



Device Configuration Menu options

Custom Attributes

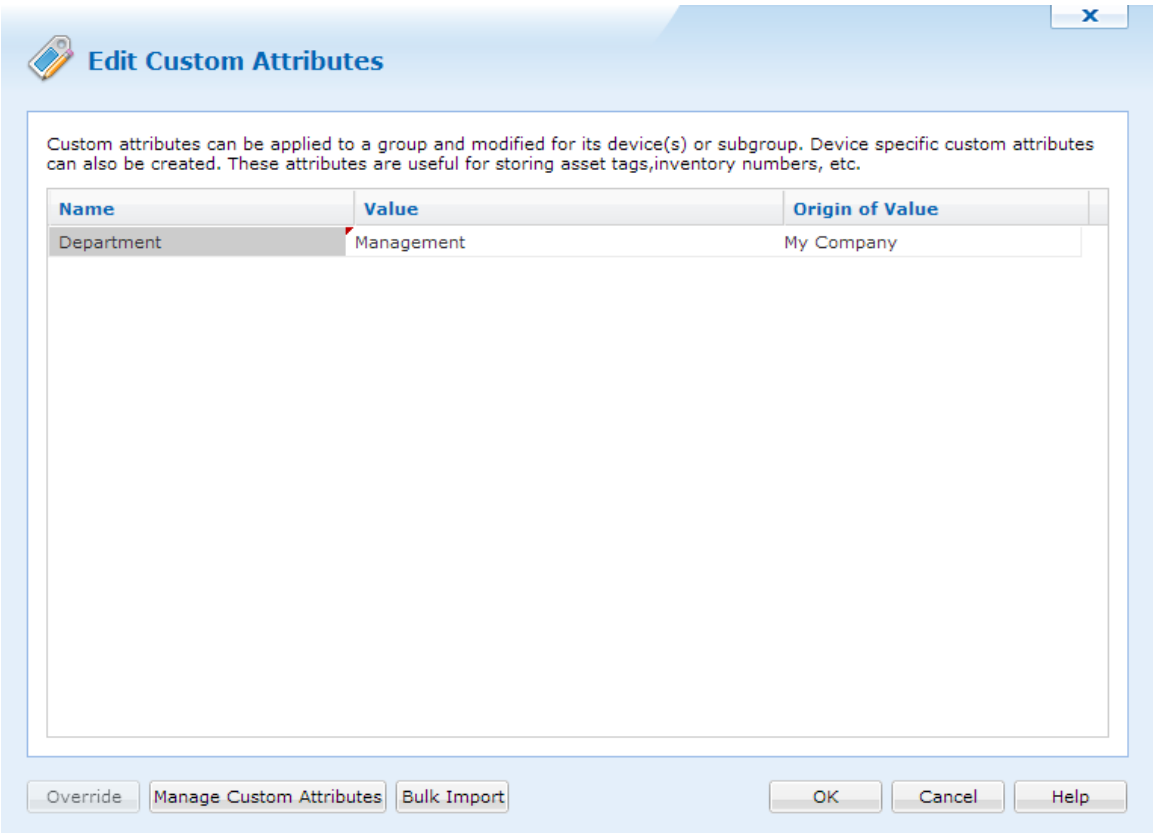
Custom Attributes allows us to create attributes to show in the information panel with our own data. This offers custom organization and labelling. For example, we can create a department attribute and put a different department for each device or device group.

Custom Attributes can also be propagated to devices so that they can be used in other applications and information.

NOTE:

Custom Attributes are available for all device types.

To set up Custom Attributes, right click a device or device group, go to Advance and click **Custom Attributes**.



Custom Attributes panel

The Custom Attributes panel has 3 columns: name, value and origin of value.

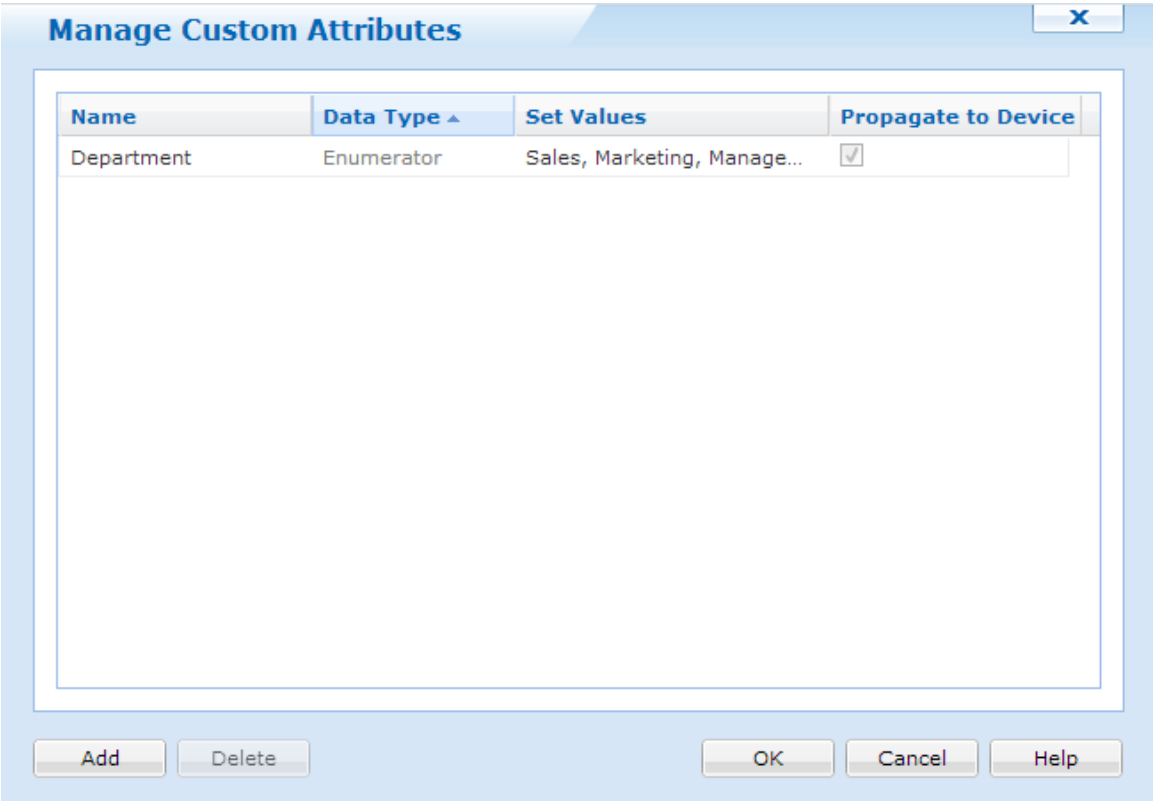
The name column shows the name of the Custom Attribute that will be shown in the info panel. Value contains the actual attribute for this field. Origin of value shows us where this field came from. For example, if Custom Attributes were set at the root level of the device tree, the origin of value will show the root level device group.

Clicking **Override** will change the origin of value to that where the device resides. This is useful if attributes change for each device. The Override button will change to **Remote Override** if we want to inherit the value from a parent group.

To create new attributes, click **Manage Custom Attributes**.

Manage Custom Attributes

When Manage Custom Attributes is clicked we a new dialog box appears. Here we will be able to create the Custom Attributes.



Manage Custom Attributes

Click Add to add a new attribute.

When Add is clicked, a new row will appear. Clicking the field under name will allow us to name this attribute.

Data Types

There are 5 available data types to have for Custom Attributes:

- Text
- Numeric
- Date
- Boolean
- Enumerator

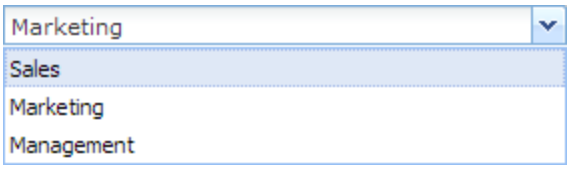
Text will allow us to create values with **letters and numbers**.

Numeric will allow us to create values with **only numbers**.

Date will allow us to set dates.

Boolean will create a checkbox for **yes or no / true or false**.

If we select enumerator, this allows us to create a drop down list when we set the attribute. To create the list, click the field in **Set Values** column. Here we can type the items we want in the drop down list. **Each value must be separated with a comma (,)**. For example, if we want to create a department attribute, we can have Sales, Marketing, Management. When we set this attribute, we will be presented with the drop down.



Enumerator Example

Propagate to Device

Checking this off will have MobiControl create the Custom Attributes in the pdb.ini file on the device. Applications can then read this file and pull the Custom Attribute value.

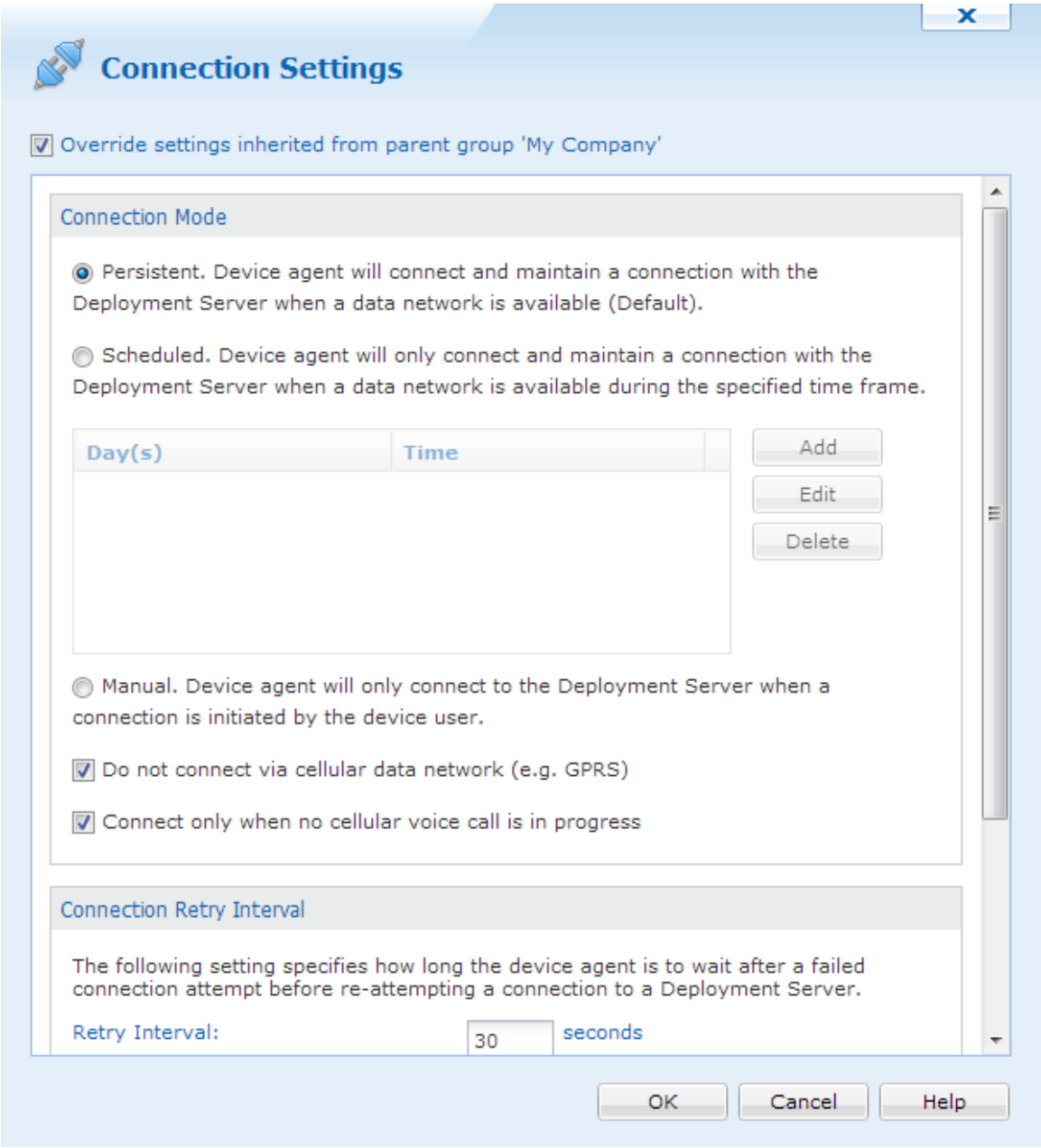
Bulk Import

If there is a large amount of Custom Attributes to be inserted, we can do a bulk import so that everything is added at once.

Once everything is set, click OK to save and close the Custom Attributes.

Android Connection Settings

To access the **Connection Settings** dialog box, right-click on a device or device group, point to **Advanced Settings,** and select **Connection Settings.**



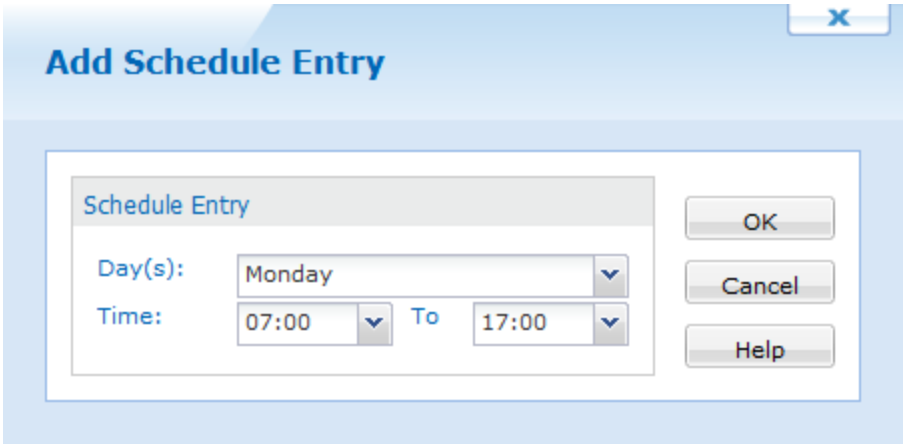
Connection Settings tab

Connection Mode

In any connection mode, the Device Agent does not force the mobile device to establish a network connection; it only takes advantage of an existing network connection.

Option	Description
Persistent	In this mode of operation the Device Agent will persistently try to establish and maintain a TCP/IP connection with the Deployment Server. This maximizes the amount of time the device is connected to MobiControl, ensuring that it is able to quickly receive updates and available for remote control.

Option	Description
	This is the recommended mode of operation for most installations.
Scheduled	In this mode of operation the Device Agent will only attempt to establish and maintain a TCP/IP connection with the Deployment Server during the defined time periods. Within the set time periods, the Device Agent operates in a "persistent" mode. Outside of the set time periods, the Device Agent will remain disconnected from the Deployment Server unless a connection is manually initiated by the device user. This is the recommended mode of operation for installations where it is not necessary for the device to always be connected to the Deployment Server. It is important that the time frame configured takes into consideration the device update schedule, and file synchronization schedules. These schedules can only be executed when the device is connected to the Deployment Server. **TIP:** If you are experiencing aggressive battery consumption with the persistent connection mode, switch to the Scheduled mode, and specify a narrow time frame (e.g. 1–2 hours)
Manual	In this mode of operation the Device Agent will never automatically attempt to establish a connection to the Deployment Server. Connections must be initiated by the device user via the device configuration applet. This is the recommended mode of operation for installations where only the remote help desk facilities of MobiControl are being used (not using deployment rules or file sync rules), and it is acceptable and/or required that the device user initiate the connection to the Deployment Server.



Add Schedule Entry settings dialog box

Connection Retry Interval

This setting determines how long the Device Agent should wait before trying to contact the Deployment Server again after a failed attempt. If your device will experience long periods disconnected from the Deployment Server, you should set this value high in order to prevent battery drain.

Option	Description
Allow Inbound TCP/IP(DIRECT) Remote Control Connections	This box needs to be checked if you intend to connect to your mobile device using the **TCP/IP (DIRECT)** connection mode. This option will enable the **Allow Inbound TCP/IP Connections** option in the Device Agent on the mobile device.

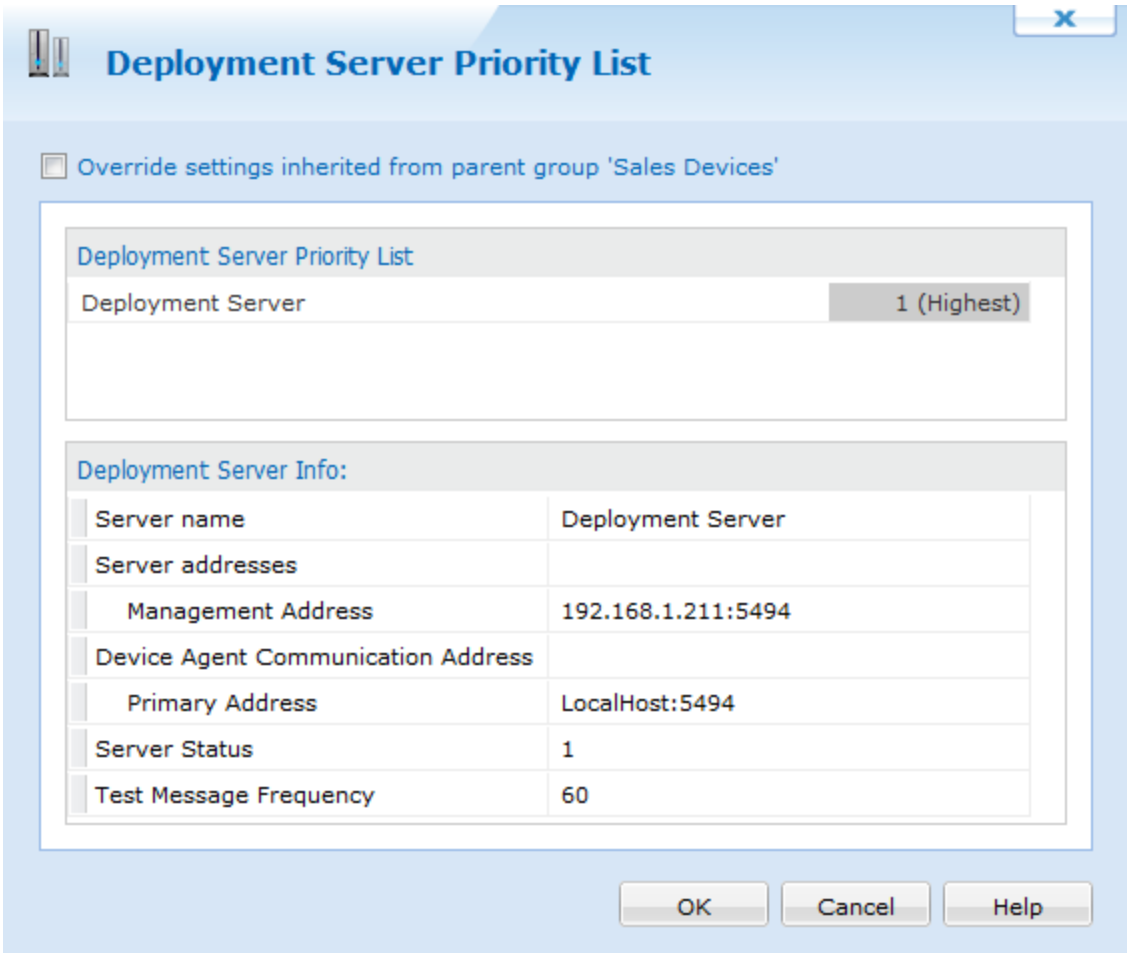
Log File Management

This set of options allows you to tune how the debug log files are managed on the device. Log management works by waiting for the log file to grow to a maximum threshold. Once the given threshold is met, the log file size is reduced down to the given minimum threshold by purging all the older entries.

Option	Description
Minimum Log File Size	Threshold size up to which the log file will be purged.
Maximum Log File Size	Threshold size, reaching which will trigger the log file to be purged to the minimum log file size
Enable Debug Logging (Normally Off)	Enables event logging on the mobile device. All MobiControl-related activity and events will be logged to a log file.The log file can provide vital information to IT support staff in diagnostics and resolving any issues that might have been reported for the mobile device with respect to MobiControl. The mobile device may operate more slowly with this option checked.

Android Deployment Server Priority

The **Deployment Server Priority List** dialog box allows you to specify the Deployment Server preferences for the devices. Priority one is the highest and five is the lowest. When a device is configured with more than one Deployment Server, it will try to connect to highest priority one first. If this server is not accessible, then it will try to connect to the next server available.



Deployment Server Priority List dialog box

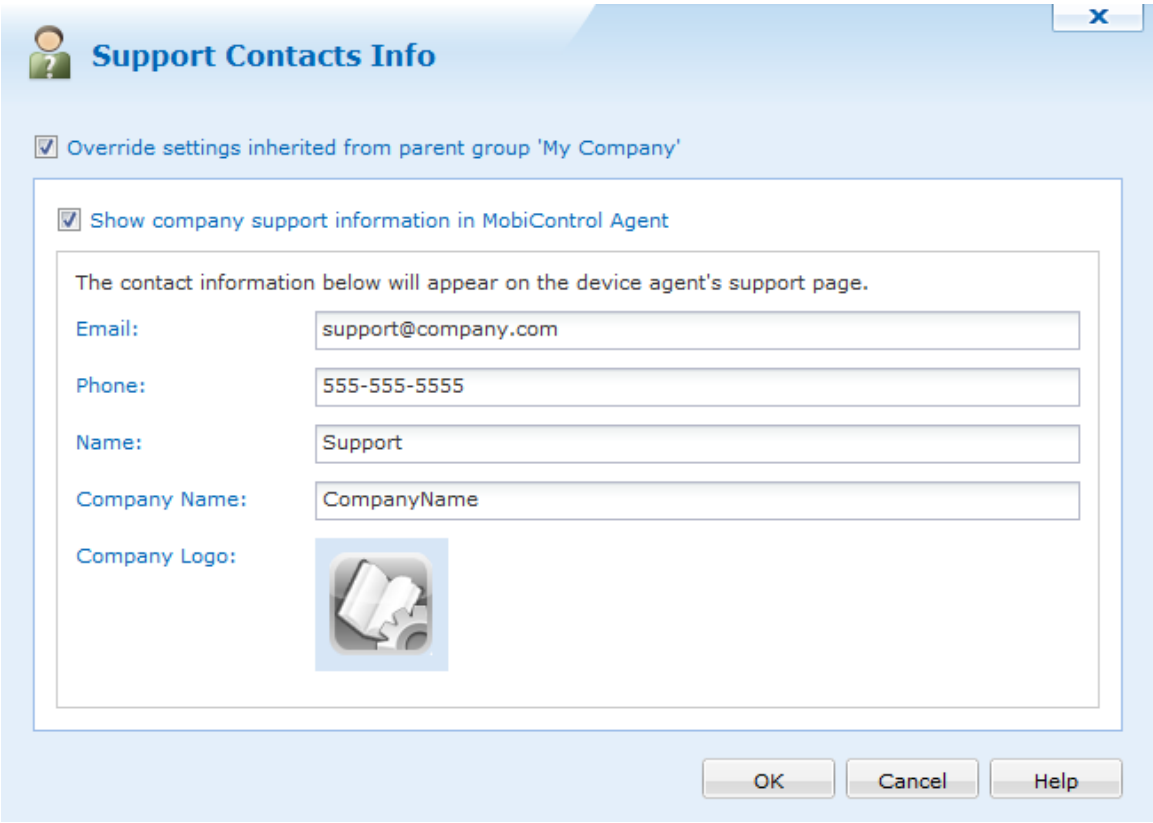
Multiple servers may be assigned the same priority level to establish a pool of Deployment Servers to balance the load of a large number of devices.

If you select "Not used," the selected devices will not connect to that Deployment Server.

Deployment Server priority is only applicable when you have installed multiple Deployment Servers using the same site name.

Android Support Contacts Info

The Support Contacts Info panel allows us to set contact information when a user opens up the MobiControl agent on their device. Information that we are able to configure are Email, Phone, Name, Company name and a company logo.



Support Contacts Info dialog box

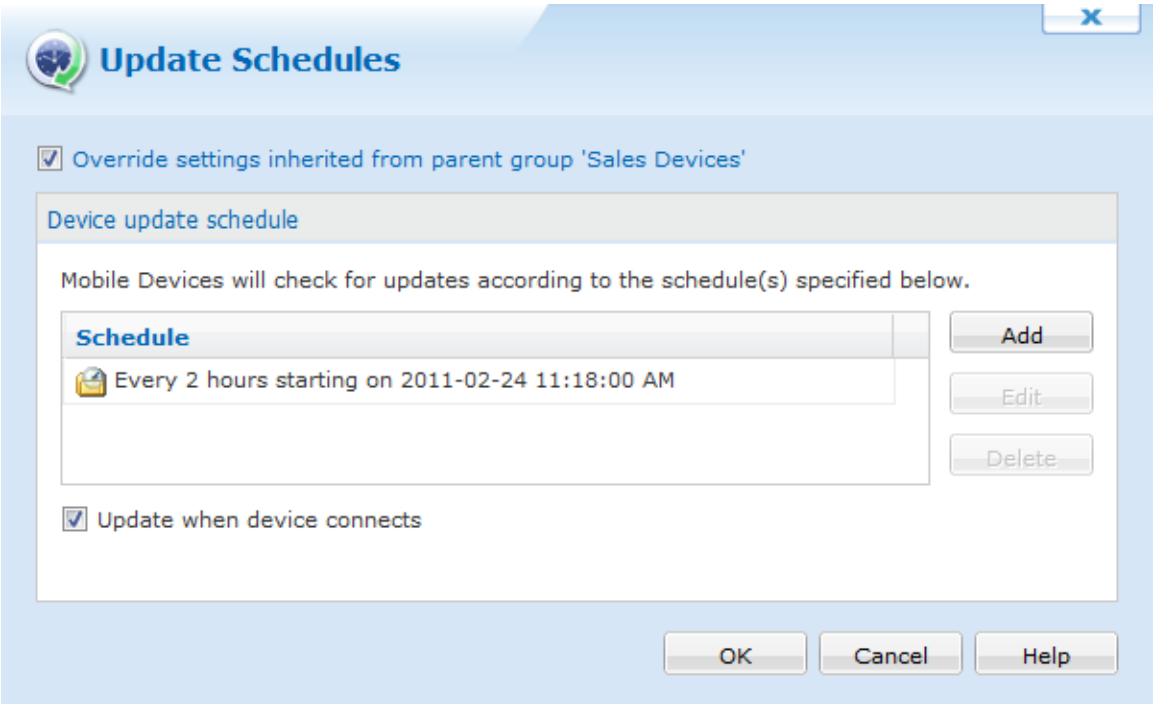
When each of the fields are set and OK is pressed, this information will then be sent down to the devices where this was configured on. When a user opens up their MobiControl agent and goes to the support info tab, they will be able to see the appropriate information.

Android Update Schedule

The device update schedule specifies when the device(s) should query the Deployment Server(s) for updates. Updates may include the addition, update, or removal of packages and modifications to device settings.

If the Deployment Server determines there are pending updates for the device, it immediately sends them to the device. The device also sends the Deployment Server a summary of its installed packages and settings. If the Deployment Server identifies an inconsistency, such as a previously-installed package that is missing on the device, the Deployment Server will re-install the package.

The initial device update schedule is specified by the add devices rule used to add the device(s) to the system. You may edit the schedule for an individual device or a group of devices that have been added to the system by selecting the target device or group in the device tree view in the main console window and selecting **Update Schedules** from the **Configure Device(s)** sub-menu.

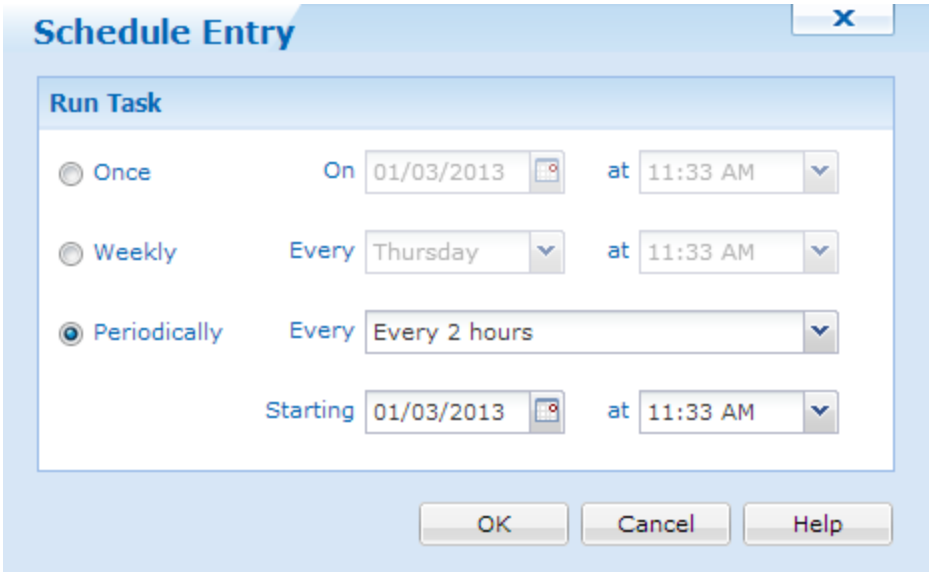


Device Update Schedules dialog box

The following table describes the **Device Update Schedules** dialog box:

Field Name	Description
Add	Select **Add** to specify additional update intervals. The **Schedule Entry** dialog box will be displayed. **EXAMPLE:** To sync a device twice a week, Monday at 06:00 and Friday at 19:00, create two weekly schedule entries.
Edit	Select **Edit** to modify an existing schedule entry. The **Schedule Entry** dialog box will be displayed.
Delete	Select **Delete** to permanently remove an update schedule entry from the dialog box.
Update when device connects	Select this check box to have the device(s) check for updates whenever they connect to a Deployment Server, that is, at every transition from offline to online. If this check box is not selected, the device(s) will only check for updates according to the schedule defined above.

Schedule Entry



Schedule Entry dialog box

The **Schedule Entry** dialog box allows you to specify schedule entries as one-time or periodic events.

Field Name	Description
Once	The device will check for updates once at the specified date and time.
Weekly	The device will check for updates once a week, on a specific day at a specific time.
Periodically	The device will check for updates periodically, at the specified interval from the set start date and time.

Android Sending Messages and Scripts

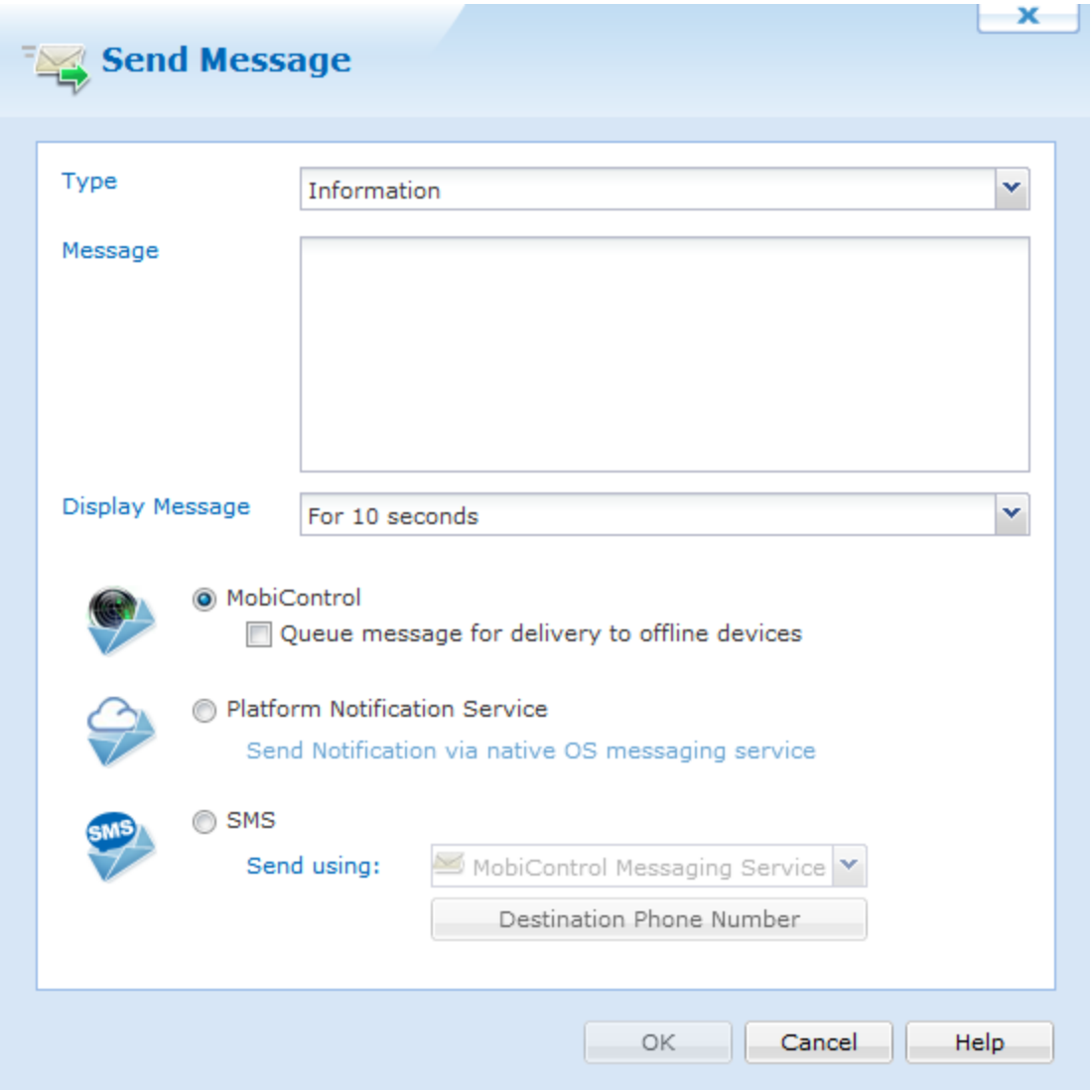
Select this option to send a message or script to one or more mobile devices. These can be sent using MobiControl or SMS (Short Message Service) from any online device or device connected via ActiveSync device. This feature can be used to keep users informed or updated remotely.

In the MobiControl Manager, right-click on a device, select **Send** and click **Message** or **Script** to start sending messages to the mobile devices. You can also choose to soft rest or turn off or suspend the device.

If your mobile device can receive SMS messages, MobiControl offers a way to send messages to the device through text messages.

IMPORTANT:

Only messages can be sent through SMS for Android devices. Sending SMS scripts to devices is only supported by Windows Mobile. To view how to send scripts to Windows Mobile devices by SMS, click here.



Send Message dialog box displaying the different message types

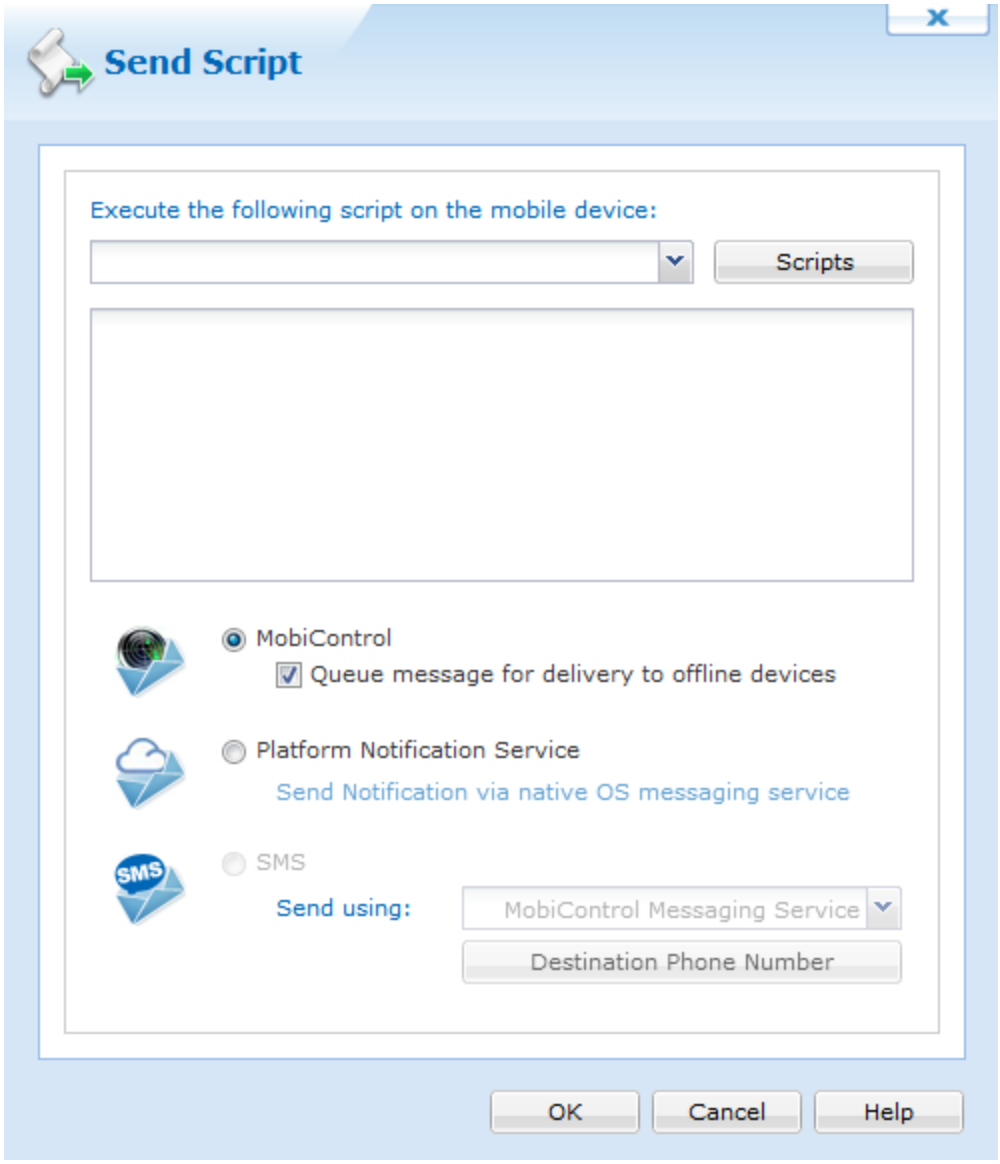
The table below describes each individual field of the **Send Message** dialog box:

Field Name	Description
Message Type	From the drop-down box, select the type of message you wish to send (information, exclamation, question, or error).
Message	A brief note to the recipient
Display the message on the device(s)	Select a time intervals for which the message can be displayed on the device.
MobiControl	Sends the messages via MobiControl. There is no character limit with this option.
Queue message	Sends the message to devices that are offline and will receive the message when they come online. The message will be stamped with the date and time it was sent.

Field Name	Description
for delivery to offline devices	
SMS (Short Message Service)	Send the message via SMS text message.
Send Using	Send a message using MobiControl's messaging service.
Destination Phone Number (s)	This is where the message will be delivered. This area is populated with the phone number(s) of the device you selected. If no phone number is present, you can double click the phone number area and manually enter a number.

Sending Scripts to the Device

If you want to run a custom script on a mobile device, you can do so with MobiControl. In the **Script** box, you can enter the script commands and instructions that you want to run on the device. When the instructions are received by the mobile device, it will then execute the script commands. These instructions can be sent using MobiControl or the device's platform notification service.



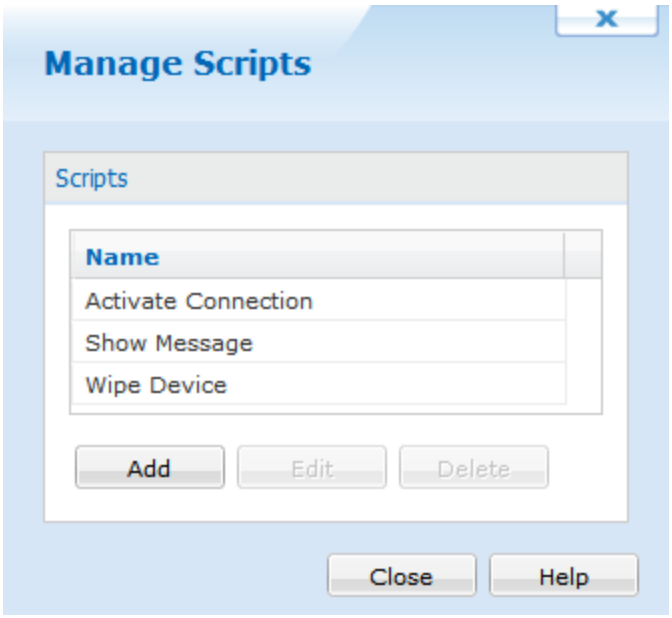
Send Script dialog box

The table below describes each individual field of the **Send Script** dialog box:

Field Name	Description
Scripts Drop Down	Select a pre-built script from the drop-down menu. Clicking the **Scripts** button opens the **Manage Scripts** dialog box where you can manage scripts. Please see the "Android Script Manager" topic below for more information.
Script	Preview or edit the selected script. Or manually type in a script from scratch.
MobiControl	Sends the messages via MobiControl. There is no character limit with this option.
Queue message for delivery to offline devices	Sends the message to devices that are offline and will receive the message when they come online. The message will be stamped with the date and time it was sent.
Platform Notification Service	Sends the script message via GCM.

Android Script Manager

You can use the **Manage Scripts** dialog box to centrally manage all of the scripts that you are using within MobiControl. The Script Manager comes pre-built with four of the most commonly used scripts. Each one is fully customizable. The Activate Connection script connects the device to MobiControl and activates the data connection if it isn't present. The Log Event script is used to log an event with your Deployment Server. The Show Message script is used to display a message on the device, and the Wipe Device script is used to wipe the device. The scripts here are stored within the MobiControl database, and can be accessed with any MobiControl Manager console. One way to open the **Manage Scripts** dialog box is to right-click on a device or group, select **Send,** and click **Script.**

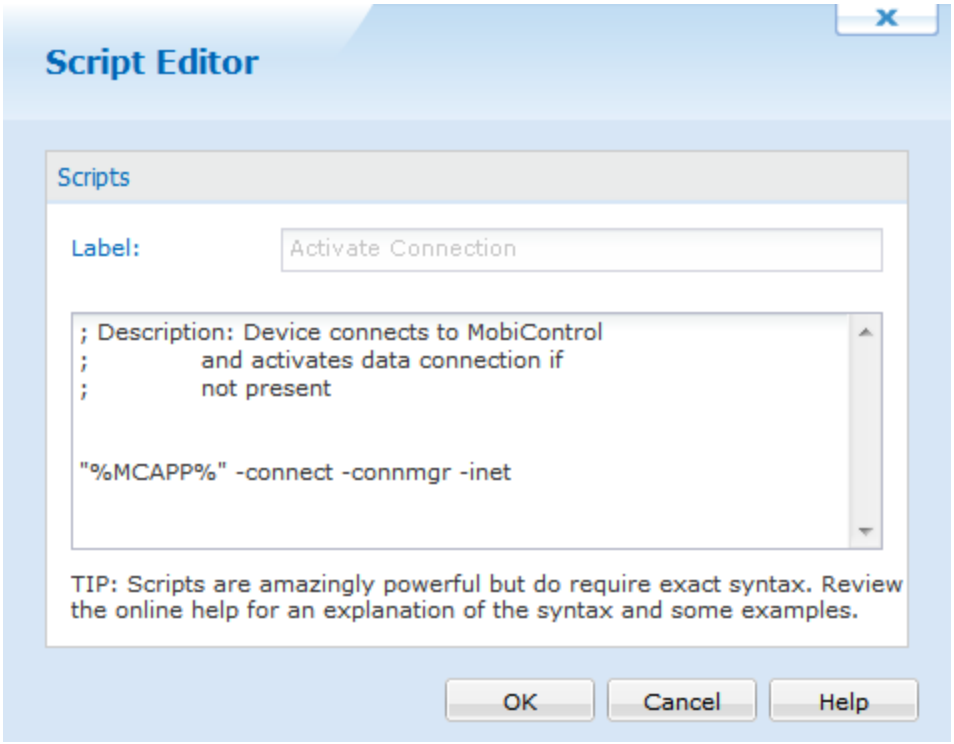


Manage Scripts dialog box

The following table describes the features of the **Manage Scripts** dialog box:

Field Name	Description
New	Creates a new script
Edit	Edits the selected script
Delete	Deletes the selected script
Import	Allows you to import a `.cmd` file containing MobiControl script commands. Please see the "Script Command Set" topic on page 72 for a full list of script commands.

Clicking the **New** button will bring up the **Script Editor** dialog box. In this window you can enter any script command that you would like to run on the device. Please see the "Script Command Set" topic on page 72 for a full list of script commands.



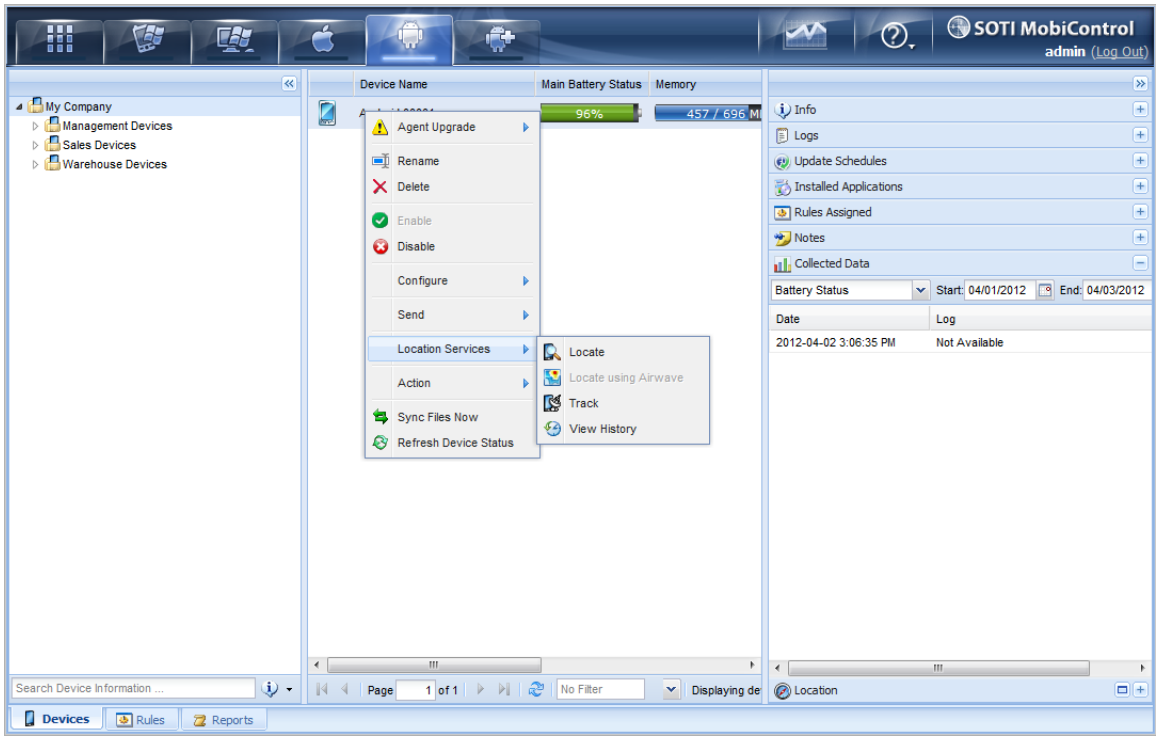
Script Editor dialog box

Android Location Services

MobiControl's Location Services provides the ability to locate and track mobile devices that are equipped with a GPS receiver that is internal or external to the unit. In order to locate a device, the GPS must be enabled and correctly configured on your device. The GPS determines the current location based on its

position relative to orbiting satellites. In order for this to happen, the device requires a clear view of the sky. Determining location may not be possible if the device is inside buildings or has an obstructed view of the sky.

You can activate Location Services for a device in MobiControl by right- clicking on a device and selecting the **Location Services** option from the menu. The first time you select an option from the Location Services menu for a device, it will automatically use the next available license. If there are no more licenses available, you will be notified to contact SOTI for information on acquiring additional licenses for Location Services.



Android Location Services

Please See the "Contact Us" page to contact us for more details on acquiring additional licensing.

NOTES:

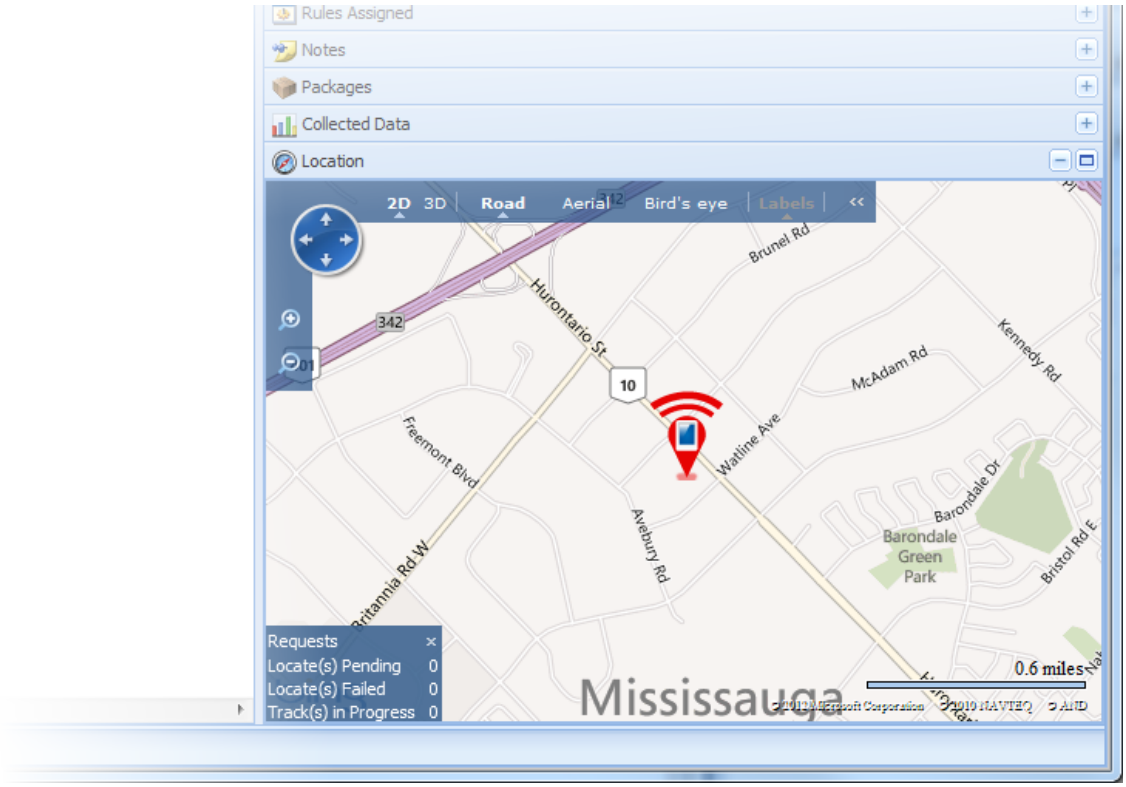
- When using Location Services in MobiControl to track devices, Internet Explorer 7 or higher is required.
- The Current Format for Regional and Language Options on your PC MUST be compatible with Bing Maps. Click here for a list of supported Bing Map control settings.

Android Locate Feature

To use the Locate feature in MobiControl's Location Services, right-click on the device you wish to locate, select **Location Services,** and click **Locate.**

The locate feature will use the GPS unit associated with your mobile device to determine the current latitude and longitude of the device. These coordinates are returned to MobiControl and displayed in the Location panel using Microsoft's Virtual Earth. The coordinates plotted in the Location panel represent the exact position of the device at the time of the request. To follow the position of the device in real time, use the **Track** option under the **Location Services** menu.

You can locate the position of multiple devices at once: select the parent folder or hold the CTRL key and select all the devices you wish to locate, right-click, select **Location Services,** and click on **Locate.** In order to use the Locate feature, the device(s) must be online and communicating with the MobiControl Deployment Server. The status of the current (and completed) Locate and Track commands is displayed in the lower left hand corner of the screen.



Location Services locate user interface

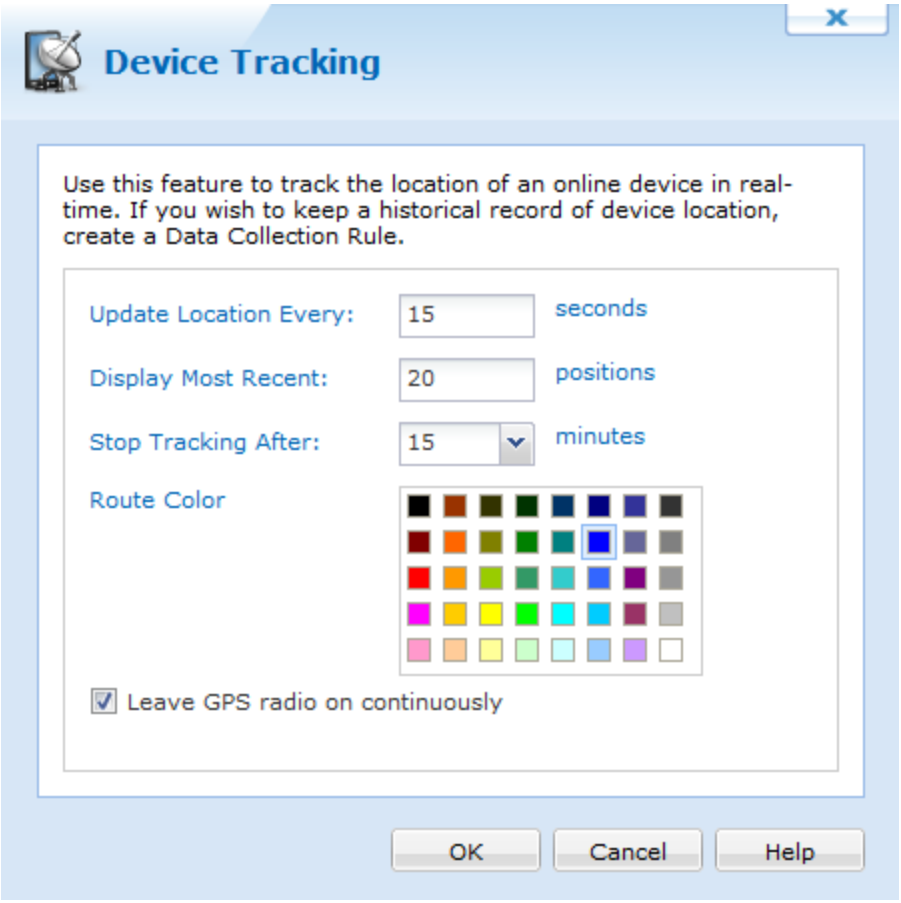
Th

NOTE:

If the MobiControl Manager is behind a proxy server and you are unable to use Location Services, please run the following command through the **Start** menu then **Run**:
`netsh winhttp set proxy -server="http=<ProxyServerIP>: <Port>; https=<SSLProxyServerIP>: <Port>"` (on Windows Vista, **with no spaces between the quotation marks**.)
This command will update the WinHTTP service with the settings from Internet Explorer.

Android Tracking

To use the Track feature in MobiControl's Location Services, right-click on the device you wish to track, select **Location Services,** and click **Track.**



Device Tracking dialog box

The track feature will use the GPS unit associated with your mobile device to determine the current latitude and longitude of the device at a given schedule and send the co-ordinates back to the MobiControl Deployment Server. These co-ordinates are then displayed in the Location panel using Microsoft's Virtual Earth. The co-ordinates plotted in the Location panel represent the exact position of the device at the time of the request along with where the device has been since the request was initiated. To view where the device has been in the past, you need to use the show history option within MobiControl's Location Services.

In order to use the track feature, the device must be online and communicating with the MobiControlDeployment Server.

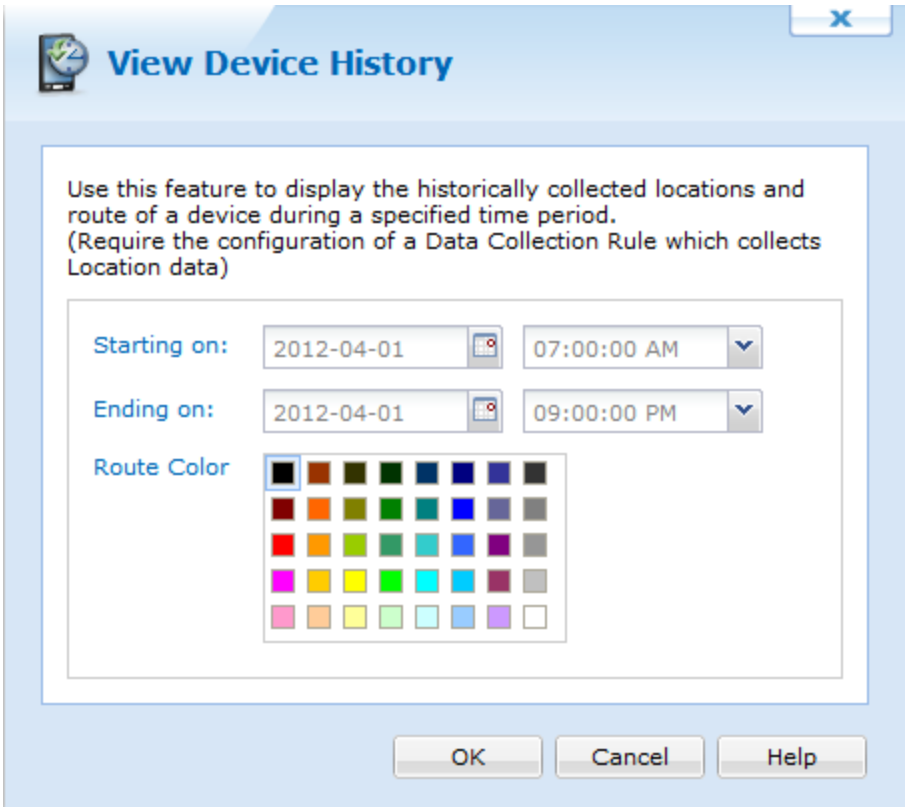
The following table describes each field in the dialog:

Feature	Description
Update Location Every	Set a time interval in seconds (5–86400) for how frequently you would like to have the device location reported.
Display Most Recent	Choose a value to represent the number of recent positions (maximum 100) that you would like to see plotted on the map of the device(s) that you will be tracking.
Stop Tracking After	Set the time interval in minutes (5– 60) for when you would like to end tracking the device.
Route Color	Identifies the device route you will be tracking
Leave GPS radio on continuously	For faster response time from the GPS radio on the device, you should enable this check box. The device's GPS radio will constantly be on.

Show Tracking History

The show history feature will use the GPS unit associated with your mobile device, allowing you to view where the device has been over a given period of time. To use this feature, you need to set up a data collection rule that collects the location information from the device on a given schedule. The data will be sent back to the deployment server, or, if there is no active data connection on the device, it will be collected and stored in a temporary file and then sent back to the server the next time the device connects. The show history feature does not require the device to be online and communicating with the MobiControl Deployment Server. You can plot information from the history that has been transmitted back to the server during the last active connection.

To use the show history feature, right-click on the device you wish to view, select **Location Services,** and click **Show History.** You will then be prompted to enter the time period for which information is desired, and the route color. Once this is filled in, click **OK** and the path will be plotted.

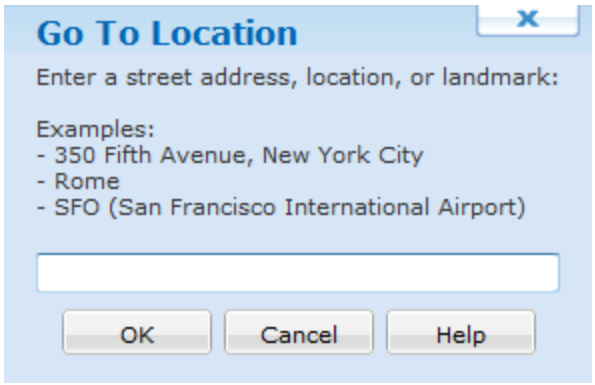


View Device History dialog box

Feature	Description
Starting On	Enter the date and time that you wish to start.
Ending On	Enter the date and time that you wish to stop.
Route Color	Select the color to be used on the map when connecting the co-ordinates.

Using Go To Location

Go To Location allows you to quickly centre and zoom the map to a specific location. Go To Location is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "Android Location Services" topic on page 1193 for more information.

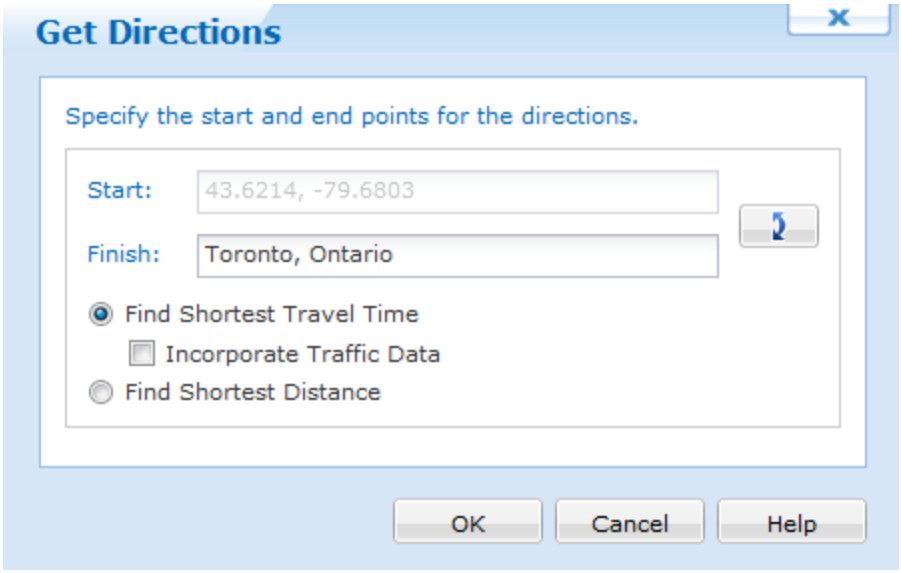


Go To Location dialog box

To use this feature, right click on the Location panel and select "Go To..." from the pop-up menu that appears to open the Go To Location window. You can then enter an address, location, landmark, or the name of an existing geofence. Once you have entered the location information, click the OK button and the map will reload centring on the information you provided. If you entered the name of an existing geofence, the map will change to the location of that geofence and display it on the screen in red.

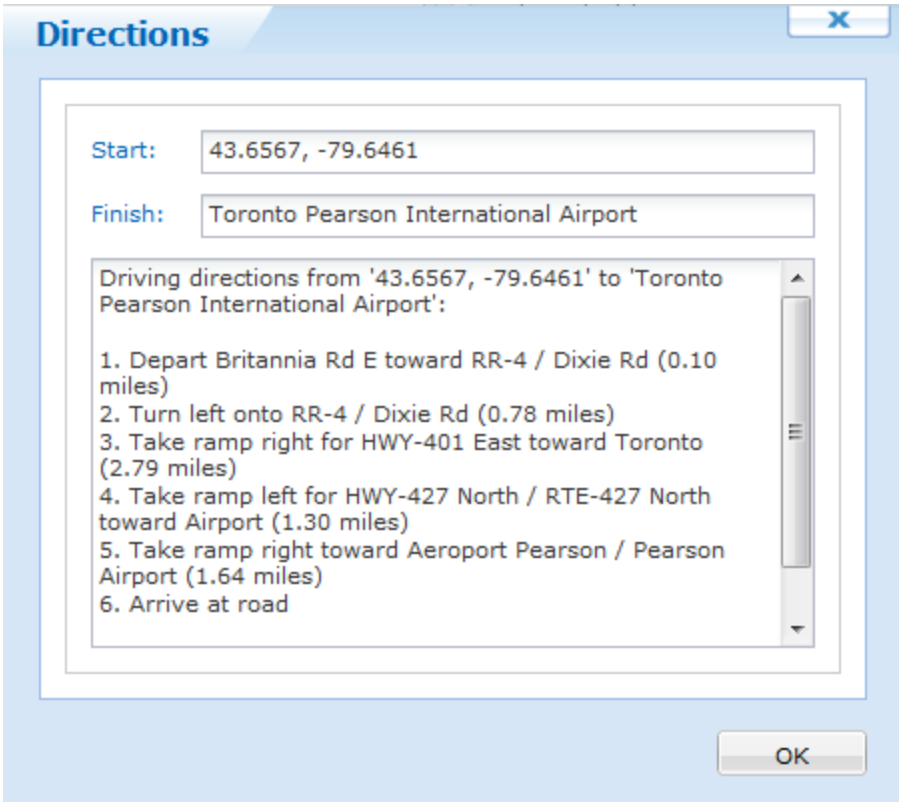
Get Directions

Powered by Microsoft's Bing Maps, MobiControl's Get Directions will return turn-by-turn directions between two locations on the map. These directions can be sent directly to the device, or they can be pasted into an email and sent to a larger group of people. Get Directions is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "Android Location Services" topic on page 1193 for more information.



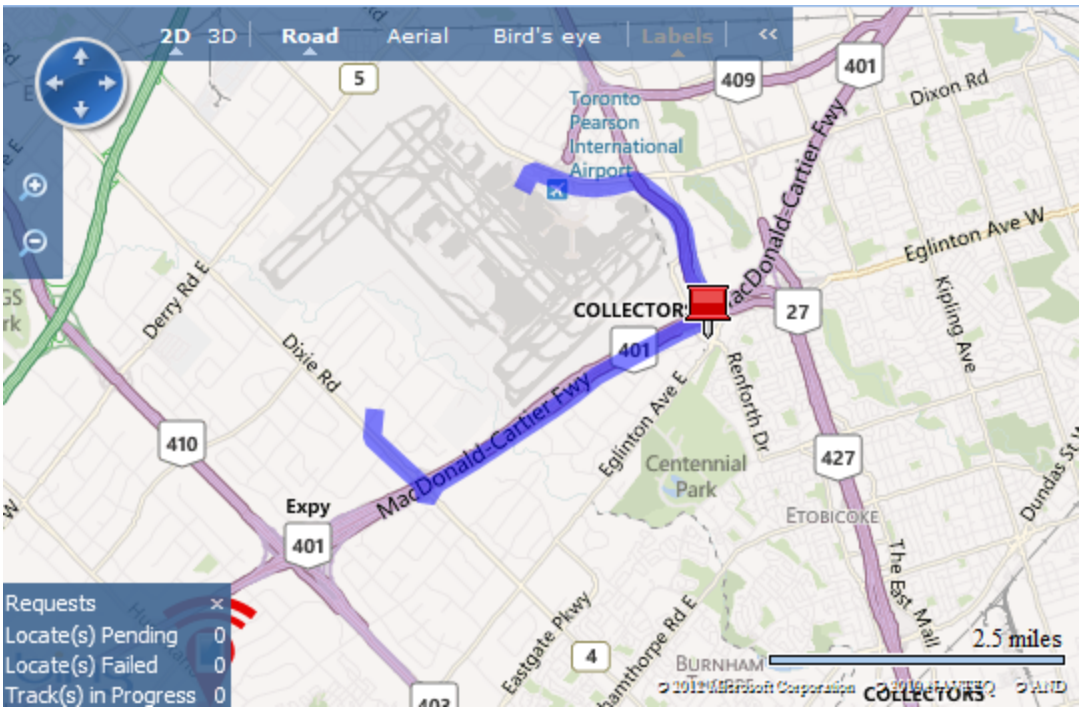
Get Directions dialog box

To use Get Directions, in the Location panel right click on any device or a point on the map and select "Get Directions" from the pop-up menu. The Get Directions dialog box will appear. Be default, the device or map location clicked on will be used as the starting point. To change this, click the double arrow button located to the left of the Start and Finish fields. You can enter GPS co-ordinates, landmarks, or an address. Directions can be optimised by selecting shortest travel time or shortest distance from the options list and press the OK button.



Driving Directions window

MobiControl will determine the turn-by-turn driving directions between the two locations you specified. The resulting directions will be displayed in the Driving Directions window. If you started by right clicking on a device, the "Send to Device" button will be enabled and you can send the instructions directly to the device. You can copy the directions from this window and paste them into an email or document or your choice.

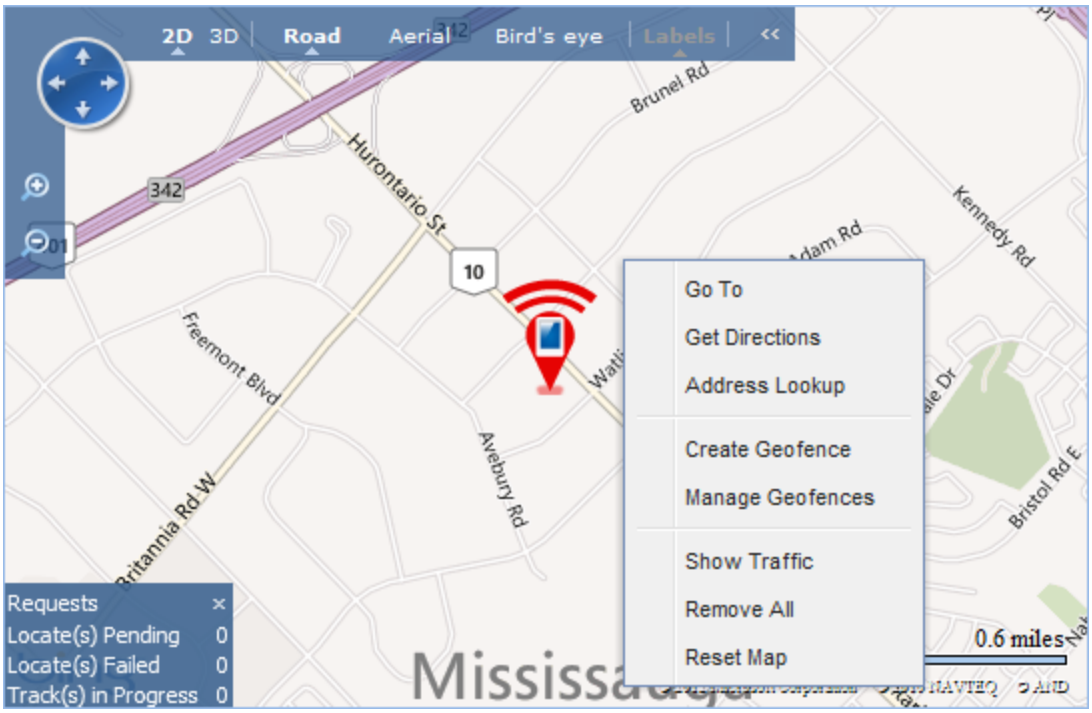


Driving directions displayed on the Map

The Location panel will reload the map to show the driving route highlighted. If the map is in Bird's Eye view, the highlight will not be displayed. Both Aerial and Road view will display the highlighted route.

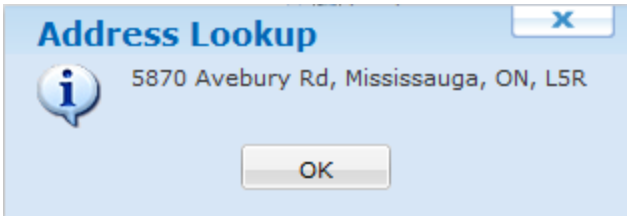
Address Lookup

The Address Lookup feature allows you to determine the address of a specific point on the map displayed on the Location panel. Address Lookup is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "Android Location Services" topic on page 1193 for more information.



Location panel right click menu with Address Lookup option

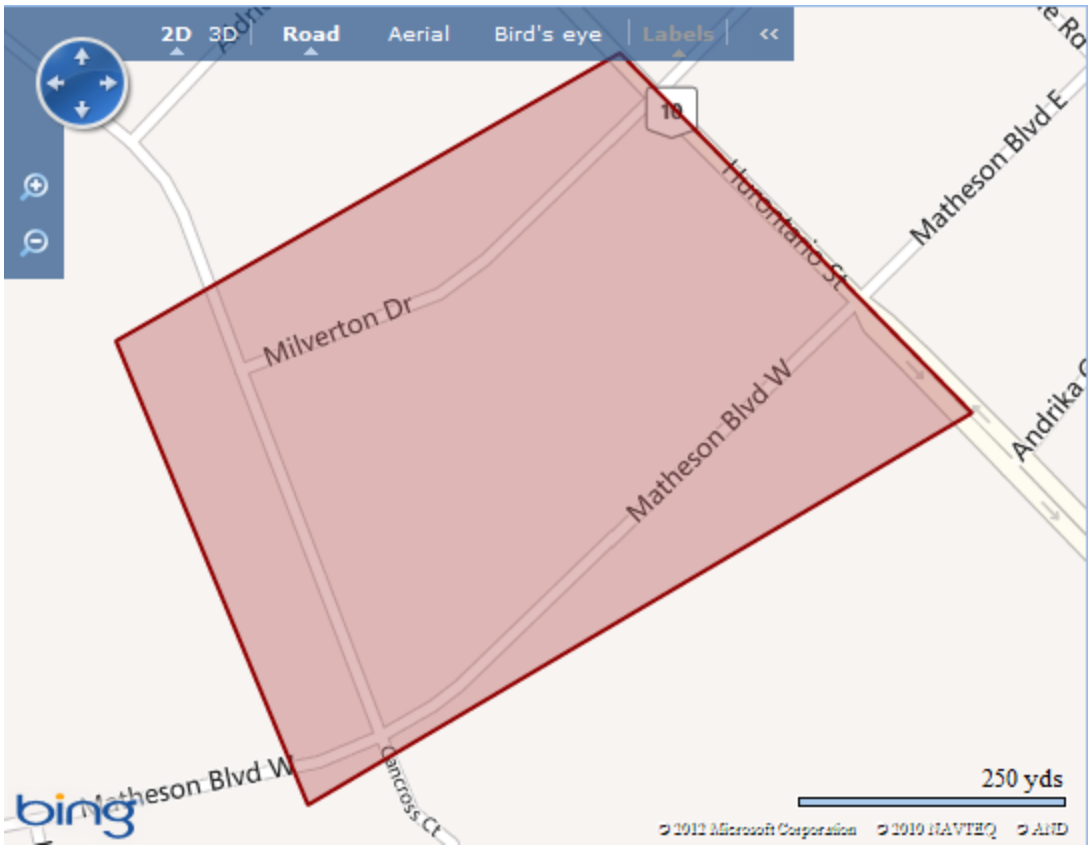
To use the Address Lookup feature, right click anywhere on the map in the Location panel and select the Address Lookup option from the menu that appears. The address of that location will be displayed in a new information window.



Address Lookup window

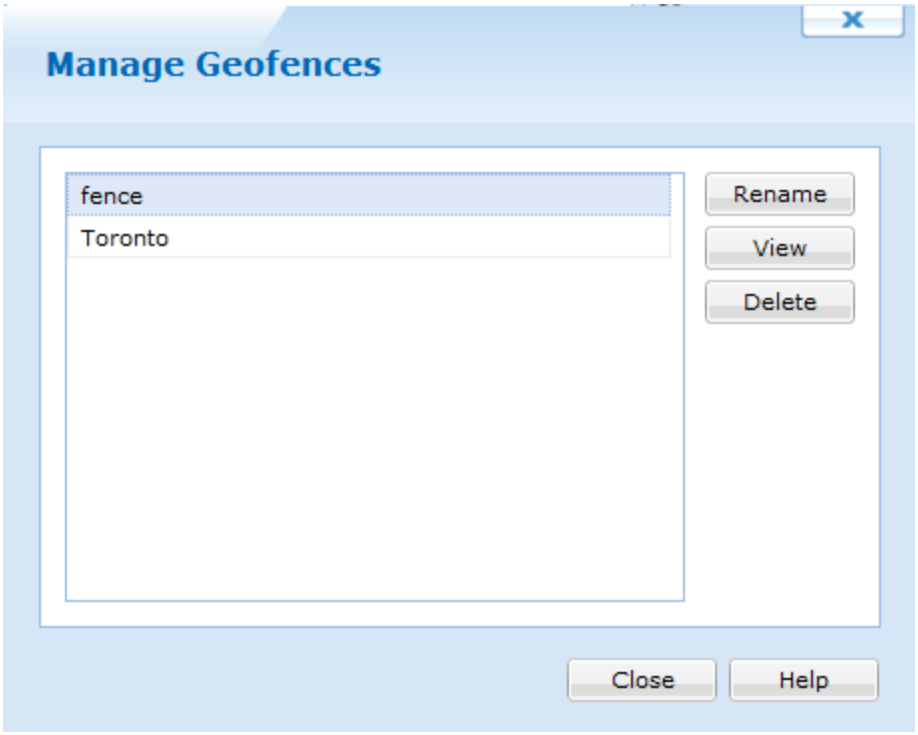
Using Manage Geofences

The Manage Geofences feature provides an area in which to rename, delete or view current created Geofences. You also have the option to create a new geofence from the drop down menu.



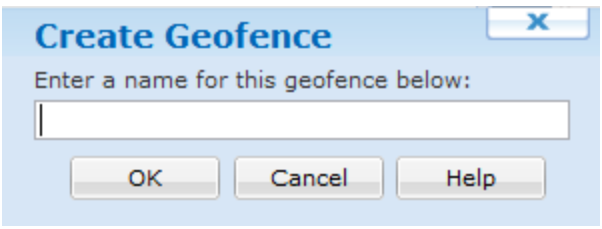
Location panel right click map and select Manage Geofence option

Selecting Manage Geofence brings up the following window.



Field Name	Description
Rename	Allows you to rename a Geofence
View	Allows you to view an already created Geofence on the map
Delete	Allows you to delete a Geofence **NOTE:** In order to Delete the Geofence, no Geofence Event can be associated with it

The **Create Geofence** option allows you to begin drawing on the map. The area drawn on the map will be defined as the Geofence. The defined area must be a complete geometric shape, which means the Start Drawing point will be the same as the End Drawing point. When you have completed a proper geometric shape you be asked to name your geofenced area.



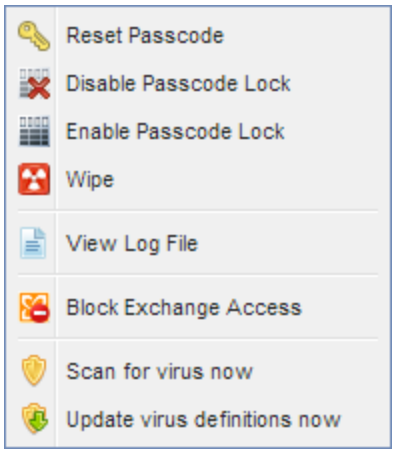
Android Actions

MobiControlallows you to reset passcodes, disable/enable passcode locks, wipe devices and block/unblock Exchange access on a group or an individual device level. These options can be viewed when you right click a device group/device and go to **Action**.

Device Level Actions

Selecting actions on a device level allows you to specifically send actions to that particular device. From here you can reset, disable or enable the passcode, wipe the device, view log file and block or enable Exchange Access. To successfully use the Block/unblock Exchange Access action, you must have the Exchange ActiveSync filter installed on your Exchange Server. For more information on how to install this, please Skin/Formats/CrossReferencePrintFormat(See "Secure Email Access Install The Secure Email Access Filter allows you to achieve greater control with devices receiving email from your Exchange Service. When the filter is installed, you can block access to Exchange on certain devices as well as other controls. To successfully install the Exchange ActiveSync Filter, the MobiControl Root CA must be installed on the server that is publishing the Exchange ActiveSync Service. Below shows how to install the filter on your Exchange Server. Prerequisite StepsInstall MobiControl's Secure Email Access filter (Optional) 3rd party Exchange ActiveSync Filter Configuration Prerequisite StepsThe prerequisite steps show how to install the MobiControl Root CA on the Exchange Server. Go to the MobiControl Administration Utility and go to Certificates. The MobiControlAdministration Utility (MCAU)Click the Export button at beside the MobiControl Root Certificate label. Export the MobiControlRoot CertificateSave the exported certificate in a directory that is easy to remember. Next we need to go to the server with the Exchange ActiveSync Service.Open the Microsoft Management Console (MMC) by opening up the run command and typing mmc. Open the Microsoft Management Console. In MMC, click File then Add/Remove Snap In...Adding Snap-insSelect the Certificates snap-in and click Add >. Adding the Certificates Snap-inA new window will appear asking to select an account. Select the Computer account and click Next. Select the Computer Account. On the next screen select Local Computer and click Finish. Select ComputerAfter clicking Finish, click OK in the Add or remove Snap-ins window. Expand the Certificates (Local Computer) tree on the left side and go to Trusted Root Certification Authorities, then Certificates. Right click the Certificates folder and go to All Tasks then Import.Importing a new CA Follow the steps in the Certificate Import Wizard leaving all settings default. After the wizard has finished you will see the MobiControl Root CA in your Trusted Root Certification Authorities. The MobiControl Root CAInstall MobiControl's Secure Email Access filterMobiControl's Secure Email Access Filter must be installed on the server that is publishing the Exchange ActiveSync service. Typically this is the same computer that is hosting OWA (Outlook Web Access). From the server where the Secure Email Access filter will be installed, open Internet Explorer and browse to the MobiControl Web ConsoleLog in to the Web Console as an Administrator based account that has the "Configure Deployment Servers" permissionSelect the All Devices tab at the top of the MobiControl Web Console and then select the Servers tab located along the bottom of the Web ConsoleRight click on the Secure Email Access filter listed under the Deployment Server, and select Install Exchange ActiveSync FilterSave and then run the ExchangeActiveSyncFilter.exe program. This will place the needed files onto the server. Note: Depending on your Internet Explorer settings, you may be prompted to allow file downloads from the web pageOpen IIS manager and select the web site that is publishing Exchange ActiveSync Select ISAPI filters and select Add from the list of actionsEnter MobiControl Secure Email Access as the filter name For the Executable, If the Exchange ActiveSync site is running in a 32-bit application pool, select \Program Files\SOTI\XAS\mcxas.dll or, if the Exchange ActiveSync site is running in a 64-bit application pool, select \Program files\SOTI\XAS\mcxas64.dllSelect OK to save the filterIn the resulting list of filters, ensure that the MobiControl Secure Email Access filter is listed above the Microsoft Exchange ActiveSync filter. If this is not the case, select View Order List from the available actions, highlight MobiControl Secure Email Access and select Move Up to place it at the top Note: MobiControl's Secure Email Access required communication between the server that is publishing Exchange ActiveSync where the filter is installed, to the MobiControl Web Console. This communication happens over SSL on

port 443.3rd party Exchange ActiveSync Filter ConfigurationBefore you begin, the following components must be installed/enabled.1. IIS 7 with ASP.NET role service enabled.2. URL Rewrite Module installed (version 2.0 is required)3. Application Request Routing version 2.5 (Link)The URL Rewrite Module and Application Request Routing version 2.5 are both installed at the same time. After installation, please follow these steps:Open the IIS managerSelect the server in the tree view on the left hand side and then click on the Application Request Routing feature.Application Request RoutingOn the right menu, click Server Proxy Settings in the Proxy SectionServer Proxy SettingsCheck the Enable Proxy check box. Leave the default values for all the other settings on this page. Click Apply on the right side to commit the change.Enable ProxyNext step is to add the HTTP_ACCEPT_ENCODING server variable and Inbound and Outbound rules. To do this, please go to the left hand panel and select the Default Web Site and then select URL Rewrite. URL rewriteIn the URL Rewrite page, select View Server Variables on the right hand side. View Server VariablesClick the Add... link on the right side of the page to add the HTTP_ACCEPT_ENCODING variable. Click OK then Back to Rules. Adding a server variableClick the Add Rule(s)... link on the right side to add Inbound and Outbound rules. Add rule(s)...When creating the Inbound and Outbound rules, select Blank Rule under the respected heading and click OK.Adding a Blank Inbound or Outbound ruleOn the page shown below, the following fields need to have values entered (Please ensure that you enter your appropriate owa address):NameReverseProxyInboundRule1Pattern^(.*)Rewrite URLhttps://owa.myDomain.com/{R:1} Inbound Rule creation pageAfter the values have been entered, the server variable needs to be added. To do this, expand the Server Variables panel. Click Add and choose HTTP_ACCEPT_ENCODING from the drop down menu. Under value, enter 0, then click OK. Set Server VariableAfter entering all required values, click Apply.Apply Inbound RuleCreate a new blank rule to create an Outbound Rule. Please see below for what values to set on this page: Outbound rule pageUnder precondition, you will need to create a new condition. To do this, select <Create New Precondition...>. When the pop up window appears, click Add... to add a pattern:Add PreconditionAfter entering all required values, Click OK then click Apply.Apply Outbound RuleAfter the rules have been created, click the IIS server, and restart. To confirm that everything has been configured properly, go to C:\inetpub\wwwroot and open the web.config file in notepad. Your file should look similar to this: <?xml version="1.0" encoding="UTF-8"?> <configuration> <system.webServer> <rewrite> <rules> <rule name="ReverseProxyInboundRule1"> <match url="^(.*)" /> <serverVariables> <set name="HTTP_ACCEPT_ENCODING" value="0" /> </serverVariables> <action type="Rewrite" url="https://owa.soti.net/{R:1}" /> </rule> </rules> <outboundRules> <rule name="ReverseProxyOutboundRule1" preCondition="ResponseIsHtml1"> <match filterByTags="A, Form, Img" pattern="^http(s)?://owa.soti.net/(.*)" /> <action type="Rewrite" value="http{R:1}://owa.soti.net/{R:2}" /> </rule> <preConditions> <remove name="ResponseIsHtml1" /> <preCondition name="ResponseIsHtml1"> <add input="{RESPONSE_CONTENT_TYPE}" pattern="^text/html" /> </preCondition> </preConditions> </outboundRules> </rewrite> </system.webServer> </configuration>" on page 1)



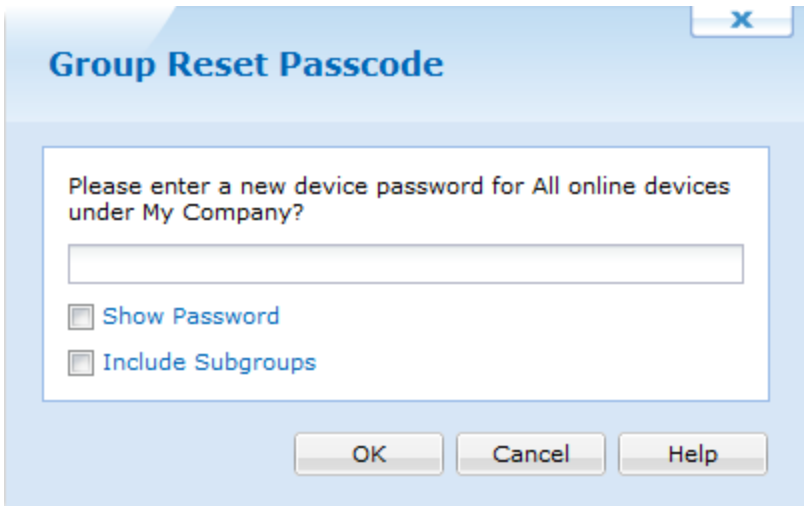
Android Device Action Selections

Group Level Actions

With group level actions, you are able to reset the passcode, disable/enable the passcode lock, wipe devices, and block/unblock Exchange access to every device under the group.

Reset Passcode

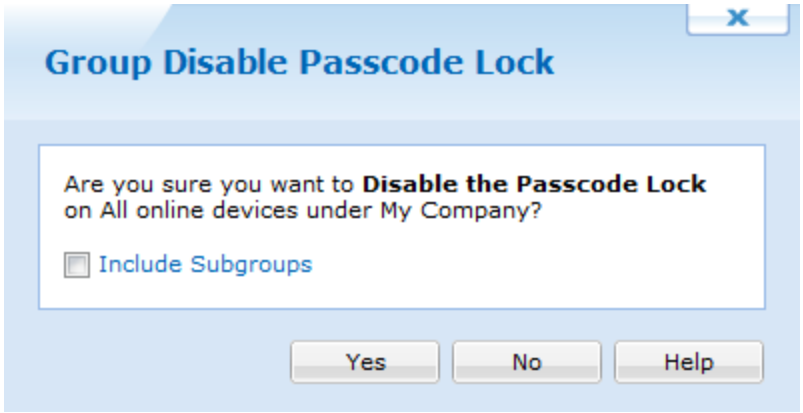
Reset Passcode allows you to reset the passcode for every device in the group. This can be useful when you move multiple devices into a specific group for resetting passcodes.



Group Reset Passcode

Disable/Enable Passcode Lock

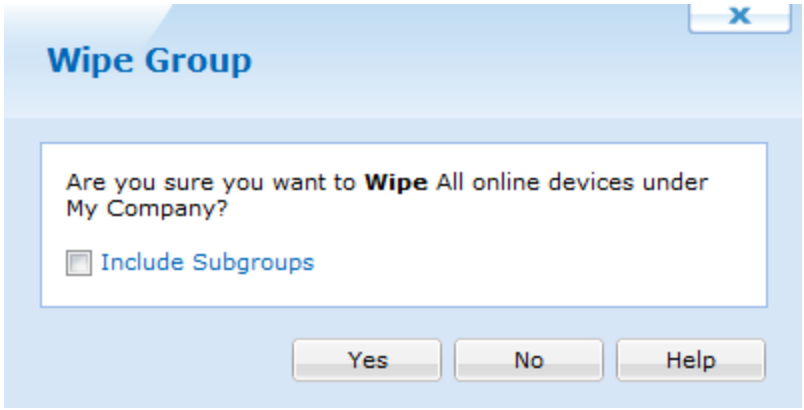
Using the Disable Passcode Lock turns off the pin code on the lock screen in iOS devices. This can be useful when you move multiple devices into a specific group for resetting passcodes. Selecting Enable Passcode Lock enabled the pin code on the lock screen.



Disabling Passcode Lock

Wipe Device

Using the Wipe Device action allows you to delete all information and apps from the devices in the selected group. This can be used when you have devices that pass between multiple users and you do not want users to see previous users accounts or information.



Wipe Group

Block/Unblock Exchange Access

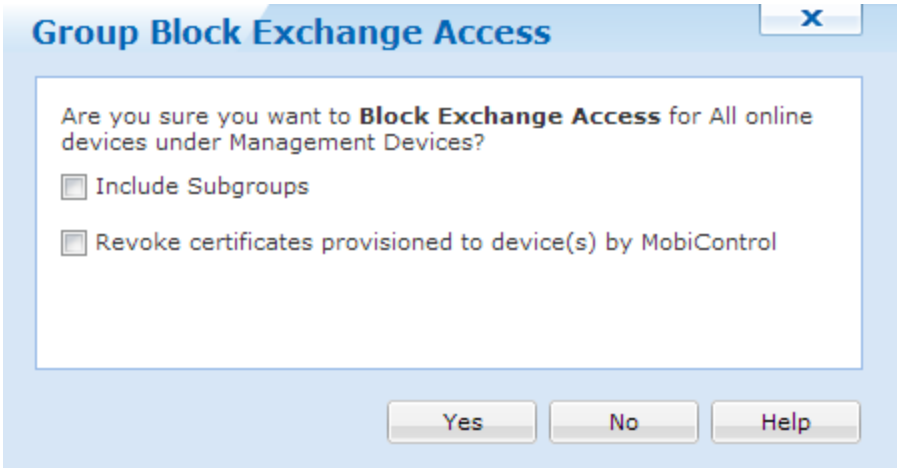
Using these options allow you to block and unblock Exchange access to every device in the group. To successfully use this action, you must have the Exchange ActiveSync filter installed on your Exchange Server. For more information on how to install this, please Skin/Formats/CrossReferencePrintFormat (See "Secure Email Access Install The Secure Email Access Filter allows you to achieve greater control with devices receiving email from your Exchange Service. When the filter is installed, you can block access to Exchange on certain devices as well as other controls. To successfully install the Exchange ActiveSync Filter, the MobiControl Root CA must be installed on the server that is publishing the Exchange ActiveSync Service. Below shows how to install the filter on your Exchange Server. Prerequisite StepsInstall MobiControl's Secure Email Access filter(Optional) 3rd party Exchange ActiveSync Filter Configuration Prerequisite StepsThe prerequisite steps show how to install the MobiControl Root CA on the Exchange Server. Go to the MobiControl Administration Utility and go to Certificates. The MobiControlAdministration Utility (MCAU)Click the Export button at beside the MobiControl Root Certificate label. Export the MobiControlRoot CertificateSave the exported certificate in a directory that is easy to remember. Next we need to go to the server with the Exchange ActiveSync Service.Open the Microsoft Management Console (MMC) by opening up the run command and typing mmc. Open the Microsoft Management Console. In MMC, click File then Add/Remove Snap In...Adding Snap-insSelect

the Certificates snap-in and click Add >. Adding the Certificates Snap-inA new window will appear asking to select an account. Select the Computer account and click Next. Select the Computer Account. On the next screen select Local Computer and click Finish. Select ComputerAfter clicking Finish, click OK in the Add or remove Snap-ins window. Expand the Certificates (Local Computer) tree on the left side and go to Trusted Root Certification Authorities, then Certificates. Right click the Certificates folder and go to All Tasks then Import.Importing a new CA Follow the steps in the Certificate Import Wizard leaving all settings default. After the wizard has finished you will see the MobiControl Root CA in your Trusted Root Certification Authorities. The MobiControl Root CAInstall MobiControl's Secure Email Access filterMobiControl's Secure Email Access Filter must be installed on the server that is publishing the Exchange ActiveSync service. Typically this is the same computer that is hosting OWA (Outlook Web Access). From the server where the Secure Email Access filter will be installed, open Internet Explorer and browse to the MobiControl Web ConsoleLog in to the Web Console as an Administrator based account that has the "Configure Deployment Servers" permissionSelect the All Devices tab at the top of the MobiControl Web Console and then select the Servers tab located along the bottom of the Web ConsoleRight click on the Secure Email Access filter listed under the Deployment Server, and select Install Exchange ActiveSync FilterSave and then run the ExchangeActiveSyncFilter.exe program. This will place the needed files onto the server. Note: Depending on your Internet Explorer settings, you may be prompted to allow file downloads from the web pageOpen IIS manager and select the web site that is publishing Exchange ActiveSync Select ISAPI filters and select Add from the list of actionsEnter MobiControl Secure Email Access as the filter name For the Executable, If the Exchange ActiveSync site is running in a 32-bit application pool, select \Program Files\SOTI\XAS\mcxas.dll or, if the Exchange ActiveSync site is running in a 64-bit application pool, select \Program files\SOTI\XAS\mcxas64.dllSelect OK to save the filterIn the resulting list of filters, ensure that the MobiControl Secure Email Access filter is listed above the Microsoft Exchange ActiveSync filter. If this is not the case, select View Order List from the available actions, highlight MobiControl Secure Email Access and select Move Up to place it at the top Note: MobiControl's Secure Email Access required communication between the server that is publishing Exchange ActiveSync where the filter is installed, to the MobiControl Web Console. This communication happens over SSL on port 443.3rd party Exchange ActiveSync Filter ConfigurationBefore you begin, the following components must be installed/enabled.1. IIS 7 with ASP.NET role service enabled.2. URL Rewrite Module installed (version 2.0 is required)3. Application Request Routing version 2.5 (Link)The URL Rewrite Module and Application Request Routing version 2.5 are both installed at the same time. After installation, please follow these steps:Open the IIS managerSelect the server in the tree view on the left hand side and then click on the Application Request Routing feature.Application Request RoutingOn the right menu, click Server Proxy Settings in the Proxy SectionServer Proxy SettingsCheck the Enable Proxy check box. Leave the default values for all the other settings on this page. Click Apply on the right side to commit the change.Enable ProxyNext step is to add the HTTP_ACCEPT_ENCODING server variable and Inbound and Outbound rules. To do this, please go to the left hand panel and select the Default Web Site and then select URL Rewrite. URL rewriteIn the URL Rewrite page, select View Server Variables on the right hand side. View Server VariablesClick the Add... link on the right side of the page to add the HTTP_ACCEPT_ENCODING variable. Click OK then Back to Rules. Adding a server variableClick the Add Rule(s)... link on the right side to add Inbound and Outbound rules. Add rule(s)...When creating the Inbound and Outbound rules, select Blank Rule under the respected heading and click OK.Adding a Blank Inbound or Outbound ruleOn the page shown below, the following fields need to have values entered (Please ensure that you enter your appropriate owa address):NameReverseProxyInboundRule1Pattern^(.*)Rewrite URLhttps://owa.myDomain.com/{R:1} Inbound Rule creation pageAfter the values have been entered, the server variable needs to be added. To do this, expand the Server Variables panel. Click Add and choose HTTP_ACCEPT_ENCODING from the drop down menu. Under value, enter 0, then click OK. Set Server VariableAfter entering all required values, click Apply.Apply Inbound RuleCreate a new blank rule to create an Outbound Rule. Please see below for what values to set on this page: Outbound rule pageUnder precondition, you will need to create a new condition. To do this, select <Create New Precondition...>. When the pop up window appears, click Add... to add a pattern:Add PreconditionAfter entering all required values, Click OK then click Apply.Apply Outbound RuleAfter the rules have been created, click the IIS server, and restart. To confirm that everything has been configured properly, go to C:\inetpub\wwwroot and open the web.config file in notepad. Your file should look similar to this: <?xml

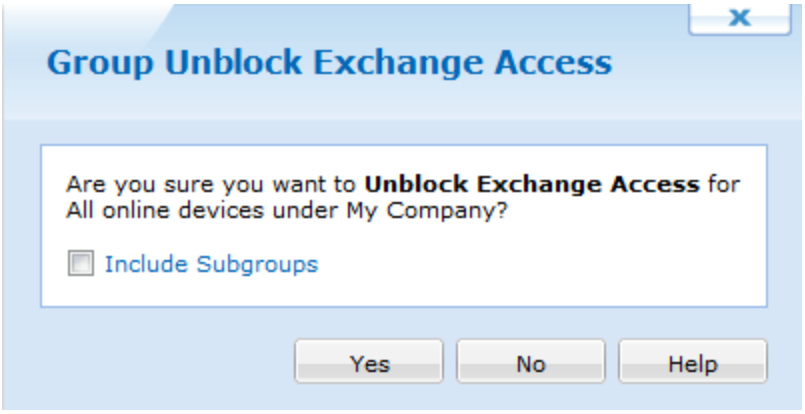
version="1.0" encoding="UTF-8"?> <configuration> <system.webServer> <rewrite> <rules> <rule name="ReverseProxyInboundRule1"> <match url="^(.*)" /> <serverVariables> <set name="HTTP_ ACCEPT_ENCODING" value="0" /> </serverVariables> <action type="Rewrite" url="https://owa.soti.net/ {R:1}" /> </rule> </rules> <outboundRules> <rule name="ReverseProxyOutboundRule1" preCondition="ResponseIsHtml1"> <match filterByTags="A, Form, Img" pattern="^http (s)?://owa.soti.net/(.*)" /> <action type="Rewrite" value="http{R:1}://owa.soti.net/{R:2}" /> </rule> <preConditions> <remove name="ResponseIsHtml1" /> <preCondition name="ResponseIsHtml1"> <add input="{RESPONSE_CONTENT_TYPE}" pattern="^text/html" /> </preCondition> </preConditions> </outboundRules> </rewrite> </system.webServer> </configuration>" on page 1) If the filter is not installed, a confirm message will appear.

If any certificates were provisioned by MobiControl to devices, we can revoke them when we block Exchange access.

No Filter installed



Blocking Exchange Access



Unblocking Exchange Access

Scan for virus now

When this is selected, MobiControl will scan the device for any virus's, rather than waiting for a schedule to scan.

Update virus definitions now

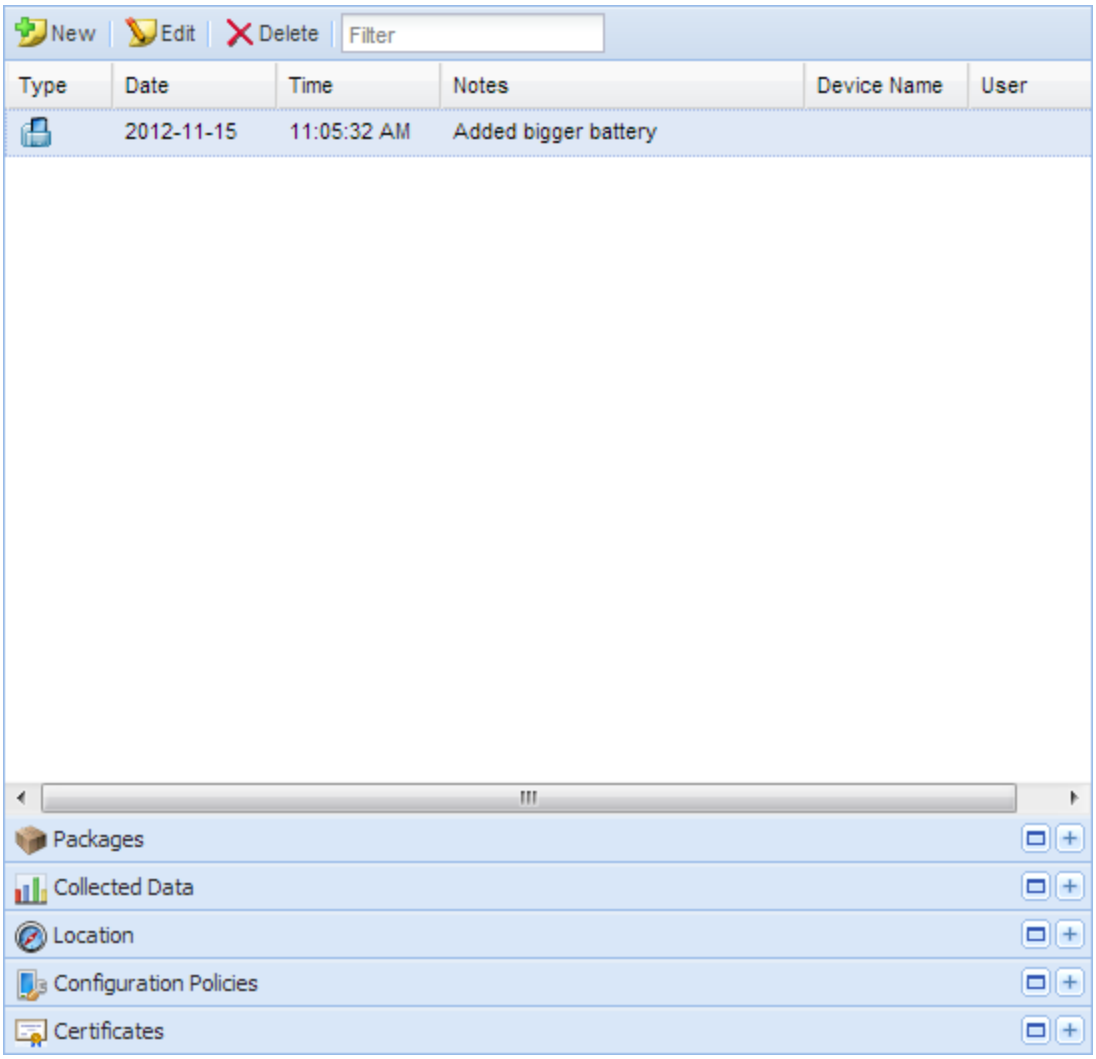
When selected, this will update the virus definition on devices.

Device Notes

The Device Notes feature allows you to create a note for a device and archive it for future reference and tracking purposes. Each note is editable and includes the date and time when the note was added or edited. The note includes the name of the user creating the note and can be assigned different colors for color-coded categorization.

This feature is useful for creating a "trouble ticket" for help desk tracking in an end-user support or CRM (Customer Relationship Management) environment. It also allows users with access to the MobiControl Web Console to document a device-specific issue and share their comments and memos related to that device with other users of the MobiControl Web console.

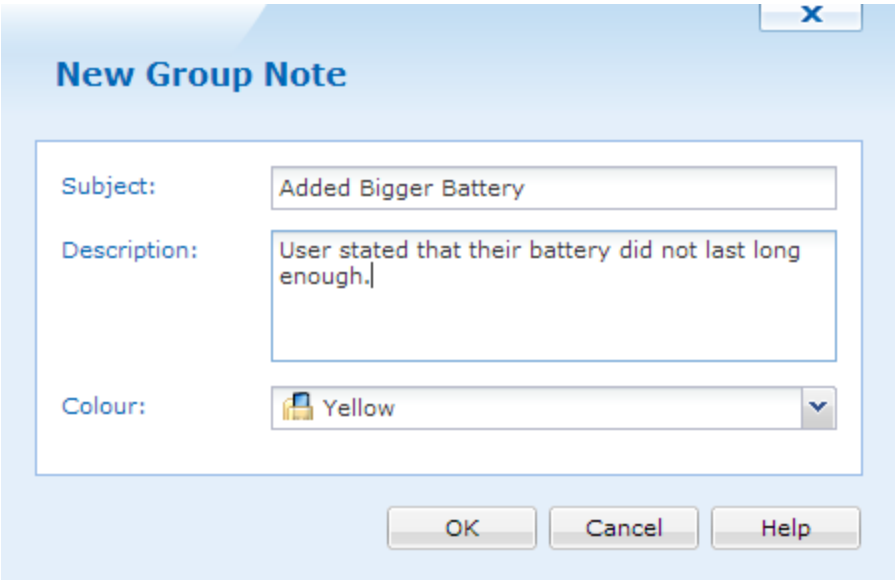
To view and edit notes for a device, select the Devices view (tab) in any of the All Devices, Windows Mobile, Windows Desktop, iOS, Android or Android Plus tab. Select a device and the notes for that device appear in the Notes panel.



Device Notes

Adding or Editing a Note

From within the Notes panel, click **New** to add a new note for the currently selected device or click **Edit** to make changes to an existing note.



Add Note dialog box

The following table describes the fields of the **Add Note** dialog box:

Field Name	Description
Subject	Text entered in the subject field appears in the Notes panel as the title of the note.
Icon	You can choose different colors for the icon to adopt a color-coding to indicate different priority levels or to distinguish between different departments or users creating the note. Notes can be sorted by icon color for a categorized view.
Description	The description field is available for viewing when the note is opened. This field can contain troubleshooting notes, administrative memos or any other device-specific information.

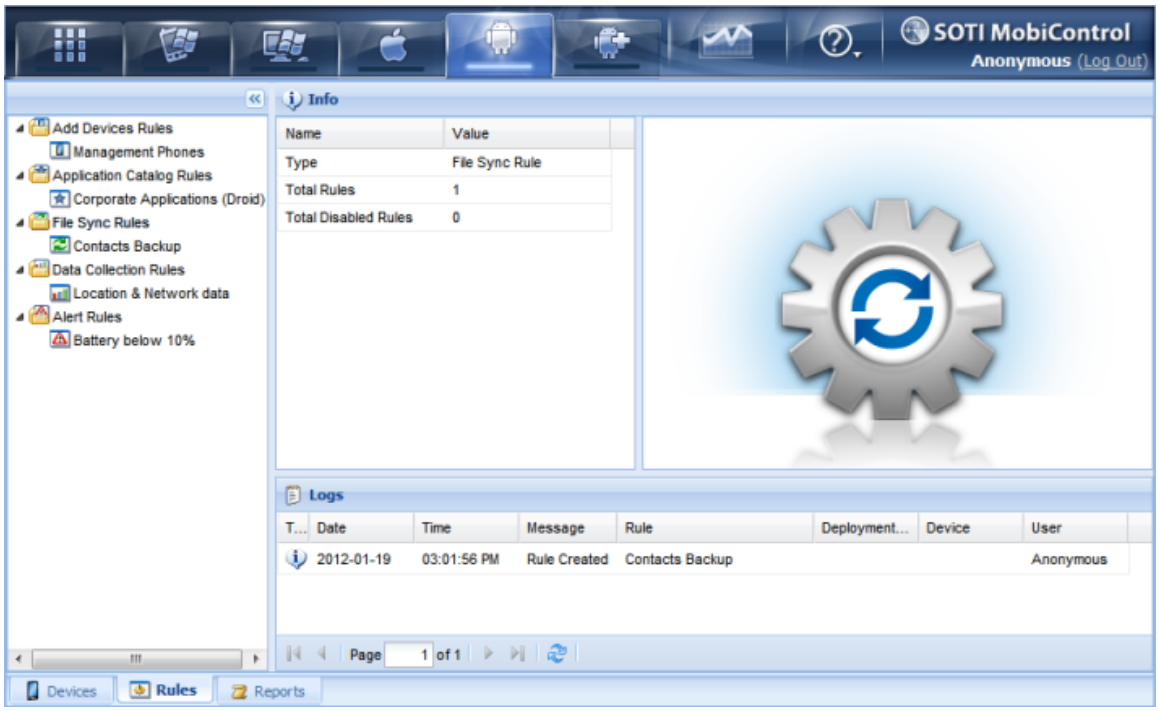
Device Group Notes

MobiControl now offers a way to place notes on a device group level. For example, if you are planning a roll out of devices across the country in phases based on location, you can add device group notes to state which phase each group is in. Therefore, when someone else logs into the MobiControl Web Console, they can see what part of the roll out each group should be in.

To create a device group level note, click a group on the left side of the MobiControl Web Console. After a group has been selected, expand the Notes panel on the right side, and click New.

Android Rules Tab

MobiControl uses rules to simplify the tasks of device management and configuration. See Below for a description of each rule.



Android Rules Tab

Add Devices

1. Create an add devices rule.

   An add devices rule allows you to configure the settings that MobiControl uses to set up and communicate with your devices. These settings include: the device group to which devices are added, how often the device is to check for updates, and the parameters to be used for remote control sessions. Please see the "Adding Android devices" topic on page 1216 for detailed information about creating an add devices rule.

Application Catalog

1. Create an Application Catalog Rule

   An Application Catalogue Rule allows Administrators to distribute proprietary, in-house applications to employees or members of the organization. Please see the "iOS Application Catalog" topic on page 1050 for detailed information about creating an Alert Rule.

2. Check the Application Catalog Rule Report.

   Once the Application Catalog Rule has been created, you may want to run a report to see what alerts have been generated. You can do this by looking at the Application Catalog Rule Report report in the Reports view (tab). Please see the "Report Types" topic on page 1110 for more detail about reports.

File Sync

1. Create a file sync rule.

   A file sync rule allows you to schedule file(s) to be synchronized between a set of devices and the Deployment Server. When creating a file sync rule, you will need to specify the file(s) you want synced (both their original location and their destination), the interval in between the syncs and which direction the sync should go in (either device to server, or server to device) and which devices should be involved in the sync. Please see the "Android File Sync" topic on page 1227 for detailed information about creating a file sync rule.

2. Check the rule execution status.

   Once the file sync rule has been created, you may want to confirm that the scheduled syncs occurred. You can do this by looking at the rule execution status or by checking the rule execution report in the Reports view (tab). Please see the "Generate Reports" topic on page 390 for more detail about reports.

Data Collection

1. Create a data collection rule.

   A data collection rule allows you to set up rules to collect data from your mobile devices automatically. Please see the "Creating Data Collection Rules" topic on page 318 for detailed information about creating a data collection rule.

2. Check the data collection rule execution status.

   Once the data collection rule has been created, you may want to confirm its execution. You can do this by looking at the rule execution status or by checking the rule execution report in the Reports view (tab). Please see the "Generate Reports" topic on page 390 for more detail about reports.

Alert

1. Create an Alert Rule

   An Alert Rule allows Administrators and Users to be notified when events of interest arise on the system. Please see the "Windows Mobile Alerts" topic on page 575 for detailed information about creating an Alert Rule.

2. Check the Alert Rule execution status.

   Once the Alert Rule has been created, you may want to run a report to see what alerts have been generated. You can do this by looking at the Alert Rule Summary report in the Reports view (tab). Please see the "Generate Reports" topic on page 623 for more detail about reports.

Telecom Expense

1. Create an Telecom Expense Rule

   A Telecom Expense Rule allows Administrators and Users to be notified on current usage of company data and voice minutes. Please see the "Android Telecom Expense Management" topic on page 1257 for more information.

2. Check the Telecom Expense Rule execution status.

   Once the Alert Rule has been created, you may want to run a report to see what alerts have been generated. You can do this by looking at the Telecom Expense Rule Summary report in the Reports view (tab). Please see the "Generate Reports" topic on page 623 for more details about reports.

Adding Android Devices

To Add Google Android Devices you need to create an 'Add Devices Rule' and then download the installation files to the mobile device. Alternately, you may Publish your **Add Devices Rule** to the Enrollment Service and provide the Enrollment ID to the mobile user.

Add devices rules allow MobiControl to name devices, place devices in the appropriate device group, and to generate a customized Enrollment ID that, when enrolled by the user, allows MobiControl to manage the devices.

To create an add devices rule, select the Google Android Tab within MobiControl Web Console, then select the **Rules** Tab. Right-Click the **Add Devices Rules** folder and select **Create Add Devices Rules**.

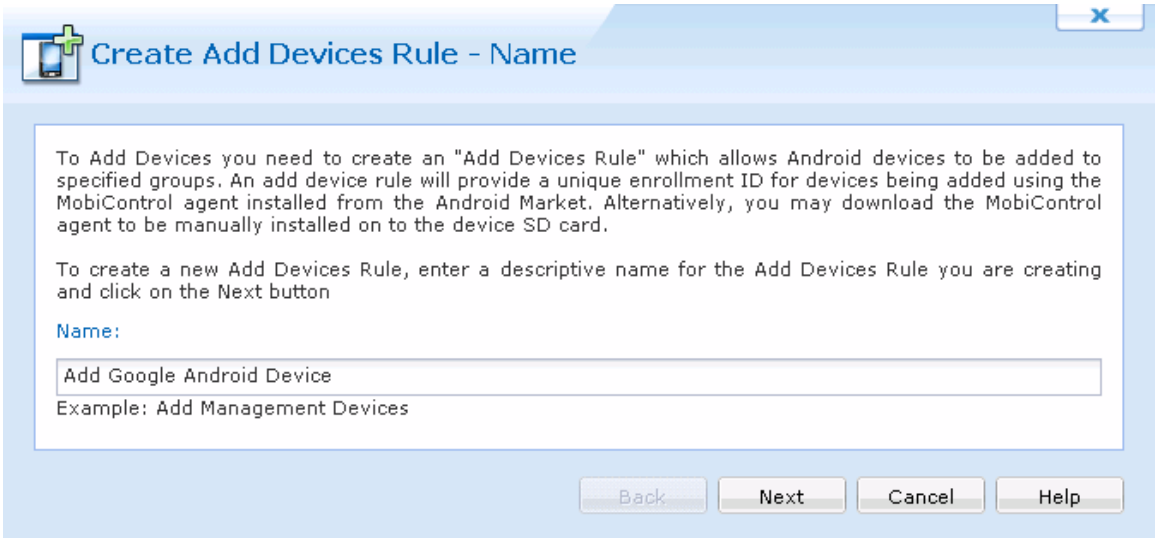
Google Android Tab

The six steps below describe how the Create Add Devices Rule Wizard can be used to create an add devices rule:

1. Start the wizard.

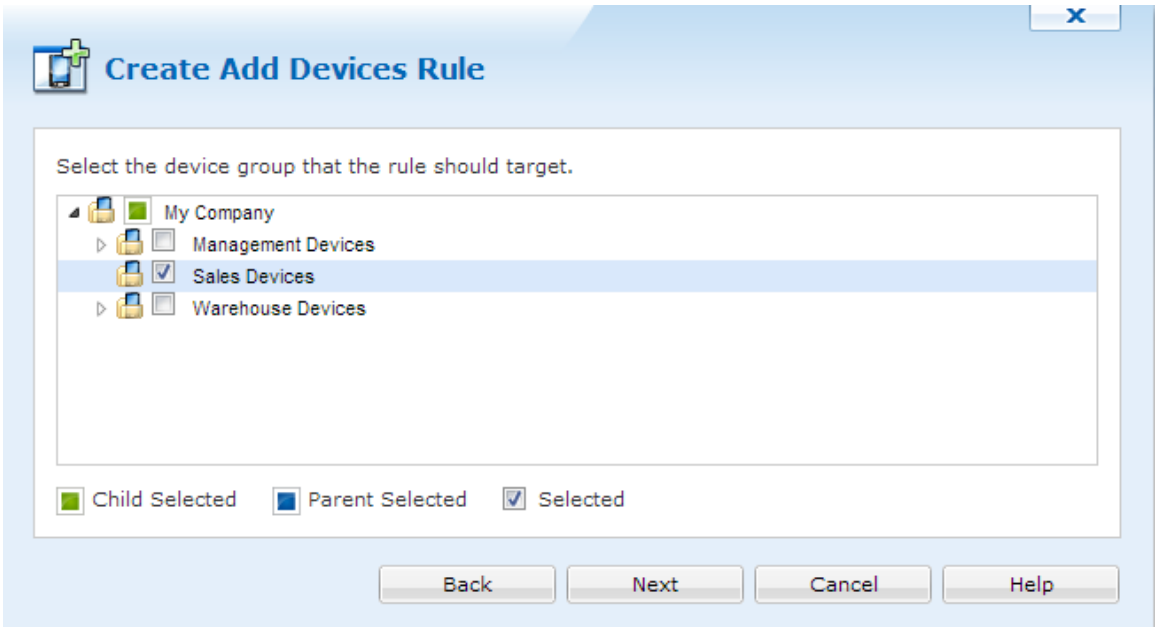
   Select the **Rules** Tab, from the **Google Android** Tab, then Right-Click the **Add Devices Rules** folder and select **Create Add Devices Rules**. The first page of the Create Add Devices Rule Wizard will be displayed.

   Enter a descriptive name for the add devices rule you are creating and click **Next.**



First page of the Create Add Devices Rule Wizard

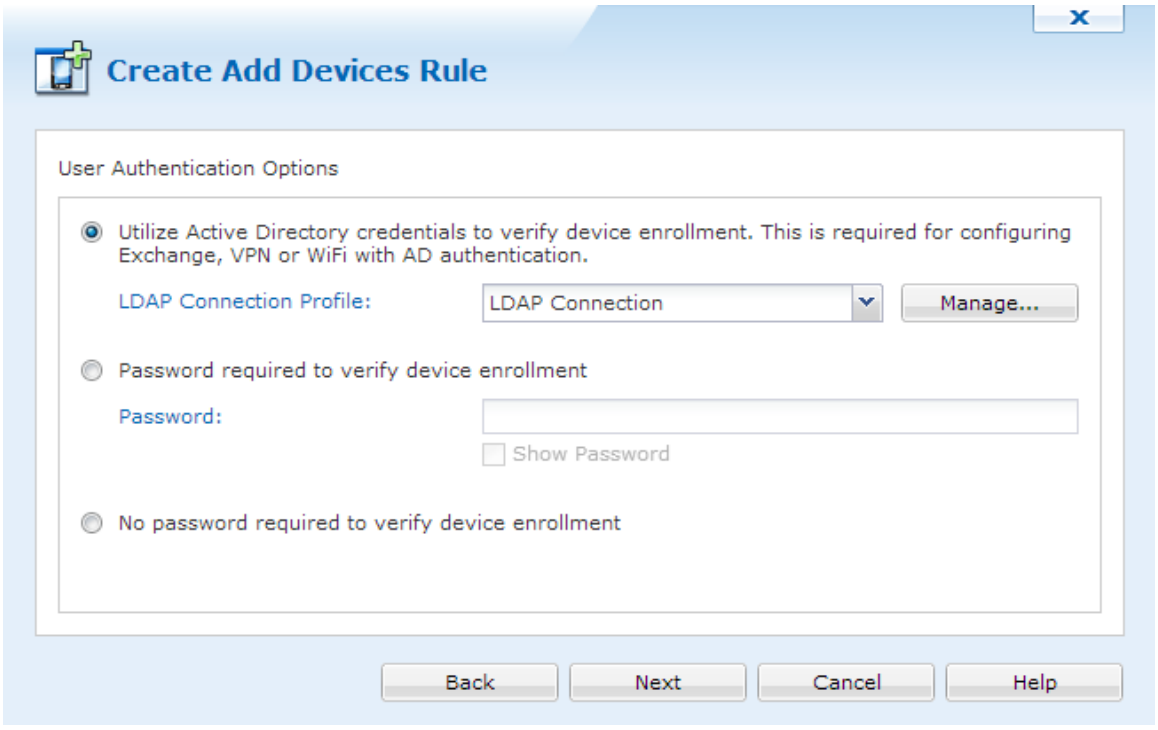
2. Configure the device group.



Device Group Selection page

First, select to which device group the devices configured by this rule will be added. The dialog box below displays the current device tree. Select the group where devices need to be inserted and then click **Next.** After selecting a device group click on the **Next** button.

3. Configure authentication options.



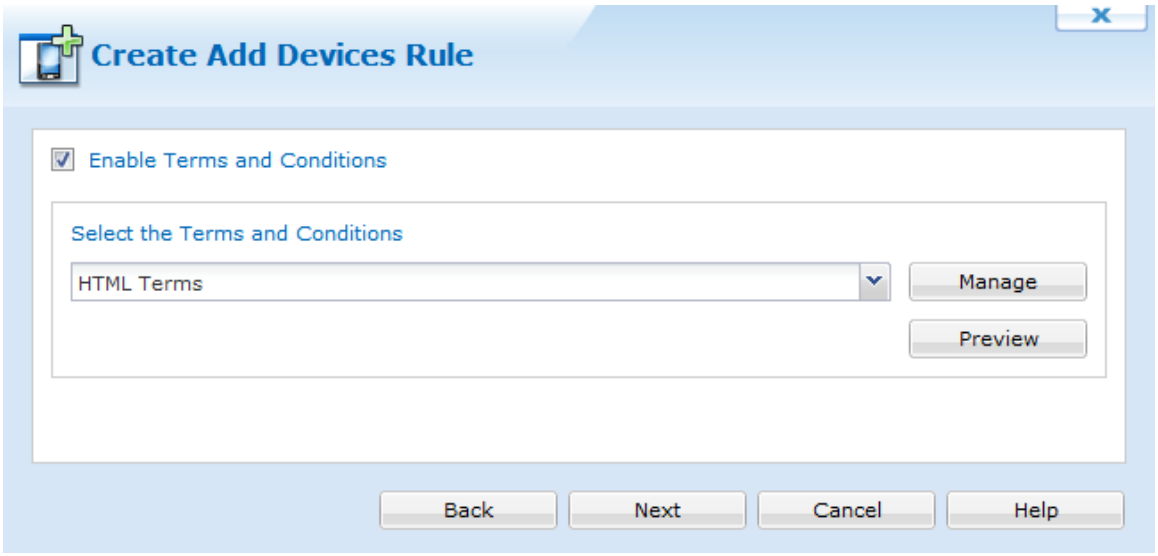
User Enrollment Authentication

Select a user authentication method for enrolling devices. A password may be set to ensure unwanted devices are unable to enroll in your network.

If Utilize Active Directory credentials is selected, choose the connection type from the drop down menu. If there is no connections, click Manage to create a new connection. Please see the "LDAP Connections Manager" topic on page 616 for more information regarding LDAP connections.

4. Terms and Conditions

The terms and conditions page allows us to send terms and conditions to devices. Users must accept these terms before they are able to enroll their device to MobiControl. If they do not accept the terms and conditions, the device will not connect. If Terms and Conditions is required, click "Enable Terms and Conditions".



Terms and conditions

To add new Terms and Conditions to the Add Devices rule, click Manage. Once clicked, we can see the Terms and Condition Manager. Please see the "Terms and Conditions" topic on page 619 for more information.

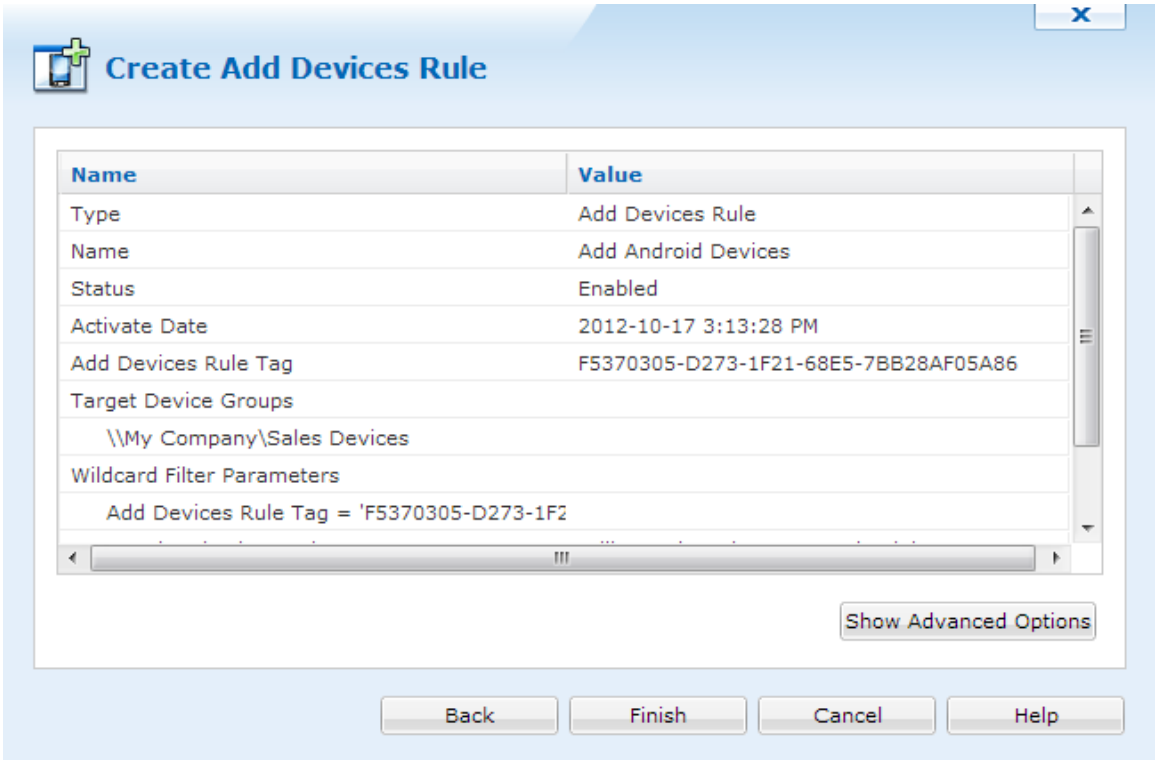
After selecting the Terms and Conditions, click **Next** to continue the creation of the rule.

5. Review summarized information.

The **Rule Summary Information** page summarizes the settings configured on the previous pages of the wizard.

If you are satisfied with the configured settings, click on the **Finish** button to create the device rule, otherwise use the **Back** button to go to previous screens and make adjustments.

Selecting the "Publish To Enrollment Service" option allows all of your Add devices rule options to be saved in the cloud and accessed by devices via an Enrollment ID. The Enrollment ID contains the information used for the Device Agent to get back to your company's Deployment Server. The Enrollment ID is entered in the Device Agent. The Device Agent is available from Google Play by searching for MobiControl

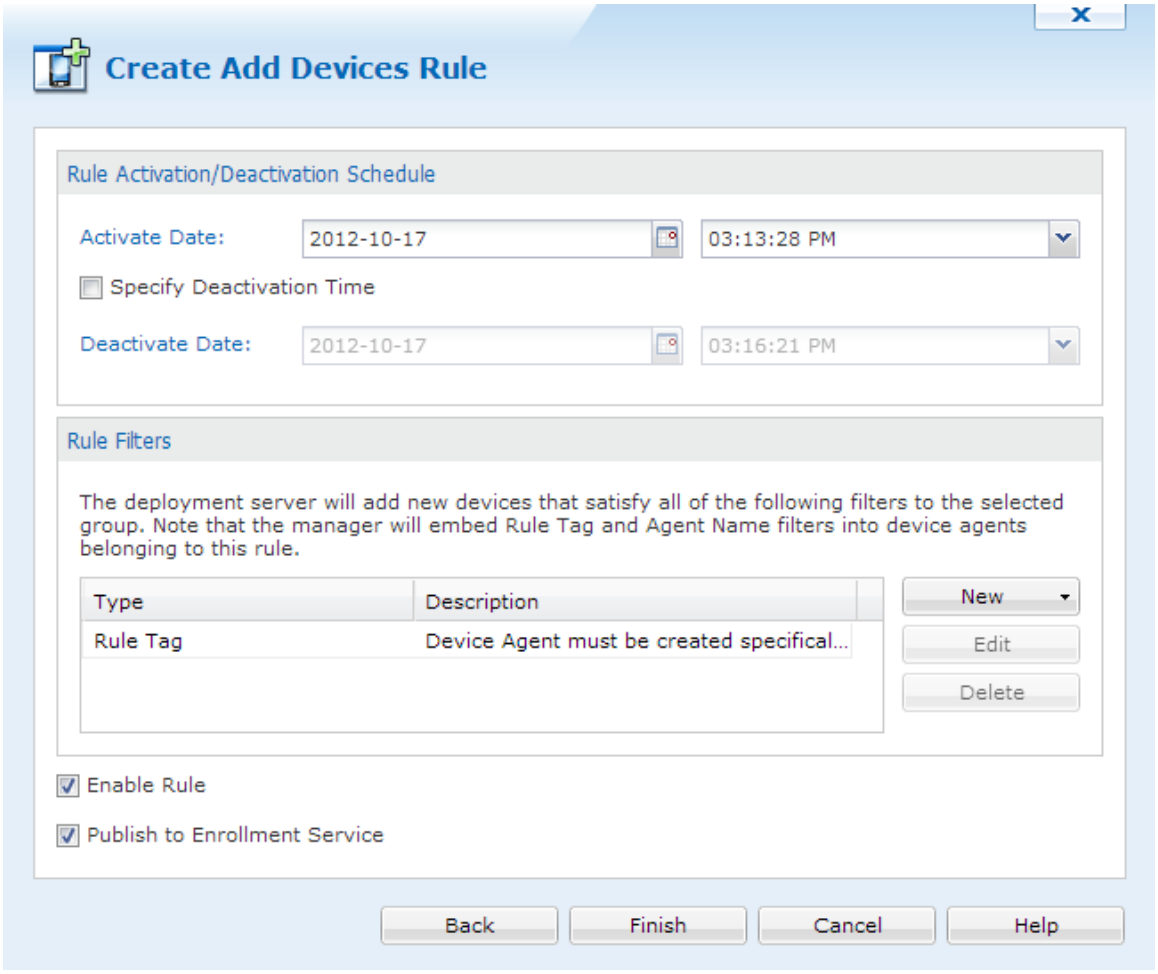


Rule Summary Page

6. Advanced Settings.

   The **Advanced Settings** button allows you to specify which devices are to be configured by this rule. By default, MobiControl will use this rule to configure only those devices that are running a Device Agent created specifically for this device rule. By using advanced settings filters, you can broaden or further restrict which devices get configured by this rule when they connect to MobiControl.

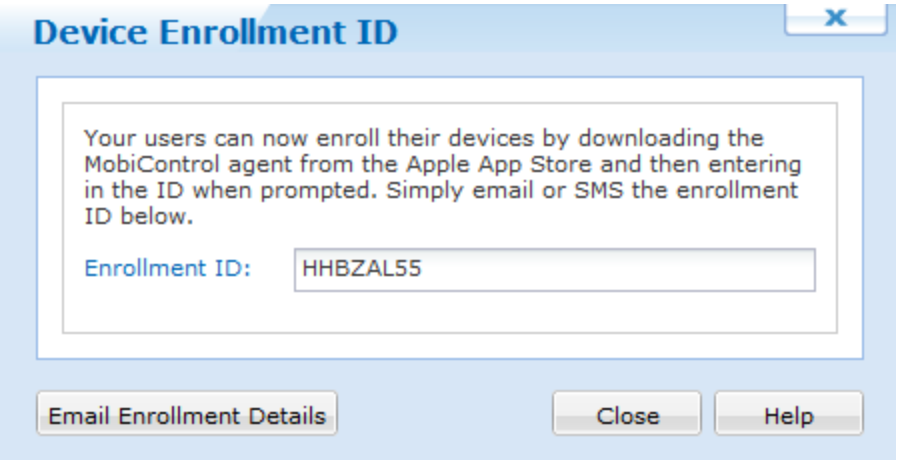
   Once you have made the changes, click **Next.**



Advanced Settings Page

6. Enrollment ID

If you download the MobiControl Device Agent from Google Play, then you should enter the ID that is shown in the Device Enrollment ID window. This allows the Device Agent to configure what server your device should connect to.

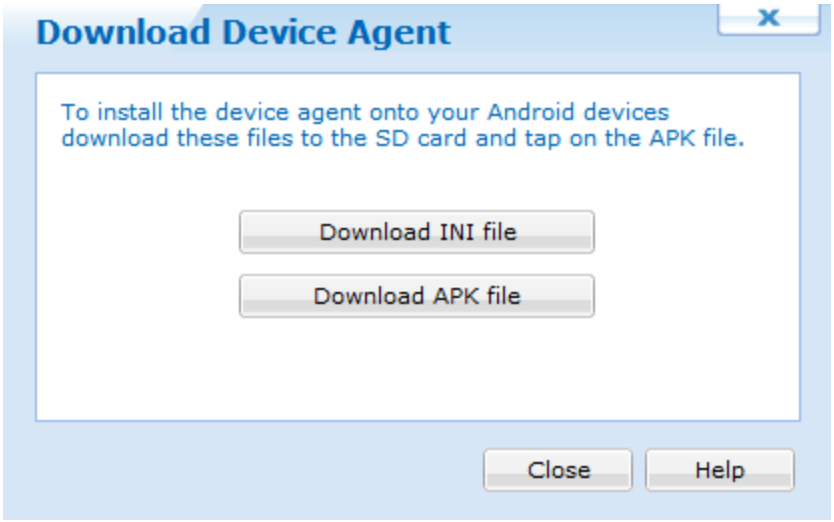


Device Enrollment ID

7. Download the MobiControl Android files

   You can download and place the Google Android Installation Files onto the Root of the SD Card and install the APK from there. If the INI file is included, then no enrollment ID is needed to be entered on the first start-up of the MobiControl Device Agent.

   From the mobile device (using a file browser), locate the MobiControl APK file and tap it to install. For more information on how to install this APK file, please click here.



Device Agent Installation Files page

Android Application Catalog

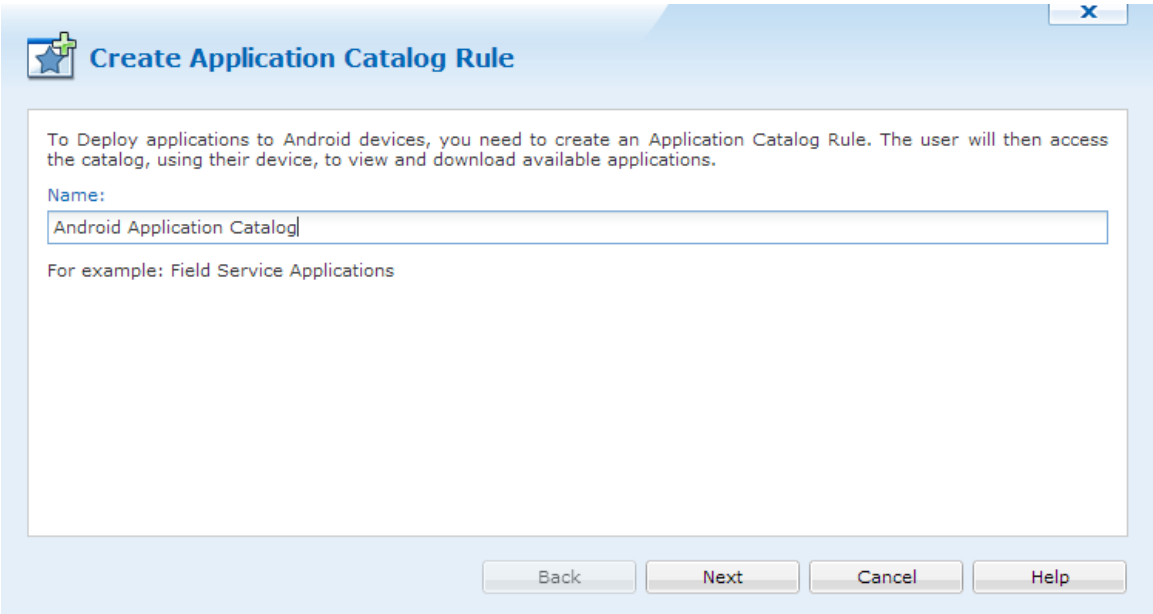
The Application Catalog allows us to let users know what approved apps they are able to download on their device. We can configure Play Store applications to appear, set it to be mandatory so that users must download it, or set it as optional. We can also upload enterprise built applications without posting

them into the Play Store.
If an application is set to mandatory, the user will constantly be prompted to download it.

To create an Application Catalog, we must first create it's rule. To do this, go to the Android rule tab. Right click Application Catalog then click **Create Application Catalog Rule**.

Naming the Rule

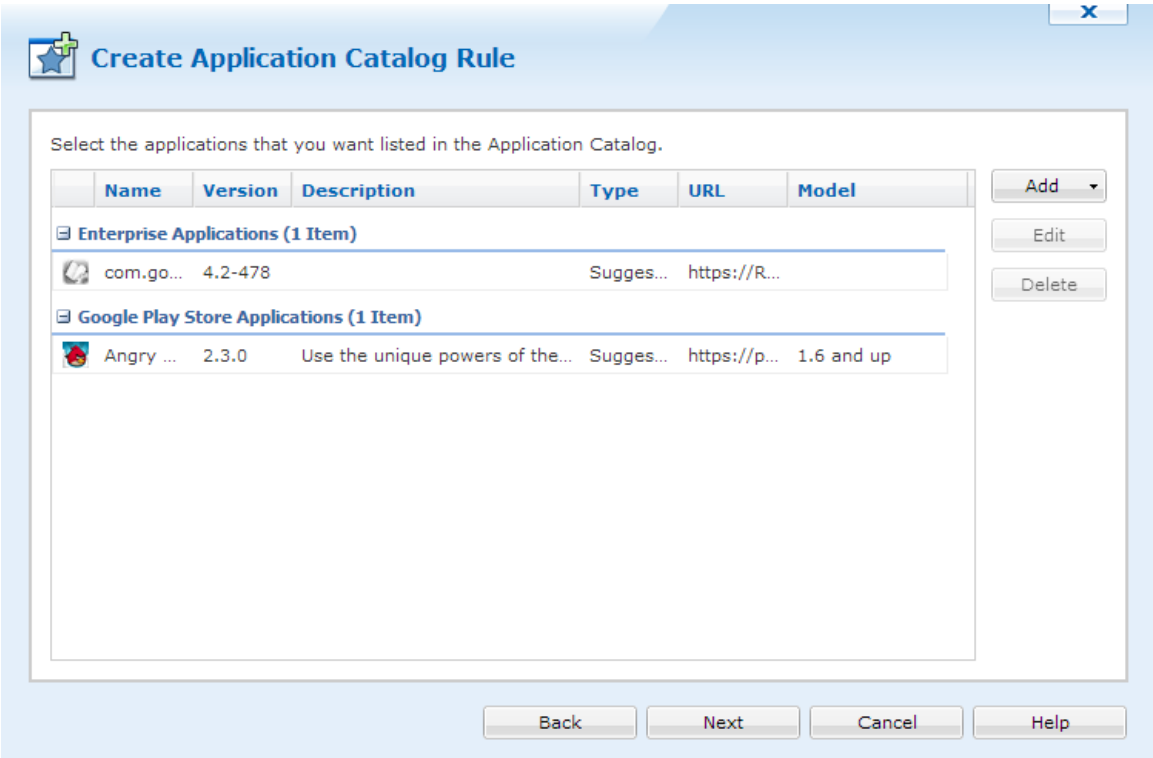
When the Application Catalog wizard appears, enter a name then click Next



Name the Application Catalog

Application Selection

The next panel will allow us to add App Store or Enterprise Apps.



Adding Applications

Click Add and select either Enterprise Applications or App Store Applications.

Clicking each header below will reveal more information about each topic:

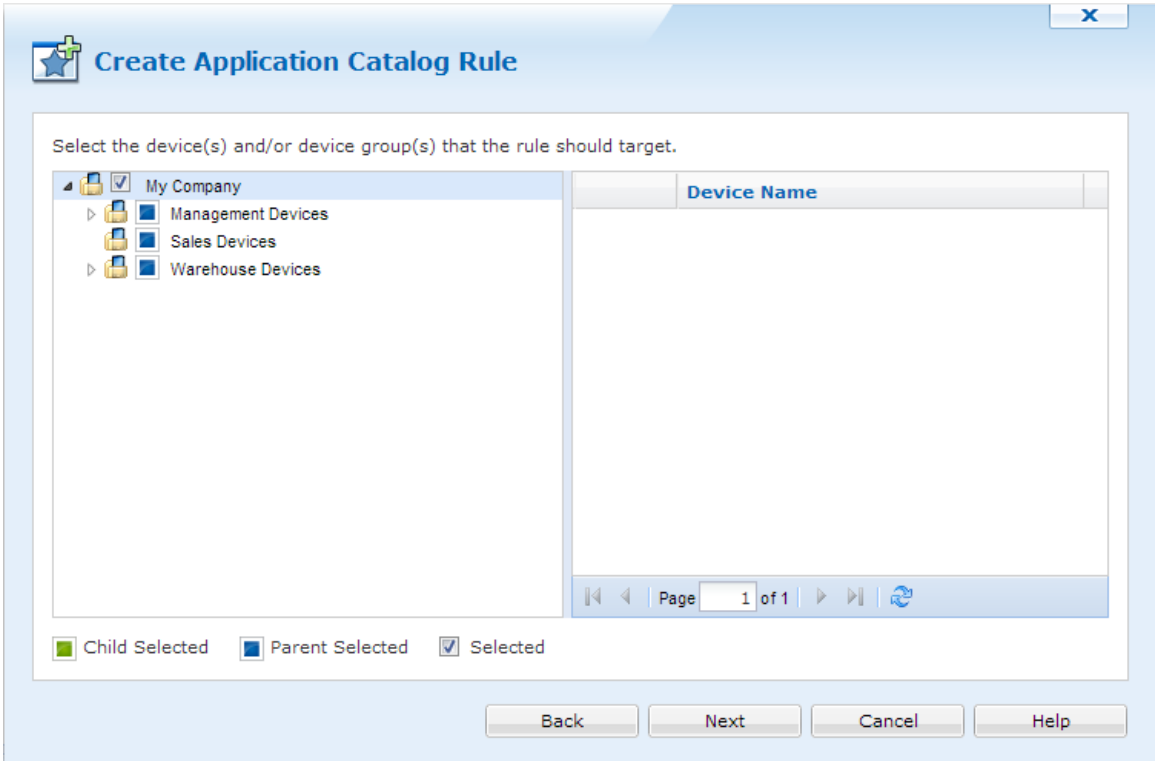
Enterprise Applications

Play Store Applications

After all desired apps are added, click Next.

Select Devices and Groups

The next panel will let us choose which groups and/or devices will receive this Application Catalog.

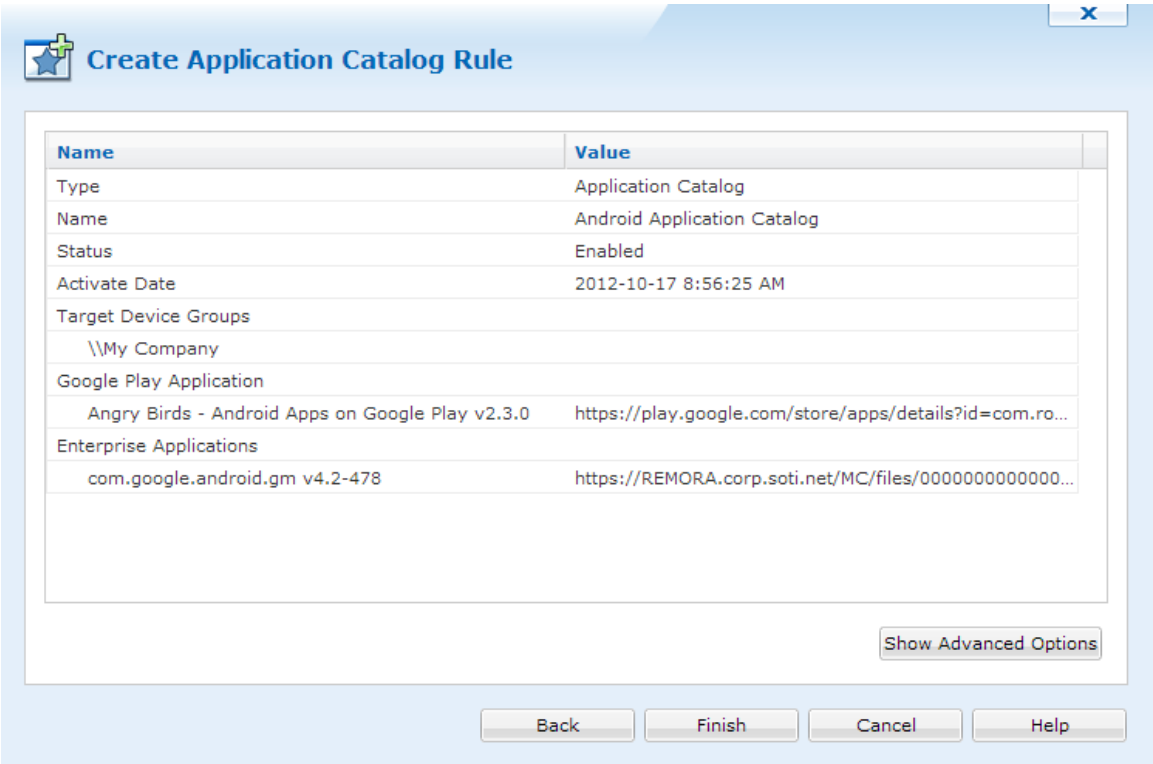


Target Groups or Devices

When devices are selected, click Next.

Summary

The last panel will show us a summary of the Application Catalog.



Application Catalog Summary

Clicking **Show Advanced Options** will allow us to configure more settings for the Application Catalog. Some of these settings include changing the Application Catalog banner.

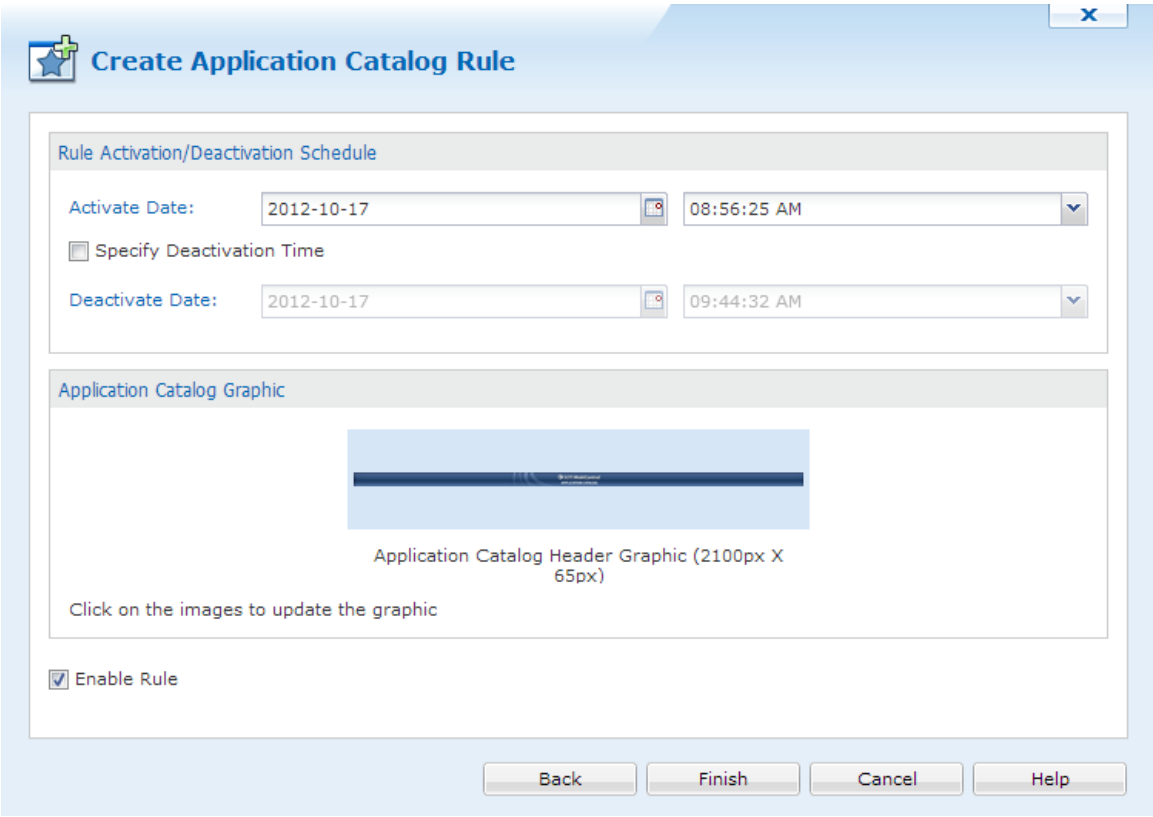
Advanced Options

Here we are able to set when this rule will be activated and deactivated, and change the Application Catalog graphics.

The Application Catalog icon is what would appear on the home screen, while the Application Catalog Header is what appears in the actual catalog. Clicking each image will allow us to upload new images.

NOTE:

The Application Catalog Header can be 2100px X 65px.



Application Catalog Advanced Options

After everything is configured, click Finish to save and close the wizard.

Android Creating File Sync Rules

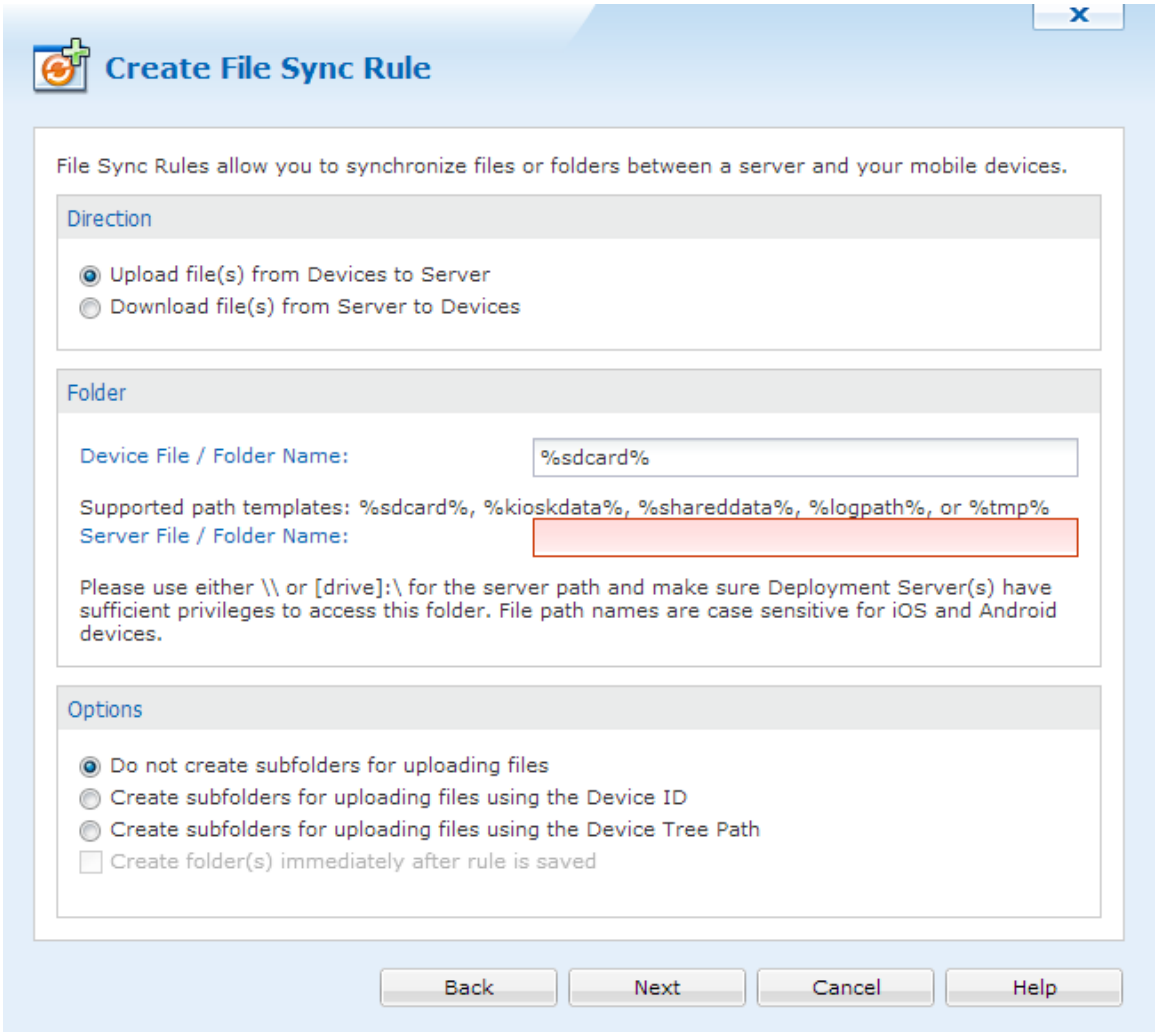
File sync rules allow you to synchronize files and folders between your devices and a server. File collection, also referred to as file uploading, is a very convenient method for gathering information from devices, for example a transaction log file. File dissemination, also referred to as file downloading, is a quick and easy way to send one or more files to a set of devices such as an updated product listing or configuration file.

1. Start the wizard.

   Select the Rules view (tab), then click **Rule,** point to **Create Rule,** and click **File Sync Rule.** Enter a meaningful name for the rule.

First page of the Create File Sync Rule Wizard

2. Configure file synchronization source and destination.



Configure file sync source and destination

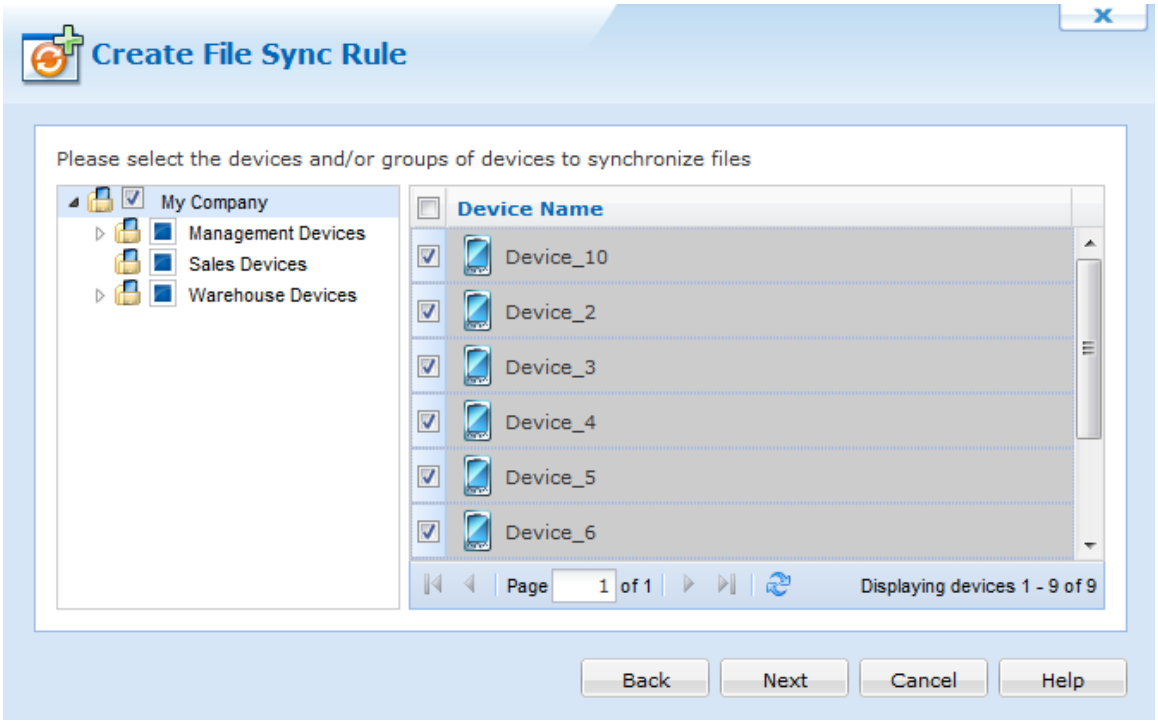
The following table describes the fields of this page of the wizard:

Field Name	Description
Direction	• **Upload** (File collection) The rule will be used to upload files from the devices to a server. • **Download** (File dissemination) The rule will be used to download files from the server to devices.
Device File/Folder	Specifies the complete file system path to the files or folders being synchronized on the device. "%sdcard%" is a global variable that is used to specify the devices external storage.

Field Name	Description
Server File/Folder	Specifies the complete file system path to the files or folders being synchronized on the server It is strongly recommended that a UNC (Universal Naming Convention) path be used. A local path (i.e. `C:\MyFiles`) can be used if only one Deployment Server is being used and the local path is on the computer running the Deployment Server. **NOTE:** It is important that the Deployment Servers have sufficient permission to read and write to the source or destination UNC path. Best practice is to run the Deployment Server under its own Active Directory user profile.
Server-side Folder Options	For **upload rules,** files collected from the devices can be written to: • A single shared folder, meaning files could potentially be overwritten if they have the same name. • A per-device subfolder, named using the device ID (i.e {00135304-41D7-019E-5800-0050BF3F5173}) • A per-device subfolder, named using the device tree path (i.e. `.\Management Devices\Device 0001`) For **download rules,** files disseminated from the server can be read from: • A single shared folder, meaning all devices get the same file (s). • A per-device subfolder, named using the device ID (i.e. {00135304-41D7-019E-5800-0050BF3F5173}) • A per-device subfolder, named using the device tree path (i.e. `.\Management Devices\Device 0001`)
Create folder(s) immediately after rule is saved	When the **Create folder(s) immediately after rule is saved** option is enabled, the server-side folders will be created immediately after the file sync rule is saved. This allows adding files to the folders on the servers that are synchronized with the devices when the file sync event occurs.

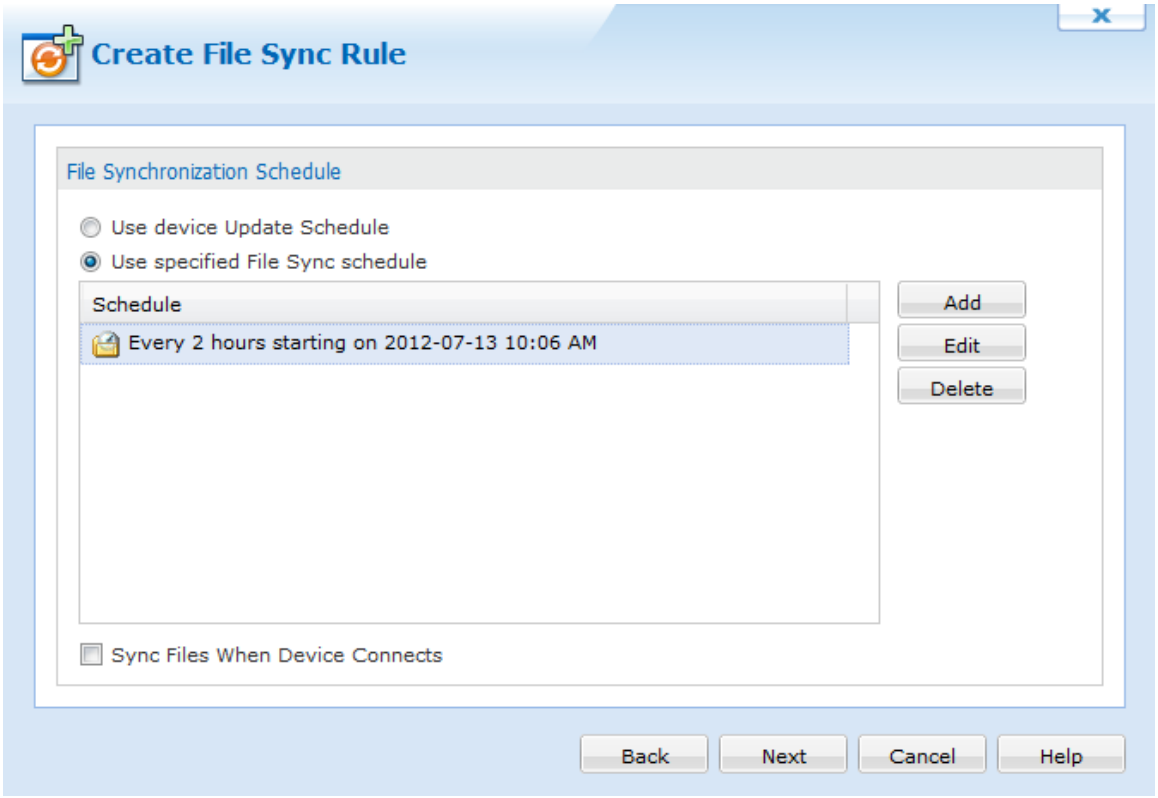
3. Select devices.

   Select the device(s) and group(s) for which the file sync rule will apply.



Device Group selection page

4. Specify the synchronization

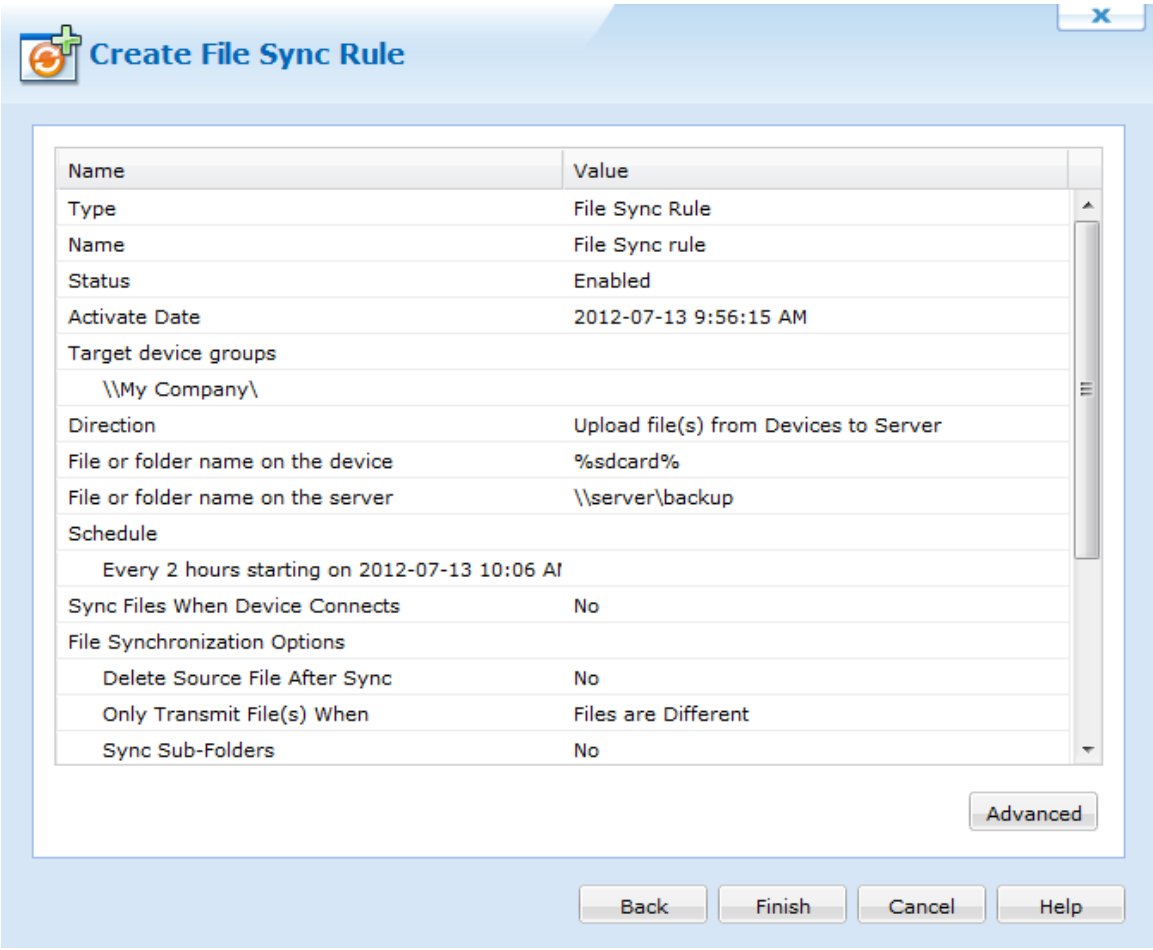


Rule activation schedule

Field Name	Description
Use Device Update Schedule	By default, the device update schedule (specified by the file sync rule used to add the devices to the system) triggers file synchronization
Use Specified File Sync Schedule	If you specify a file synchronization schedule in this dialog box, only that schedule will be used, and the device synchronization schedule will not trigger file synchronization. To Specify the custom schedule click the **Add** button. Please see the "File Synchronization Schedule" topic on page 1238 for more information about creating a custom file sync schedule.

5. Review summarized information

Review information on the **file sync rule summary page**. This page gives you an opportunity to review the settings of the file sync rule before committing them. If you wish to make any corrections, click the **Back** button. Clicking the Advanced button allows additional File sync rule configuration.

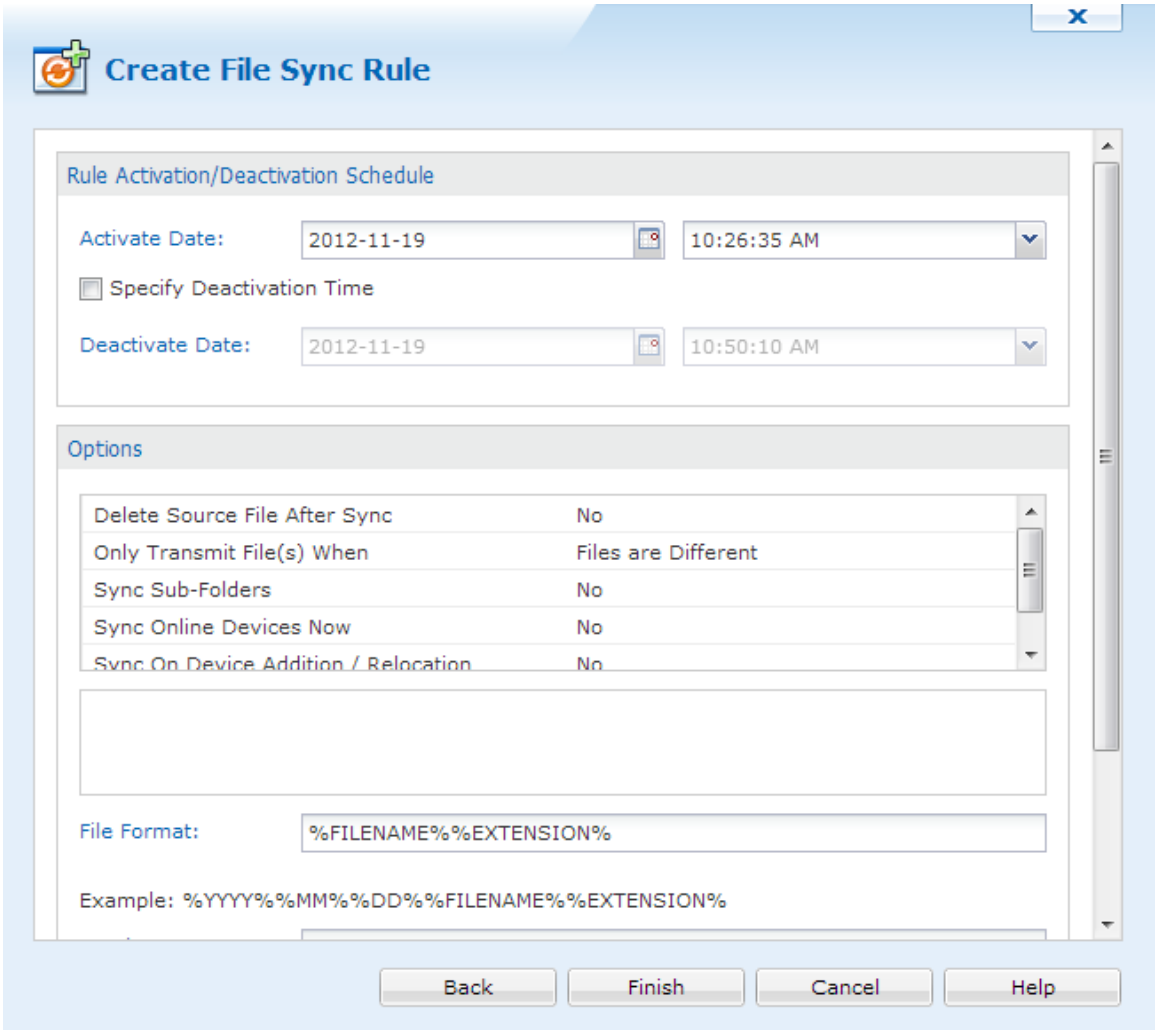


Summary page

6. Advanced options

The following table describes the file synchronization options on this page of the Create File Sync Rule Wizard. By default, the file sync rule will be activated immediately upon completion of the wizard. If you wish to delay the activation you can modify the activate date. A deactivate date can

optionally be entered to specify a date from which the rule will be disabled.



File synchronization options

Field Name	Description
Delete Source File After Sync	(This applies only to upload rules.) When selected, the source file(s) on the device are transmitted to the server and then deleted from the device.

Field Name	Description
Only Transmit File (s) when	• The **Always Transmit** option will cause file(s) to be uploaded or downloaded regardless of whether or not the source and target are different or the same. • The **Files are different** option will cause file(s) to be uploaded or downloaded only if the source file is different from the destination file. • The **Source file is newer** option will cause file(s) to be uploaded or downloaded only if the source file has a more recent date-time stamp. • The **Destination file does not exist** option will cause file(s) will cause file (s) to be uploaded or downloaded only if the destination file does not exist.
Sync Sub-Folders	Synchronize files in sub-folders in addition to the files located in the target folder
Sync Online Devices Now	File synchronization will be executed immediately following the completion of the wizard for online devices.
Sync On Device Addition or Relocation	Perform file synchronization when a device is added or relocated to a device tree group for which this rule has been configured This setting is useful to easily invoke file synchronization when a device is moved from one group to another in the device tree.
Network Restriction	Restrict whether file synchronization should take place over cellular data networks (i.e. GPRS)

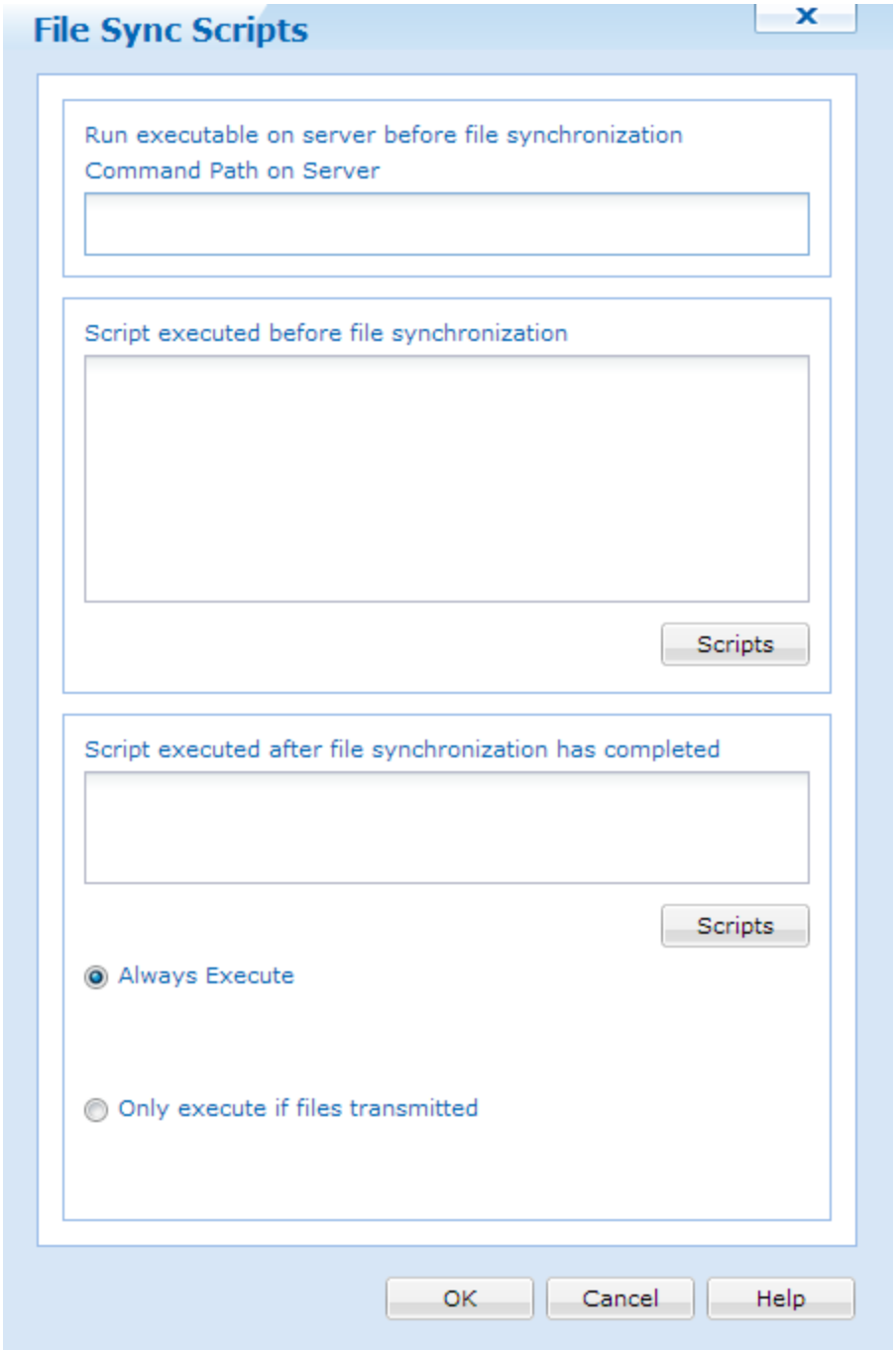
Click the **Scripts** button to configure file synchronization scripts.

File Synchronization Scripts

File synchronization scripts provide flexibility in automating actions on the server before the file sync or on the device pre or post file synchronization.

EXAMPLE: RUN EXECUTABLE ON SERVER

MobiControl contains plenty of server side utilities used to manage devices in the deployment server. One of these utilities is a device move. If this utility is ran before the file sync, we can ensure that all the devices are in the proper location before syncing the files down. For additional help with this utility and more, please contact us.



File synchronization advanced options

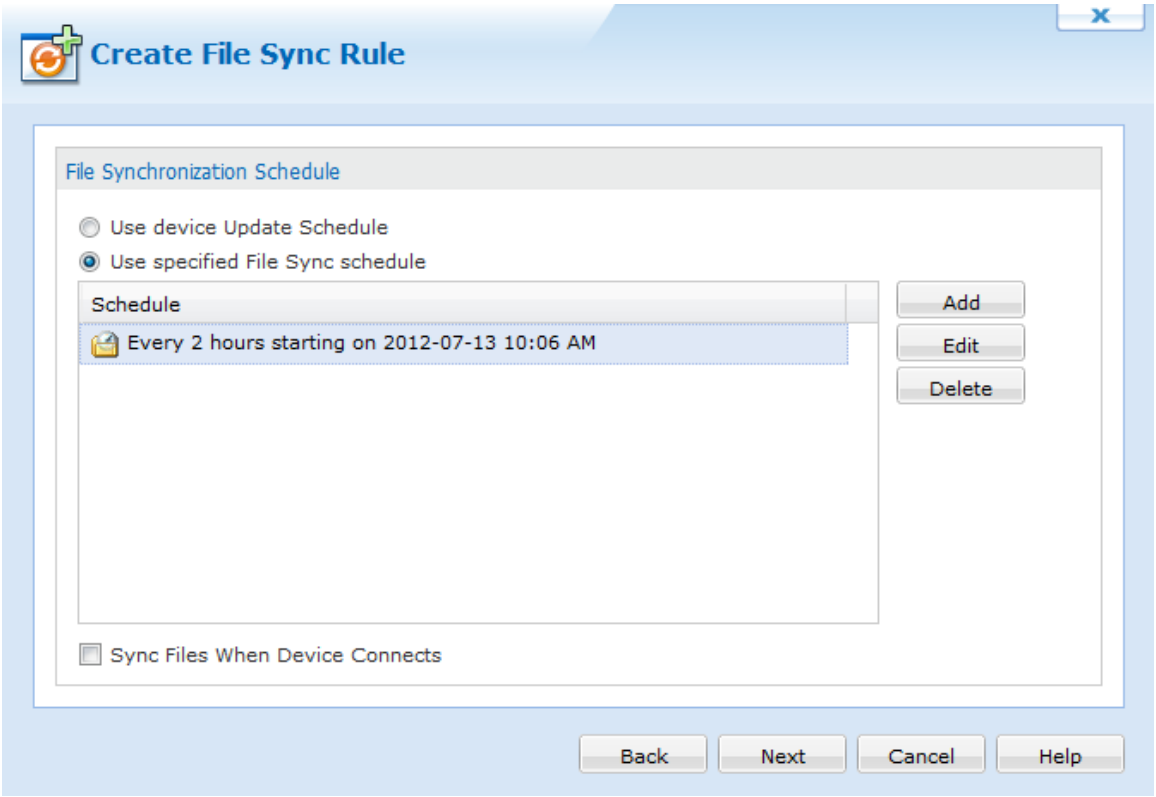
Field Name	Description
Always execute	Will execute the script every time there is a scheduled sync, even if the files are updated or not
Only execute if files transmitted	Will execute the script when files have been updated by the sync schedule
Scripts	Will allow you to import previously created scripts

Android File Synchronization Schedules

The file synchronization schedule specifies when the Deployment Server(s) should check device(s) for synchronization.

If the Deployment Server identifies an inconsistency, such as a mismatch in the file size or finds the new file, the Deployment Server will act according to the file sync rule.

By default, the device synchronization schedule, specified by the add devices rule used to add the devices to the system, is selected for file synchronization. You may add, edit or delete the custom schedule using the following dialog box.



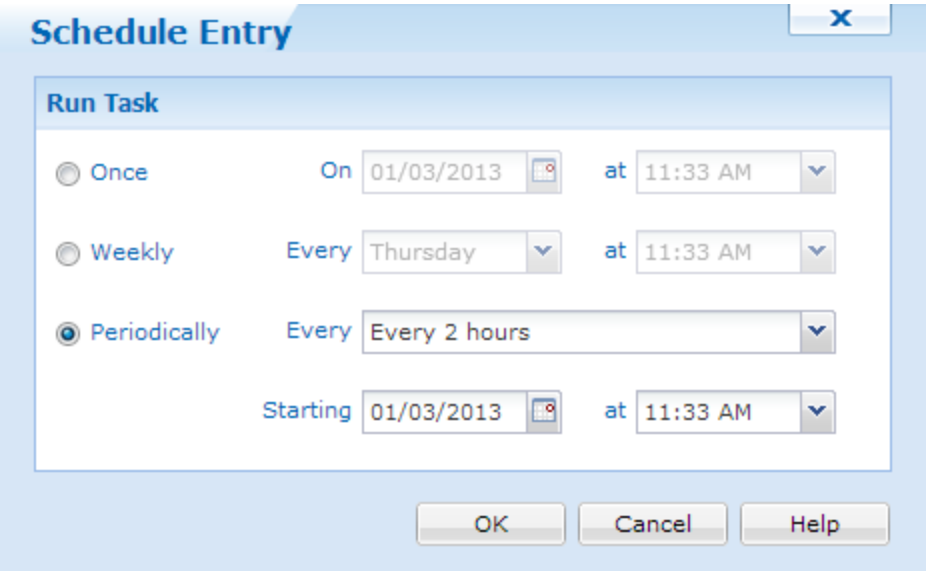
Create File Sync Rule Wizard dialog box

The following table describes the fields of the Create File Sync Rule Wizard dialog box.

Field Name	Description
Add	Specify your own file synchronization intervals. When you select **Add,** the **Schedule Entry** dialog box is displayed. **EXAMPLE:** To sync twice a week (Monday at 06:00 and Friday at 19:00), create two weekly schedule entries.
Edit	Select **Edit** to modify an existing schedule entry. The **Schedule Entry** dialog box is will be displayed.
Delete	Permanently remove a file sync schedule entry from the dialog box
Sync Files when device connects	Sync whenever devices under this rule connect to a Deployment Server (i.e. transition from offline to online)

Schedule Entry

The **Schedule Entry** dialog box allows you to specify schedule entries as one-time or periodic events.



Schedule Entry dialog box

Field Name	Description
Once	Device will check for file synchronization once at the specified date and time.
Weekly	Device will check for file synchronization once a week, on a specified day and time.
Periodically	Device will check for file synchronization periodically at the specified interval from the set, start date-time.

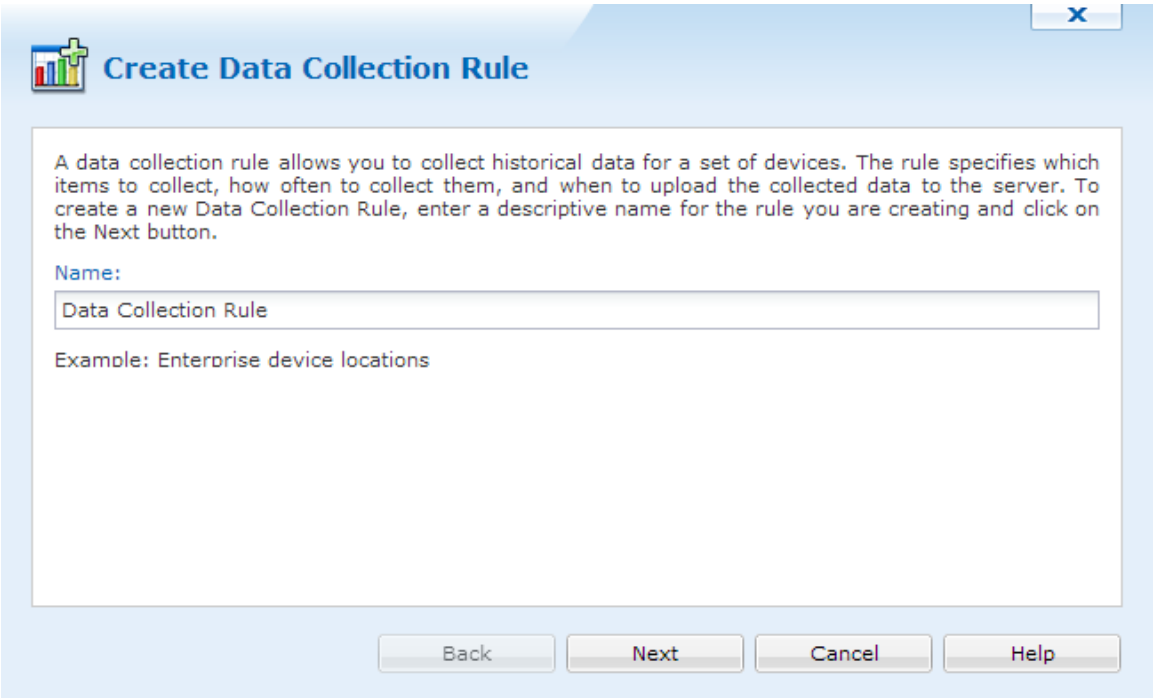
Android Data Collection Rules

Data collection rules allow administrators to automatically collect a variety of data from mobile device(s).

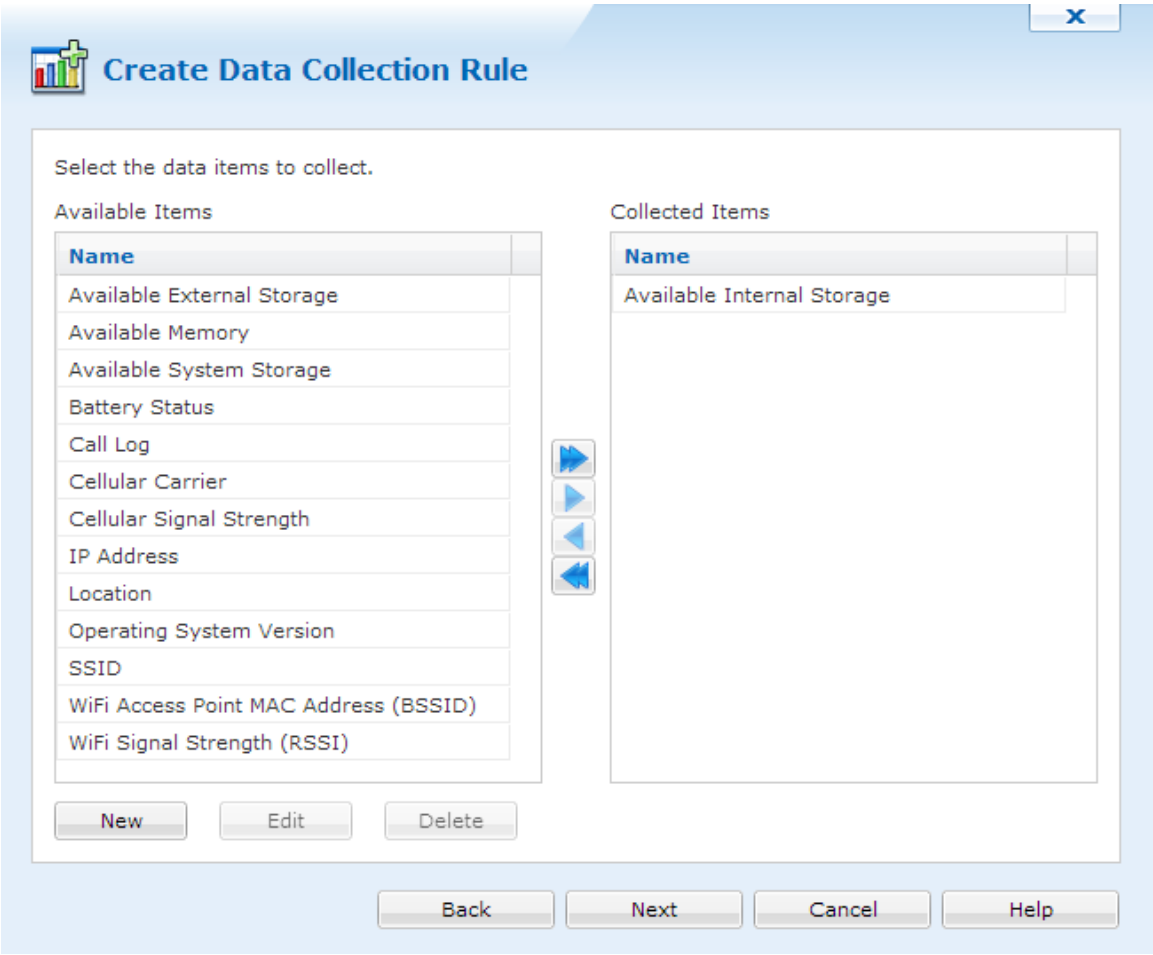
The following series of steps describes how to use the Create Data Collection Rule Wizard to create a data collection rule:

1. Start the wizard.

   From MobiControl Manager, select the Rules view (tab), then click **Rule,** click **Create Rule,** and click **Data Collection Rule**. Enter a meaningful name for your new data collection rule and then click **Next**.



2. Select data items to collect.



Select individual items or all items from the **Available Items** list by highlighting and then select the corresponding direction arrow(s). These items will move to the **Collected Items** list. If you have added something that you would like to remove from the **Collected Items** list, simply select the

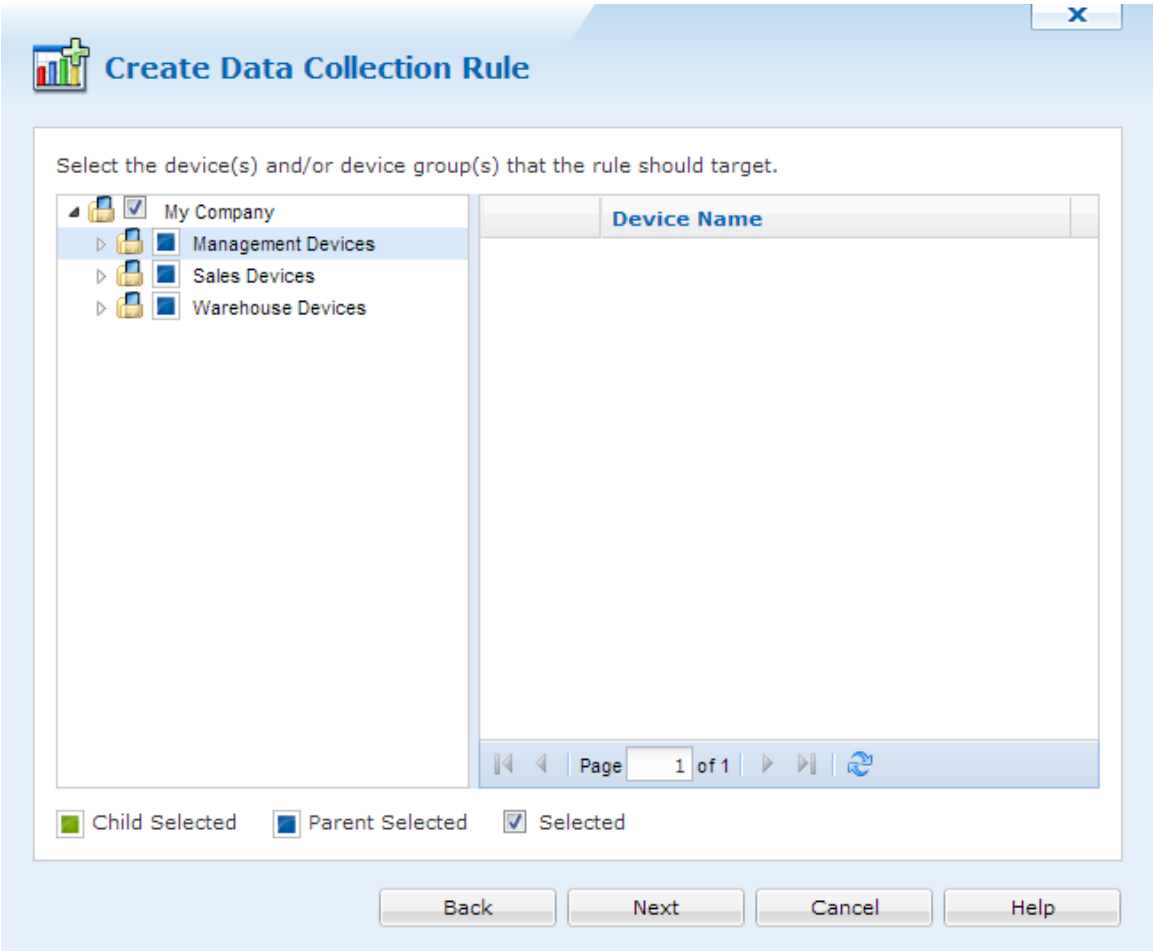
item and then click the direction arrow(s) to place the item(s) back into the **Available Items** list.

Item Name	Description
Available External Storage	Shows the amount of external storage available on the device
Available Internal Storage	Shows the amount of internal storage available on the device
Available Memory	Shows the amount of RAM the device has available
Available System Storage	Shows the total amount of system storage available on the device
Battery Status	Shows what percent the battery was at the time the data collection rule ran
Call Log	Shows the call log of the device. i.e. What numbers were dailed outbound and inbound.
Cellular Carrier	Shows what carrier the device is connected to at the time the data collection rule ran
Cellular Signal Strength	Shows what the signal strength is of the device at the time the data collection rule ran
IP Address	Shows the IP address of the device at the time the data collection rule ran
Location	Collects the location of the device
SSID (Wi-Fi Name)	Shows the SSID that your device is currently connected to
RSSI (Wi-Fi Signal Strength)	Shows the signal strength of a wireless connection. A value of 0 is collected when there is no Signal listed in Manager
BSSID	Shows the MAC address the device is connected to

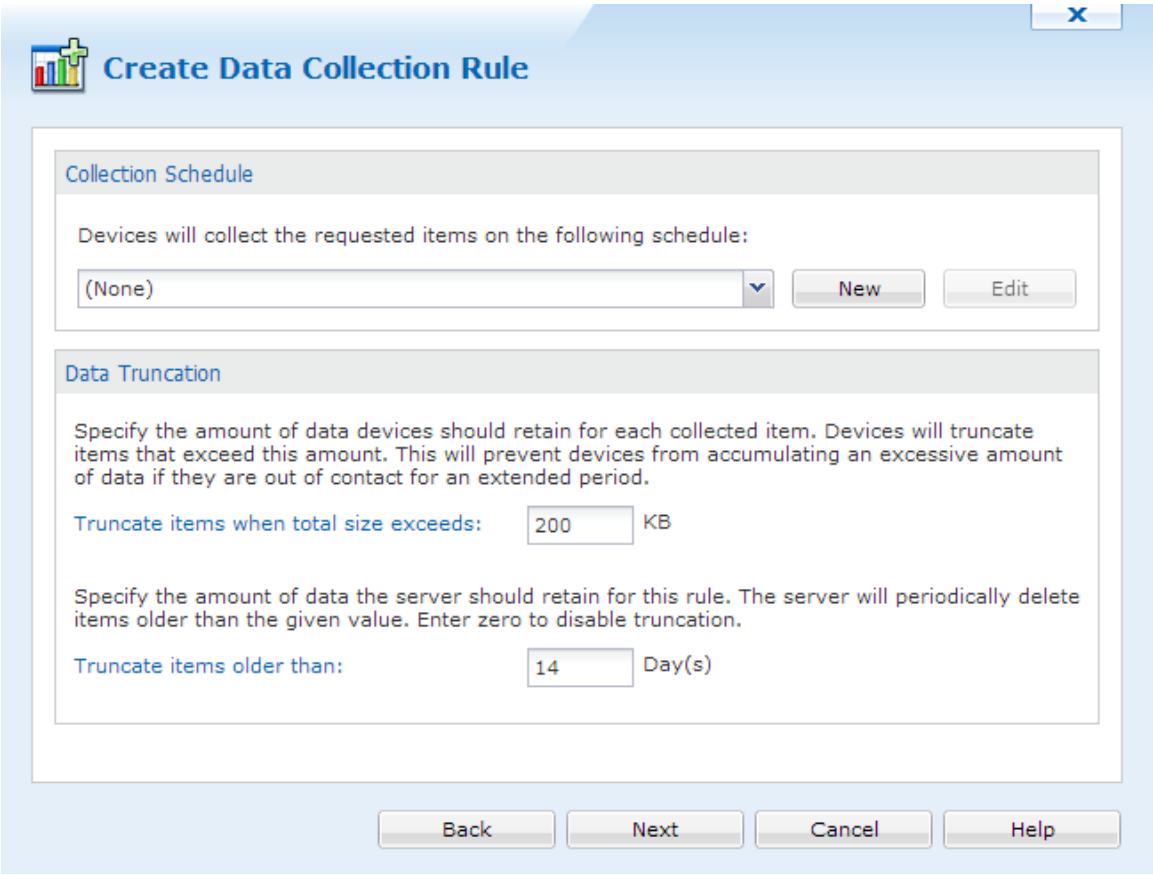
After selecting the choice(s), click the **Next** button.

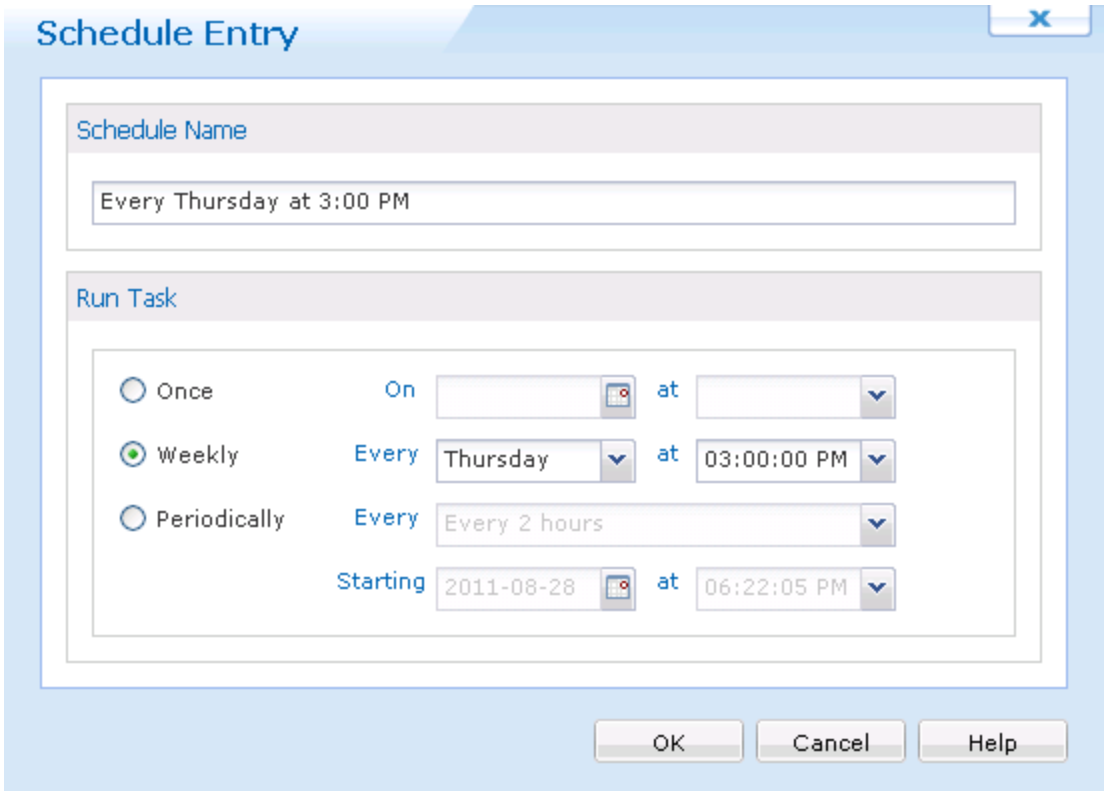
3. Select devices.

   Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



4. Configure data collection rule schedule and optional settings.




Schedule Entry
Schedule Name
Every Thursday at 3:00 PM
Run Task
Once
On
at
Weekly
Every
Thursday
at
03:00:00 PM
Periodically
Every
Every 2 hours
Starting
2011-08-28
at
06:22:05 PM
OK
Cancel
Help

Section Name	Description
Collection Schedule	This option enables you to create a custom data collection schedule with a custom date and time. Select the **New** button to create the new schedule. This will open up the second dialog box above. If you already have a previously created schedule, you can select edit to open the second dialog box above.
Schedule Name	Enter a meaningful schedule name that will be used to identify your custom schedule(s).
Run Task	Select the frequency for which you want to initiate the data collection on your device (s).
Delivery Schedule	This option will deliver the data collected from the device to the Deployment Serverbased upon the set update schedule. Currently, this option uses device schedule as the delivery schedule and is not configurable.

NOTE:

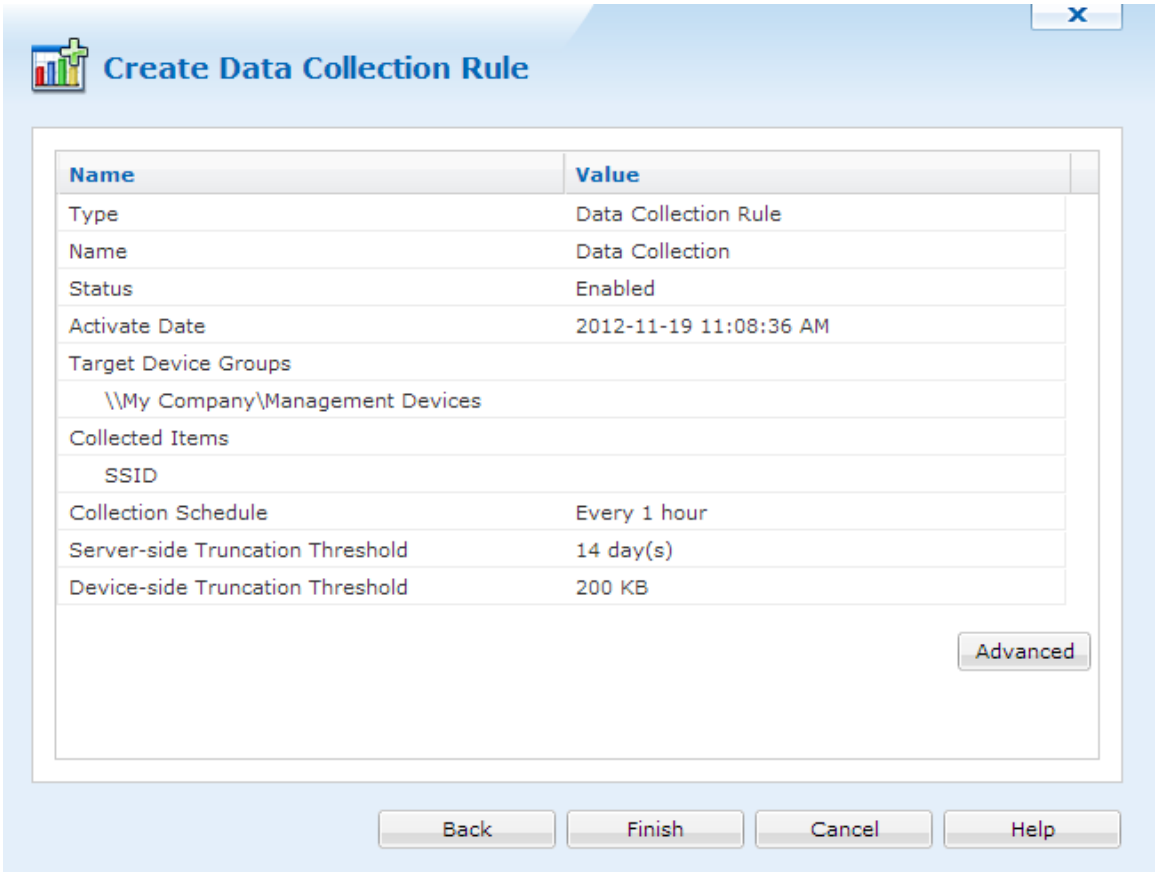
Creating a frequent collection schedule may affect the device's battery life. Also, frequent data collection can be managed with the truncation options available. This will help control how much data is kept on the device and in the database.

Choose the size of the data being collected. This helps control memory used on the device and the number of days you would like to retain the data in the database.

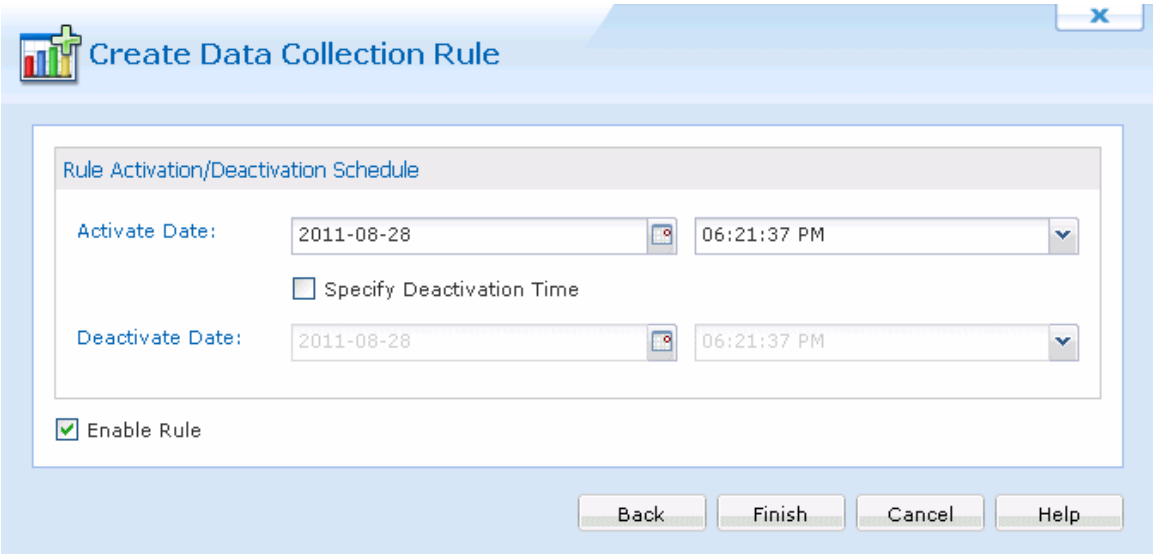
Section Name	Description
Device-Side Data Truncation	Specify the maximum size of data to be stored from the data collection ruleon the device(s).
Database Data Truncation	Specify the number of day(s) that you would like to retain the information in your database. Data collected older than the number of days listed will be deleted from the database

After entering your choice(s) in the above dialog box, click the **Next** button.

5. Review the summarized information.



By clicking on the Advanced button, the data collection rule Advanced window will appear. By default the rule will be activated immediately upon completion of the wizard. If you wish to delay the activation, you can modify the activate date. A deactivate date can optionally be entered to specify a date from which the rule will be disabled. A data collection rule can also be explicitly disabled by clearing the checkbox next to Enable Rule.



Section Name	Description
Activate Date	This option enables you to define a date and time when the rule will start collecting data from the selected devices
Deactivate Date	If the **Specify Deactivation time** box is checked, you can define the time at which you wish the data collection to stop.
Enable Rule	You can use this option to enable or disable the rule. This option is also available by right-clicking the rule.

The data collection rule can be deployed real-time or at a pre-set time. The data collection rule, although set to be activated at a scheduled time, can also be set to be deactivated. The deactivation setting is optional.

Click **Finish** to complete the wizard.

Android Alert Rules

Alert Rules allow Administrators to be notified when events of interest arise on the system. This notification system allows Administrators to quickly and effortlessly communicate an event message to large groups of people via email, and notifies users via the MobiControl Manager Alert tab. For every type of scenario, whether it is a Rule Change or a Device Error, the system will rapidly deliver your message to a designated audience.

NOTE:

The Deployment Server must be online in order for Alerts to be generated and sent out.

The MobiControl Web Console allows you to create Alerts based on the Devices Operating System (OS). Some Alerts are specific to the OS Tab that has been selected . For detailed information on the Alerts Available please see below.

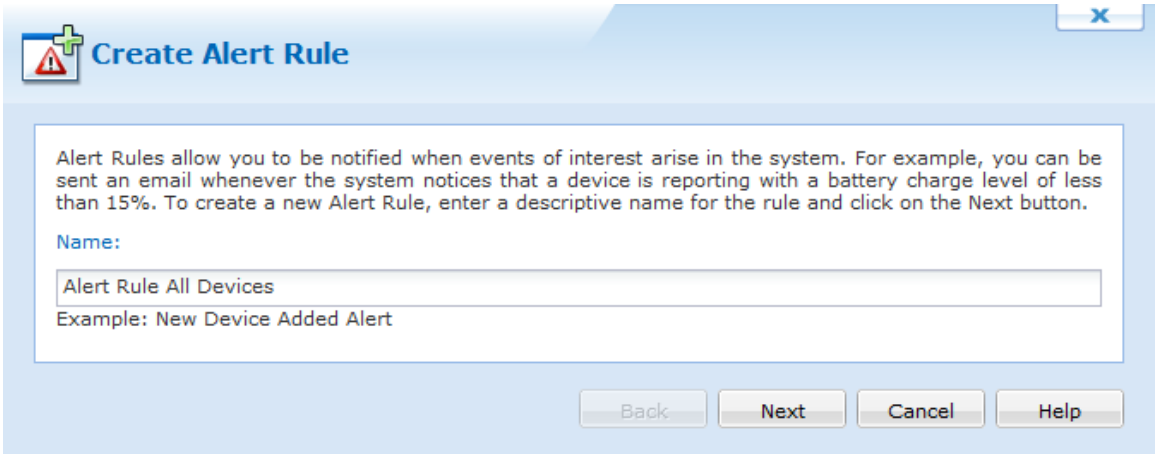
Type	Description
Device Event	Trigger alerts based on an assortment of device specific conditions.
Device Status and Custom Data	Trigger alerts based on Custom Data vales that you have configured.
Geofence Event	Trigger alerts based on devices entering or exiting geofenced areas.

The steps below describe how the Create Alert Rule Wizard can be used to create an Alert using the MobiControl Web Console:

1. Start the wizard.

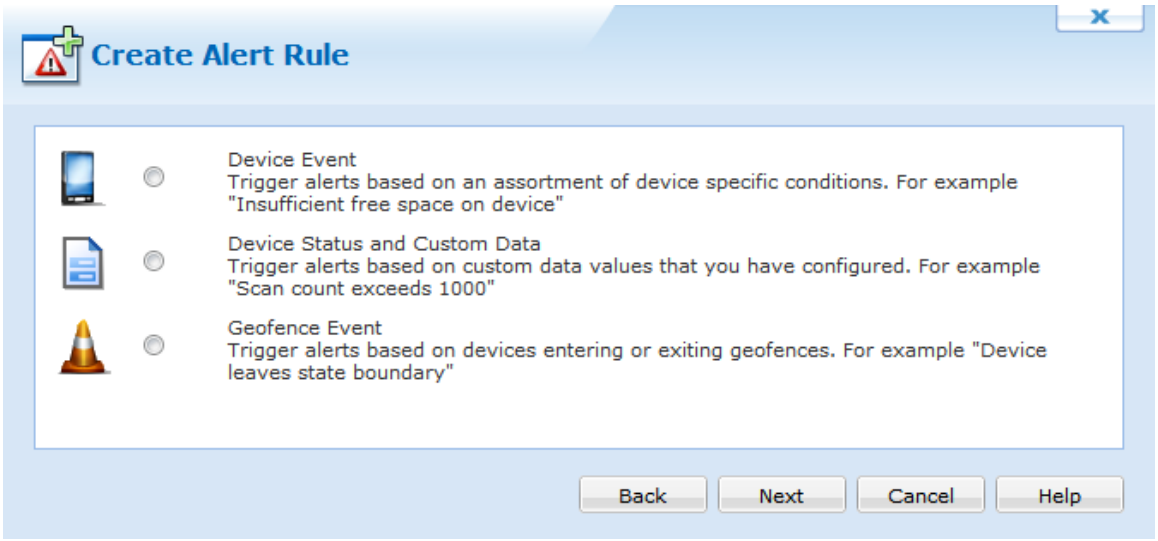
   Select the All OS's Tab, then select the Rules tab, then Right click on the **Alert Rule** folder, and select **Create Alert Rule**. The first page of the Create Alert Rule Wizard will be displayed.

   Enter a descriptive name for the Alert Rule you are creating and click **Next.**



First page of the Alert Rule Wizard

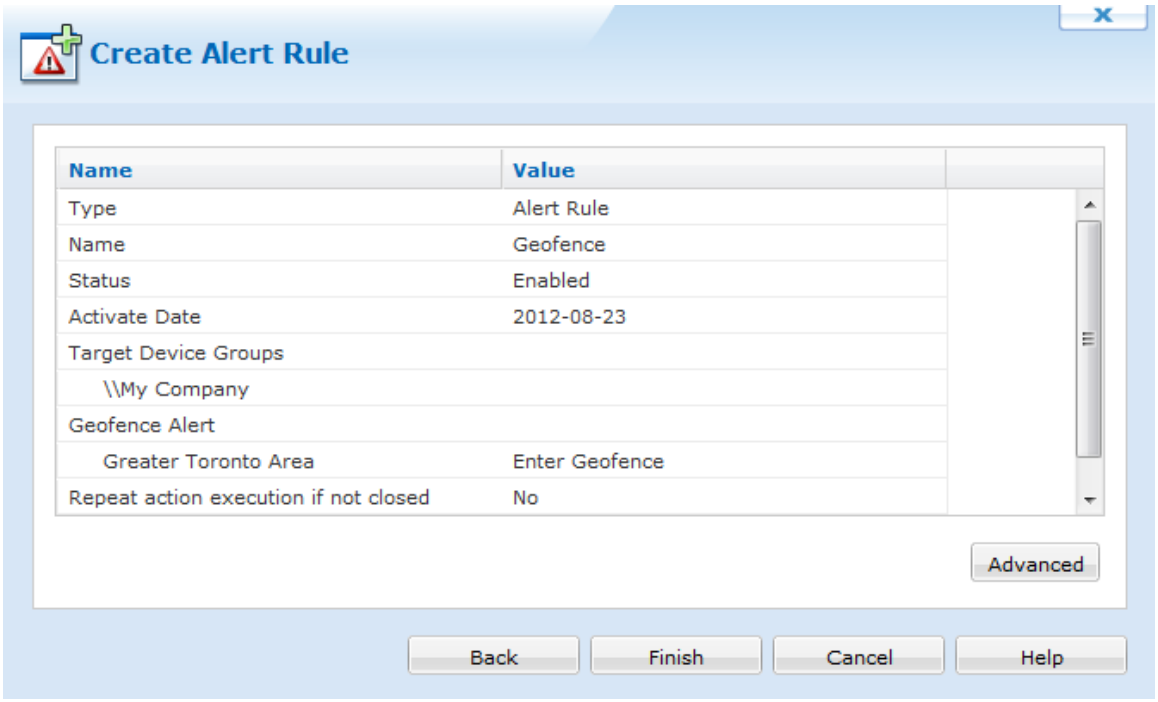
2. Select the Alert Rule Type.



Select the Alert Rule Type and click Next. After Clicking Next you will be asked to specify the Alert Options for the selected Alert Type. Select the type of alert below for more information on the Alert Options available.

Type	Description
Device Event	Trigger alerts based on an assortment of device specific conditions.
Device Status and Custom Data	Trigger alerts based on Custom Data vales that you have configured.
Geofence Event	Trigger alerts based on devices entering or exiting geofenced areas.

3. Review the summarized information.



Click **Finish** to complete the wizard.

Geofence Event

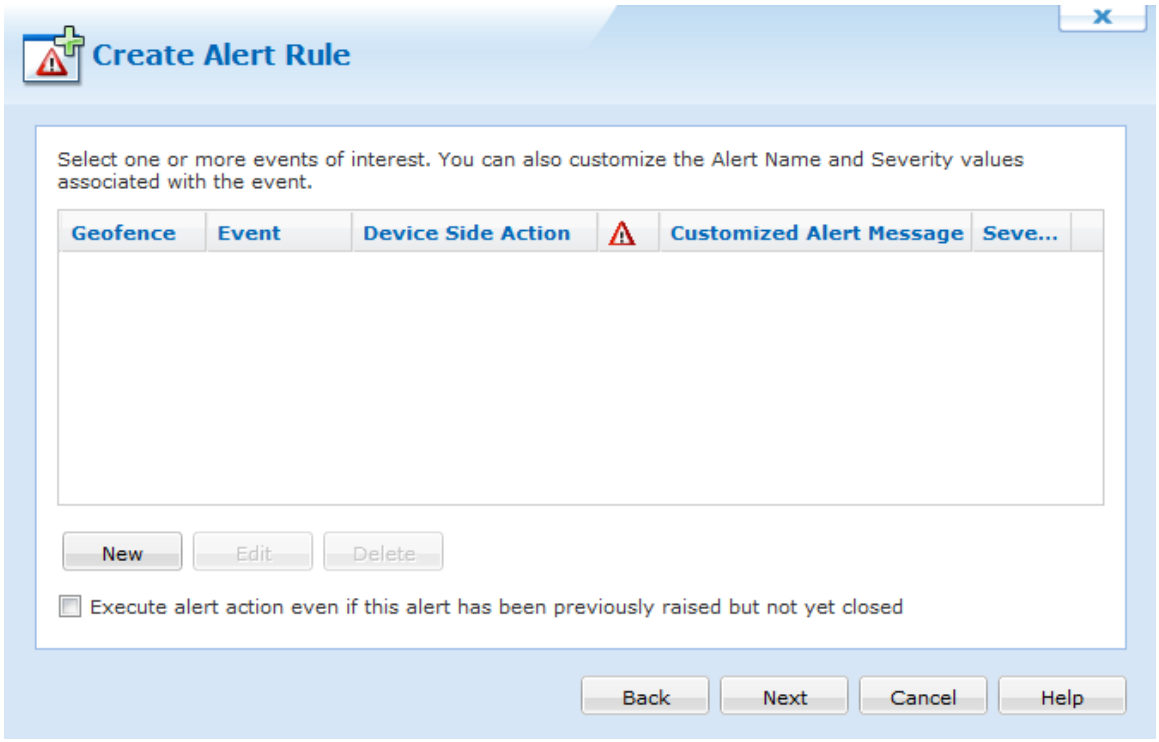
A Geofence Event is an alert trigger based on a GPS enabled device entering or leaving a Geofenced area defined by MobiControl administrators.

EXAMPLE:

If there are devices that should not leave a building complex, a geofence alert rule can be created to ensure that MobiControl administrators are alerted if these devices do leave the complex. Geofence areas can be as small as a house, or a big as a continent.

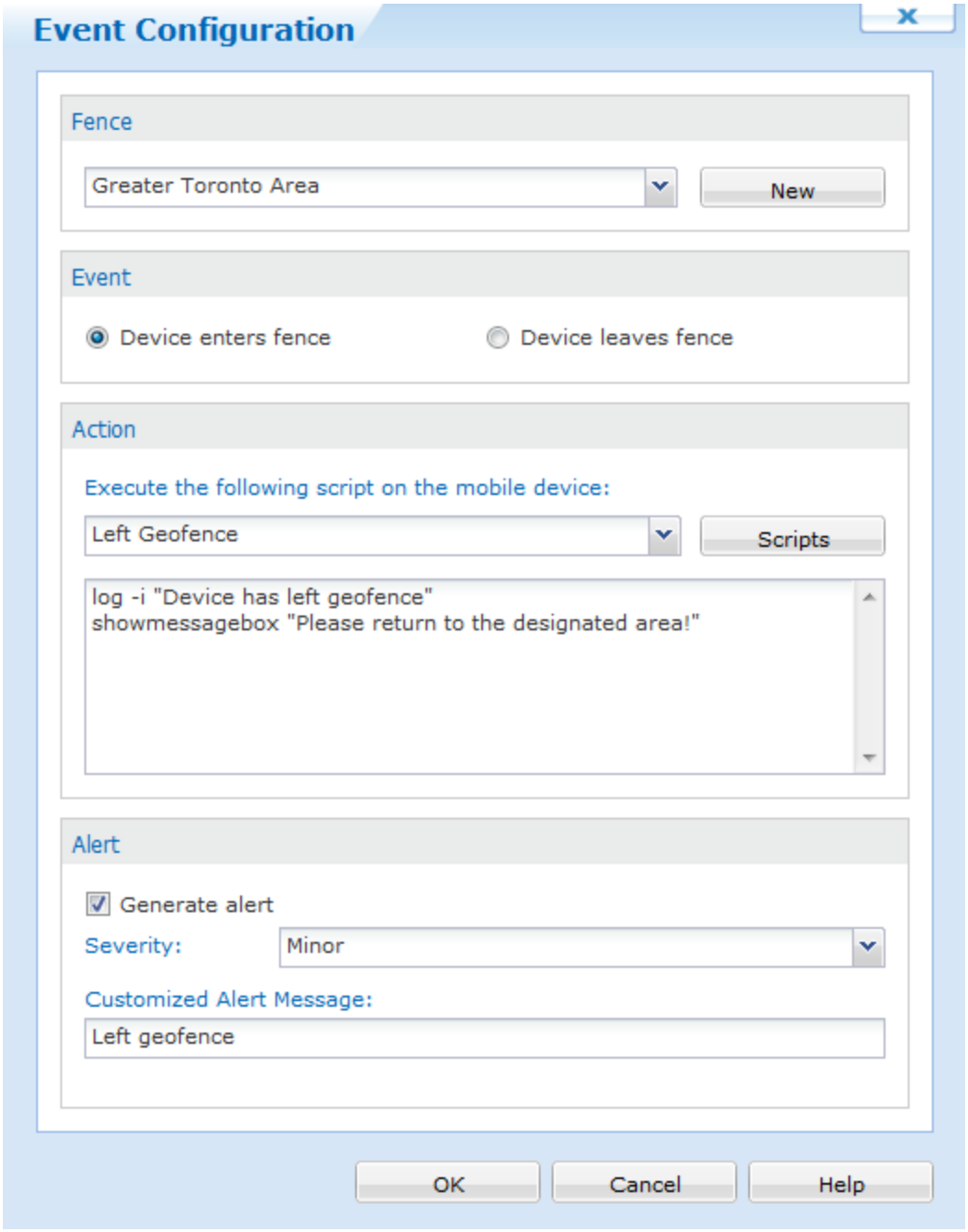
In order to create a Geofence event, an Alert Rule is needed with the Geofence Event type. Please see the "Android Alerts" topic on page 1248 for assistance with creating an alert rule.

After selecting the Geofence alert type, you will be presented with a window that has all previously created Geofences. If no Geofences have been created click the **New** button.



Geofences

Clicking new brings up the Event Configuration window. Here we can create a new geofence.



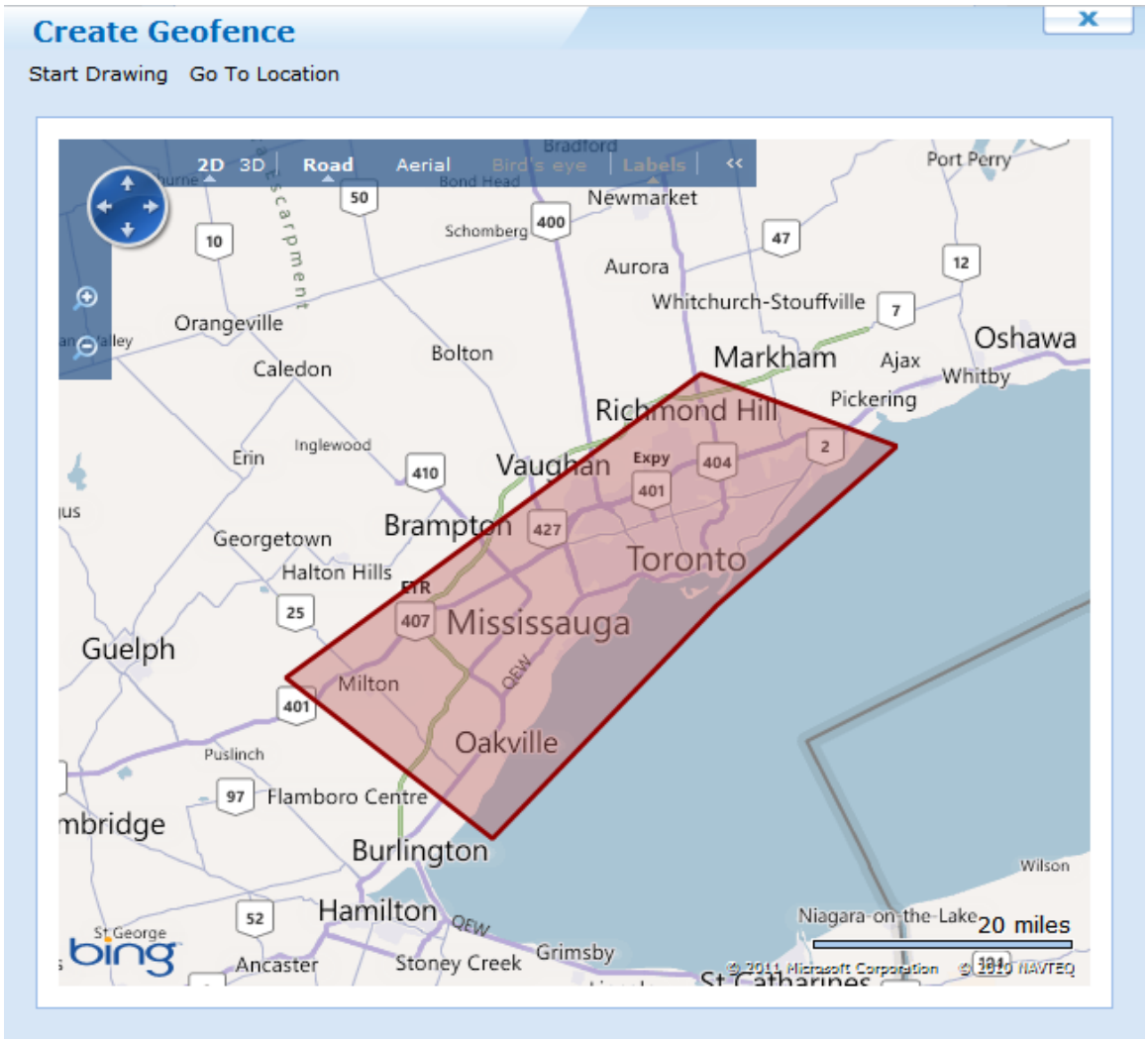
The **Fence** section allows you to create a geofence by clicking on the New button in the dialog box.

The **Event** section allows you to configure if this event should be triggered on entry or exit of a fence.

The **Action** section allows you to configure what script you want to run on the mobile device when the event is triggered. This is optional, but you have for example the ability to run an Activate Connection, Log Event, Show Message or even wipe the device completely.

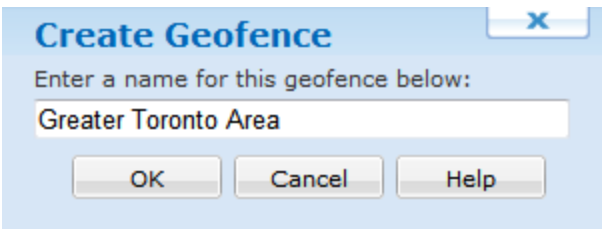
The **Alert** section allows you the option to Generate an alert, configuring its Severity (Minor, Serious and Critical) and add a Customized Alert Message, such as "Left geofence".

When you click on the **New** button in the **Fence** section, the following Geofence Creation dialog box appears:



The two options available are to Start Drawing and Go to Location.

The **Start Drawing** option allows you to begin drawing on the map below the button. The area drawn on the map will be defined as the Geofence. The defined area must be a complete geometric shape, which means the Start Drawing point will be the same as the End Drawing point. When you have completed a proper geometric shape you be asked to name your geofenced area.



Prior to selecting the Start Drawing button, you have the ability to use the view control buttons in the map in order to move to a desired location, zoom in and out, switch to 3D, Road, Aerial and Bird's eye views among the many options. This allows you ease to create an appropriate view for your geofence.

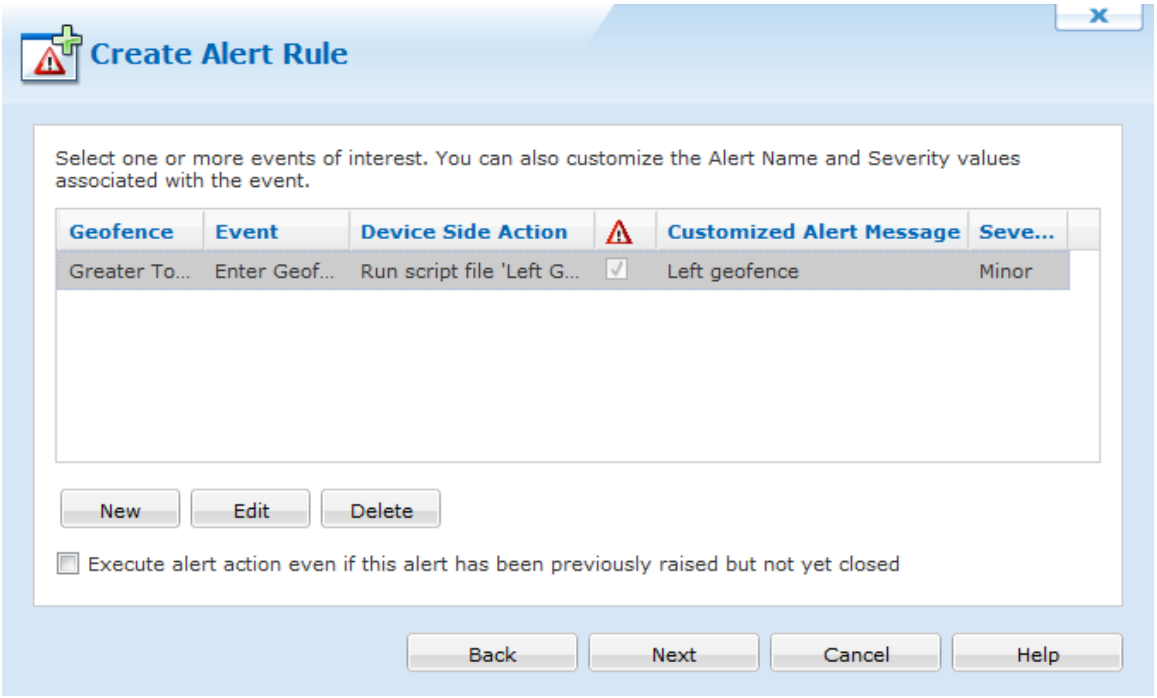
Alternatively to identify the appropriate view of the map, you can click on **Go to Location** which will allow you to specify a street address, location, landmark, or an existing geofence.

EXAMPLE:

- 350 Fifth Avenue, New York City
- Rome
- SFO (San Francisco International Airport)

Once you have the appropriate view displayed, you can click on Start Drawing and you are now able to create a fence. The first click of the mouse is first point of the fence. In order to complete the fence, you must have at least 3 distinct points selected on the map. In order to complete your fence, the last point must end off at the first point so it completes the closure of the fence. Once the last point is selected, a pop-up requesting the name of the geofence is shown. Here you should enter a meaningful name for that specific geofence in case you would like to use it again.

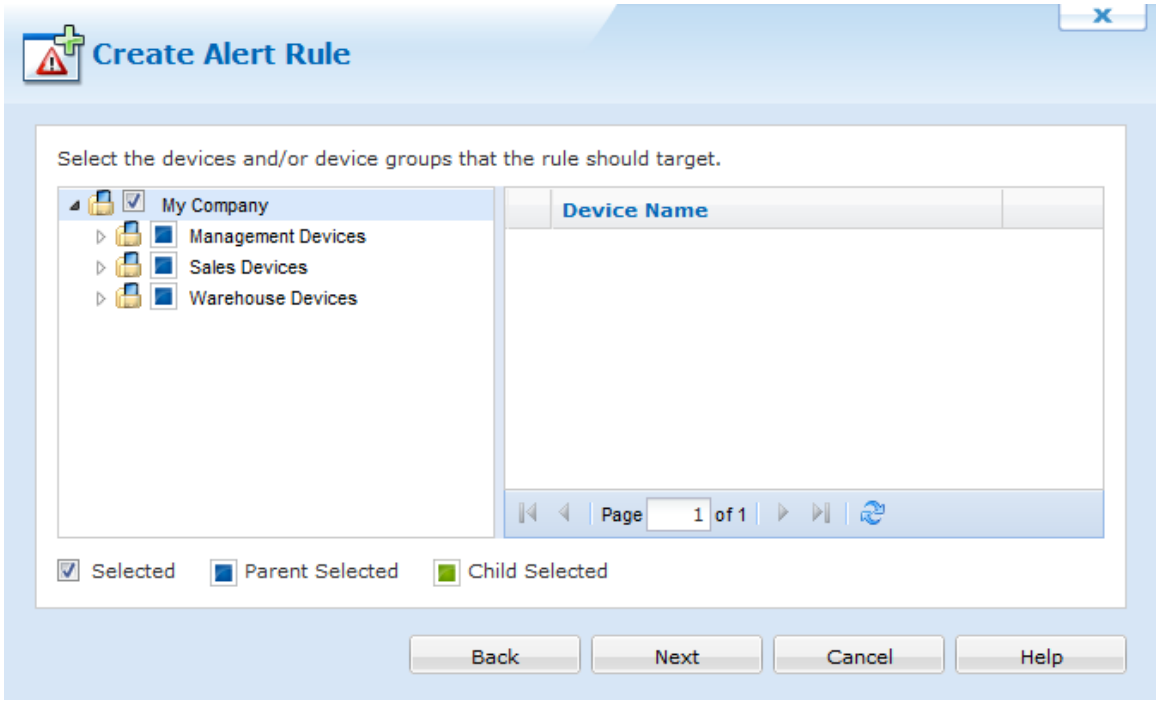
Select Geofence



Once the event is configured it will display as shown in the above diagram. Here you have the ability to create new events, edit existing events or delete events. Also, on this dialog box, there is a checkbox at the bottom allowing you to determine whether or not you want to Execute alert action even if this alert has been previously raised but not yet closed.

Select Devices

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



Select Power Policy

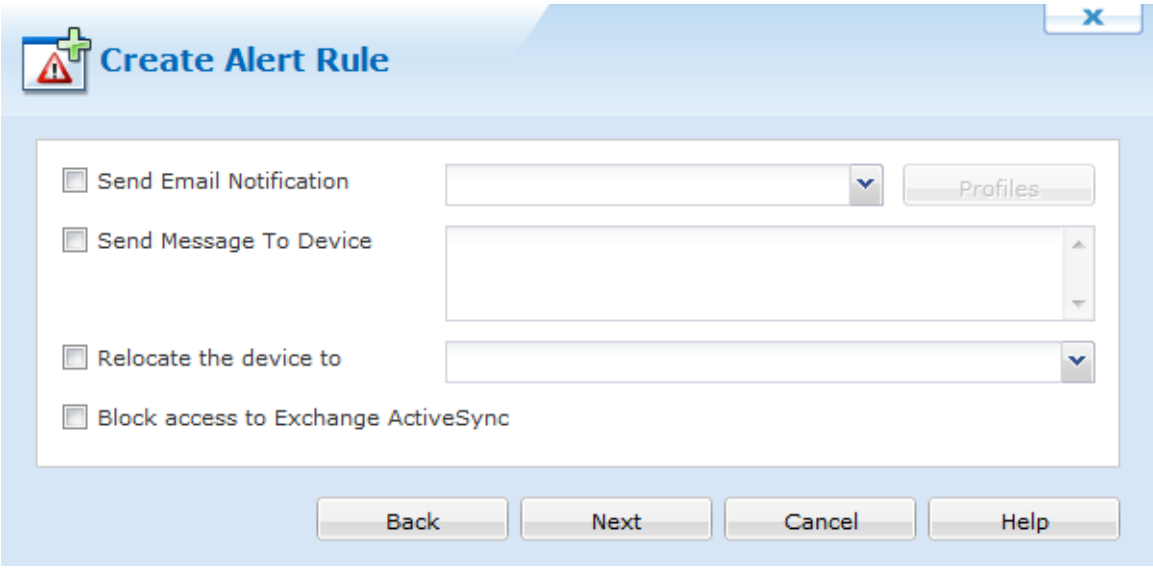
Clicking Next moves you to the Power Policy section as seen below.

The options available for the Power Policy are Continuous and Periodic.

Power Policy	Description
Continuous	This indicates the GPS radio is always on and the location will be monitored in real time. It is best to use this option with devices that have an external power source or are vehicle mounted because this option takes up a lot more power.
Periodic	This will turn on the radio based on a schedule that you define. Based on your business requirements, this can be as responsive as every 2 minutes, or every weekday all the way up to every year. It is best to use this option when you have battery powered devices in order to minimize the amount of power consumed with having this feature on.

Action Settings

Once the power policy is selected, you must select your an action to be done.



Select any action to be done when the Geofence alert has been triggered. MobiControl gives the option to send an email to administrator groups, send a message to the device, relocated the device to a different group, or block access to Exchange Active Sync. One or many of these options can be selected.

After selecting your actions, click Next and continue the Alert Rule Wizard here.

Android Telecom Expense Management

The Telecom Expense alert rule allow MobiControl Administrators to monitor how much data and minutes a group of devices/individual devices use based on a company data plan. This rule allows Administrators to set a soft threshold along with a hard threshold. When data or voice minutes reach either the soft or hard threshold, devices can automatically be relocated to another group and have either data or voice disabled. An email can also be generated and sent to a configured email address when a soft or hard threshold is reached.

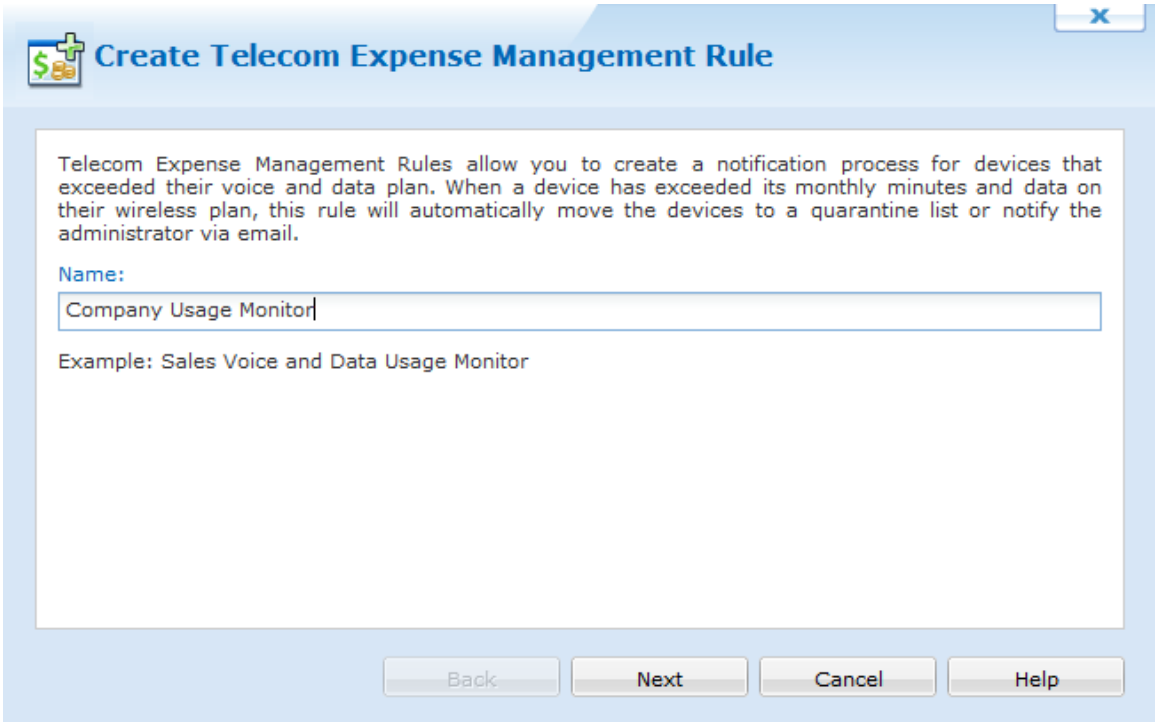
This allows enterprises to better manage company data and voice minutes.

The steps below describe how the Create Telecom Expense Management Wizard can be used to create an Telecom Expense Alert using the MobiControl Web Console:

1. Start the wizard.

   Select the Android+ Tab, then select the Rules tab. After, right click on the **Telecom Expense** folder, and select **Create Telecom Expense Management Rule**. The first page of the Create Telecom Expense Management Wizard will be displayed.

   Enter a descriptive name for the Telecom Expense rule and click **Next.**



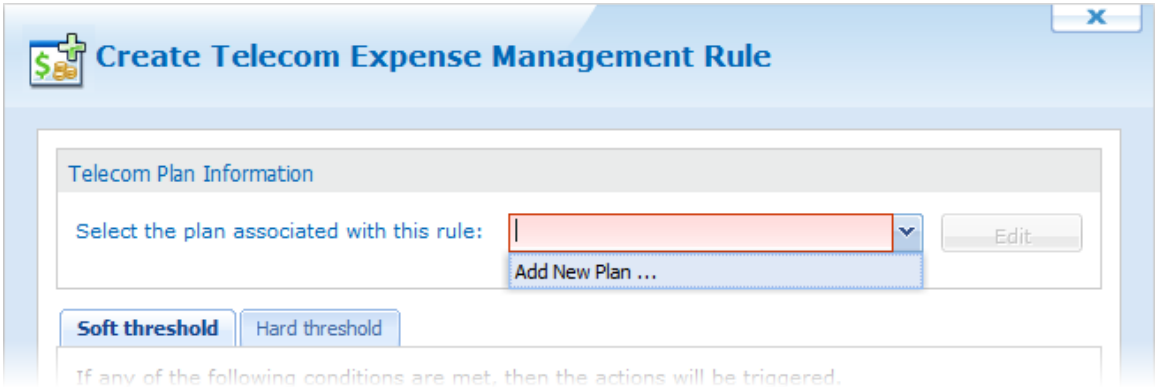
Enter a descriptive name for the Telecom Expense Rule

2. Select the target for the rule.

Here, we can select which group or device will be monitored with the Telecom Expense Management rule. Groups or devices that have ■ means that they are automatically selected because their parent group is selected. Groups that have ■ means that a child of that group is selected. Click **Next** to continue.

3. Telecom Expense Management configuration

On this screen, we are able to create a new data plan that will be associated with this rule, or choose an existing one. To create a new plan, choose the **Add New Plan** from the very top drop down menu.

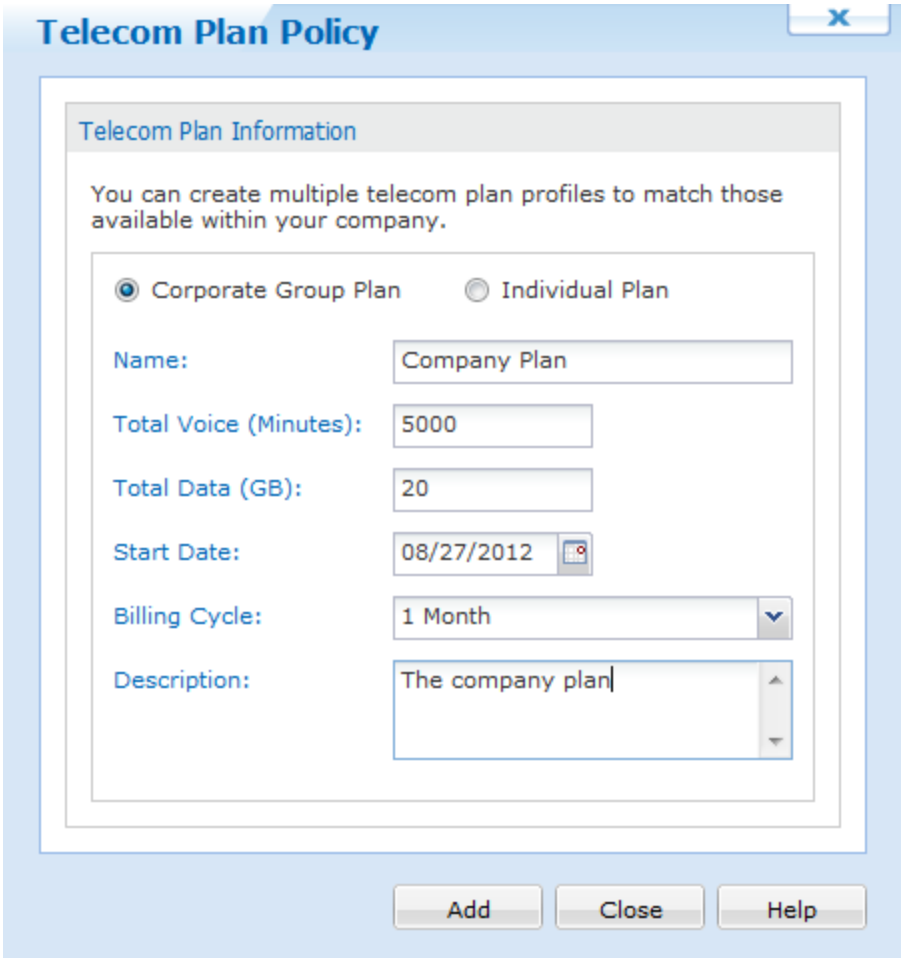


Adding a new Telecom plan

When **Add New Plan** is selected, the Telecom Plan Policy window is shown. Here we can choose whether this plan should be for a Corporate Group plan or an Individual Plan.

It is recommended that Corporate Group Plan is selected if the Telecom Expense Management rule is targeting a group of devices.

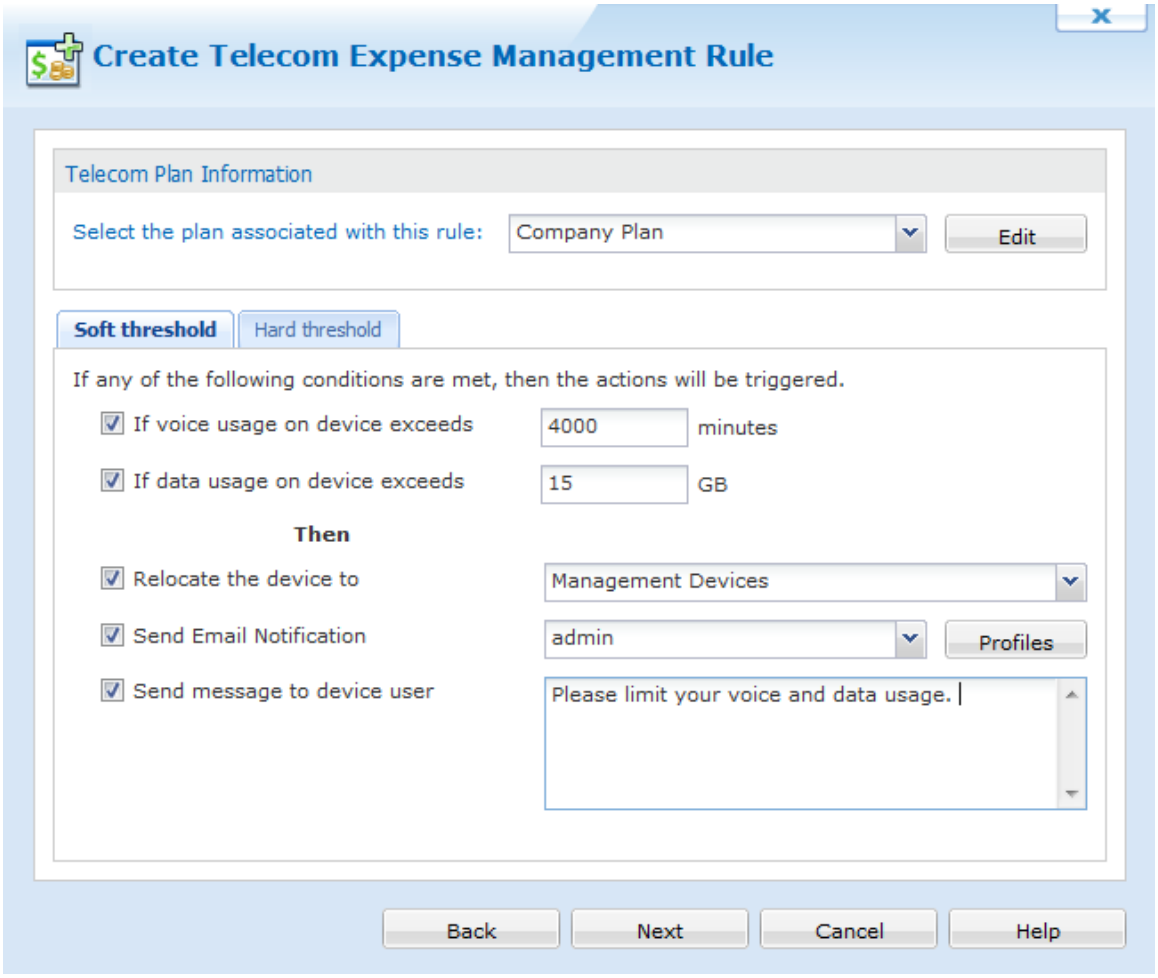
- A name and a billing cycle must be entered to add a plan.
- Voice is calculated in minutes, while data is calculated by gigabytes. If either of these are left blank, then unlimited is automatically listed.



Telecom Plan Policy

When a plan policy is created we can then configure the soft and hard threshold for the rule. Think of the soft threshold as a warning, and the hard threshold as critical. If the "voice usage on device exceeds" check box is selected, MobiControlwill check if a device or devices reach the number specified. The same rule applies for monitoring data usage. If any of the numbers are reached, MobiControl can then move the device to a new group, send an email notification, or send a message to the user.

After setting up the configurations here, click **Next**.



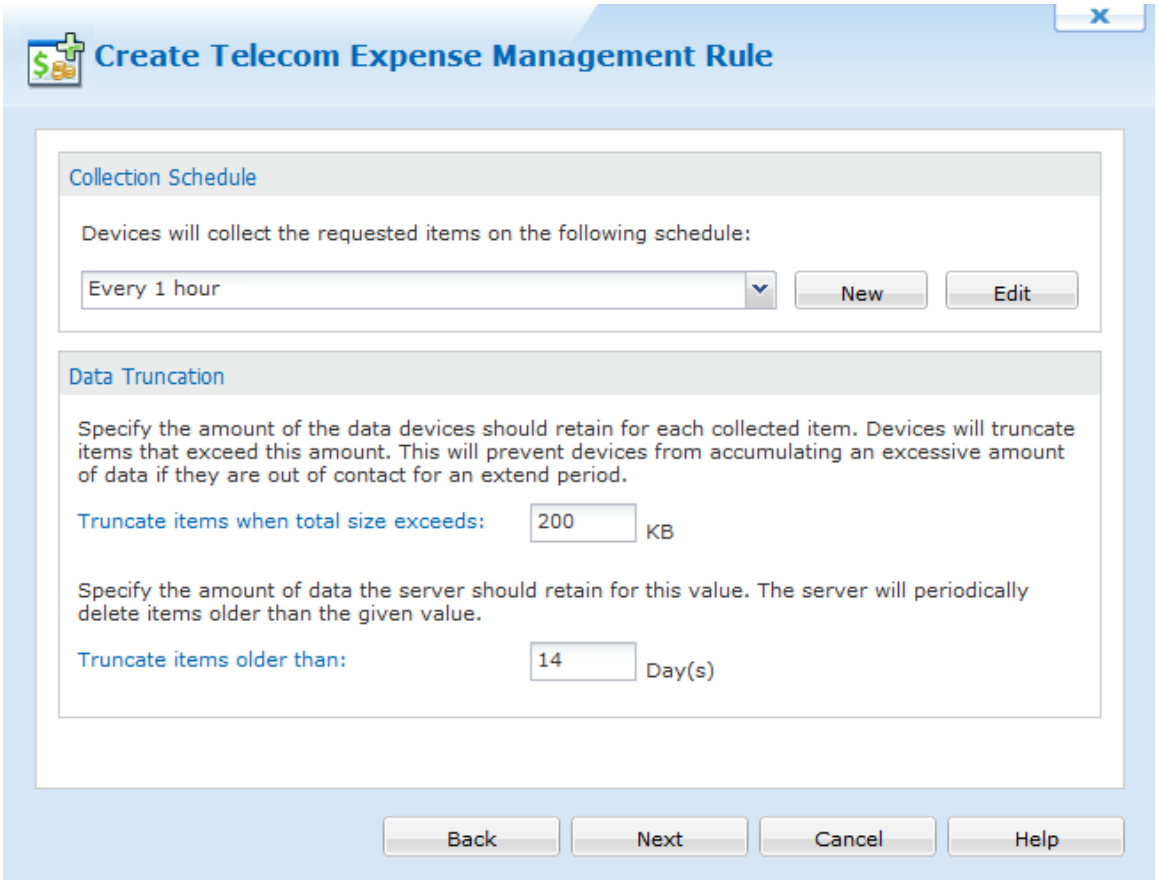
Telecom Expense configuration

4. Configure Data Collection and Optional Settings

Here, we can set how often the data is to be collected. Options include every 30 minutes, every hour, every two hours or daily. We also have the ability to create a custom collect schedule.

Data truncation specifies the amount of data that each device should retain. Any amount of collected data that goes above this number, will be truncated. This can be left as the default value.

After specifying the collection schedule and data truncation settings, click **Next**.

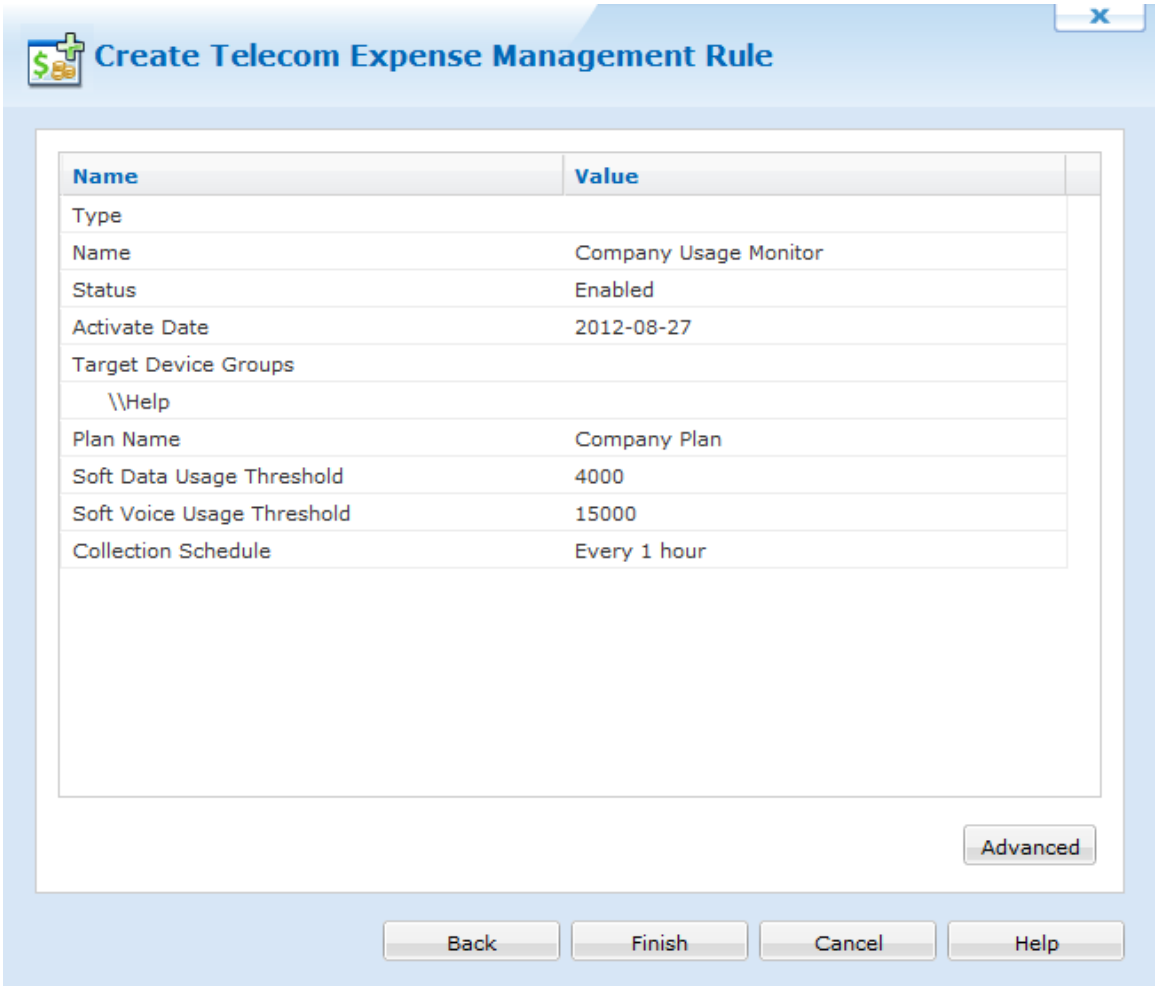


Data collection and optional settings

After specifying the collection schedule and data truncation settings, click **Next**.

5. Review the summarized information.

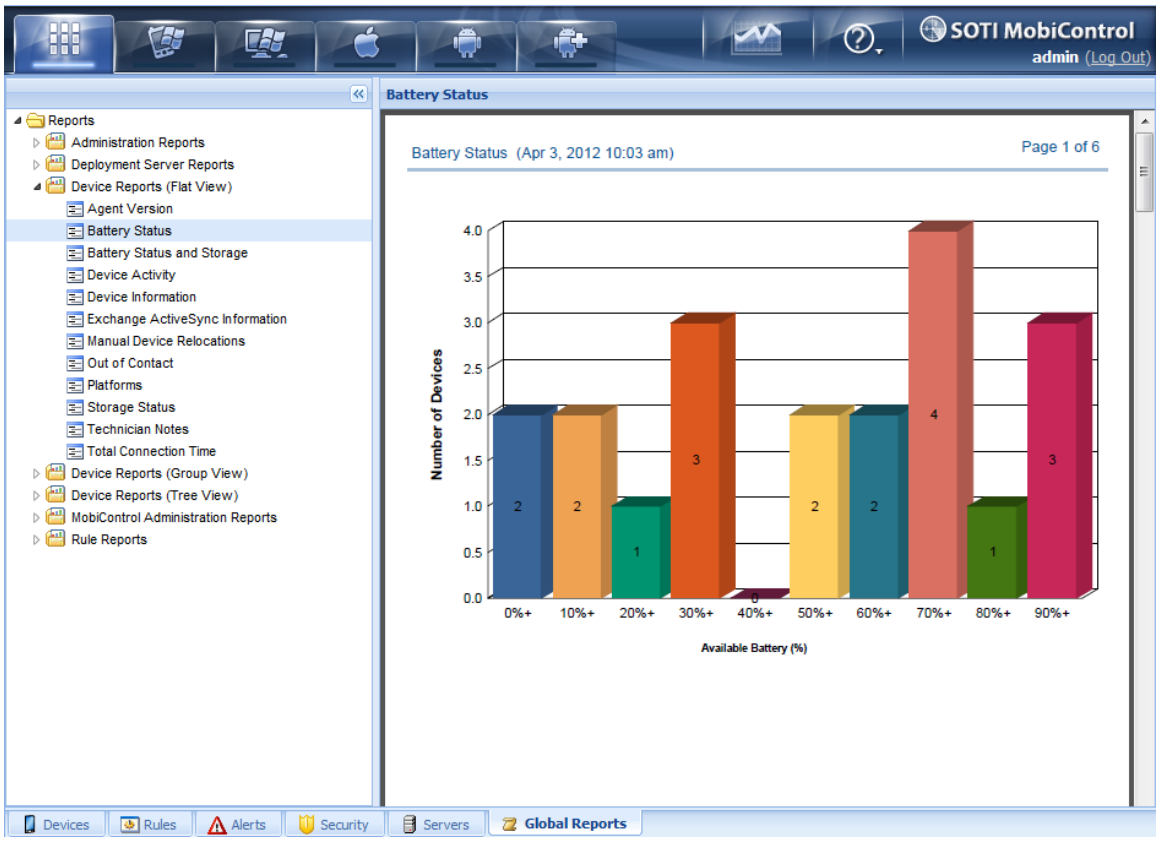
   The summary page will show all options and configurations that was specified in the previous steps. If something is needed to be changed, just click back and change the setting.



   Once everything is confirmed, click **Finish** to complete the wizard.

Android Reports Tab

MobiControl includes an advanced reporting engine—Crystal Reports—that gives detailed information about all aspects of system operation. The product includes a set of canned reports that provide information about key areas of system operation. Reports can also be customized as well as new reports can be created and added to the system as needed.



MobiControl Manager Reports view (tab)

The MobiControl Web Console allows you to generate Reports based on the Devices Operating System (OS). Some Reports are specific to the OS Tab that has been selected. For detailed information on the Reports available please see the specific Reports that can be created below:

Report Types

The following reports are included with MobiControl:

- A **deployment server activity report** is a detailed report for deployment server activity over a specified time period.
- A **deployment rule report** is a detailed report of deployment rules and all devices.
- A **Battery and Storage Report** is a detailed report of the battery and storage of the selected devices.
- A **Cellular Signal Strength Data Report** is a detailed report of the cellular signal strength of the selected devices.
- A **deployment rule summary report** is about deployment rule exceptions, showing how many devices have executed the rule successfully, are pending, or have encountered an error.
- A **Deployment Server activity report** is a detailed report of Deployment Server activity over a specified time period.
- A **device activity report** provides information about the device activity during a specific time period.
- A **device custom data report** provides information about devices with the custom data values of selected custom data fields.
- A **device note report** provides information about the notes for your devices.
- A **device package report** provides information about packages installed on your device.
- A **device program report** provides information about all the programs installed on your devices.
- A **device relocation rule report** provides information about all the relocation rules for your devices.
- An **out of contact devices report** provides information about devices that have not connected to the system since the specified date.
- A **package deployment report** provides information about package deployment.
- A **Location Collected Data Report** is a detailed report of the location data collected for the devices.
- A **Connectivity Information Report** is a detailed report regarding device's connectivity.
- A **Device Tree Report** provides information about the device tree structure.
- A **Device Tree with Virtual Groups Report** provides information about the device tree structure along with the virtual groups.
- A **Log Information Report** provides information about the device logs.
- A **Phone Number Report** provides information about the phone number of devices.
- A **Alert Summary Report** provides summary of the alerts.
- A **deployment rule report** is a detailed report of deployment rules and all devices.
- A **Geofence Report** provides detailed report based on the Geofence.
- A **Uninstalled Mandatory Applications Report** provides information about the mandatory application not installed on the devices.
- And many more.

Generating a Report

1. In MobiControl Manager, select the Reports view (tab).
2. Select a report in the left pane of the Reports view (tab).
3. Click the **Generate Report** button.

4. For some reports, a window will appear requesting additional parameters (e.g. time period) that may be required.

Saving a Report

1. Generate a report.
2. On the report screen, click the **Export Report** button. (It is the first icon in the toolbar, beside the **Print Report** button.)
3. Select the desired file type. Available file types are:
    - Adobe PDF (`.pdf`)
    - Crystal Reports (`.rpt`)
    - HTML 3.2/4.0 (`.html`)
    - MS Excel 97-2000 (`.xls`) or Data only (`.xls`)
    - MS Word editable RTF (`.rtf`)
    - ODBC
    - Record-style (columns of values with or without spaces) (`.rec`)
    - Report definition (`.txt`)
    - Rich text format (`.rtf`)
    - Comma-separated values (`.csv`)
    - Tab-separated text (`.ttx`)
    - Text (`.txt`)
    - XML (`.xml`).
4. Select the location to which you want to export the report. The options available are:
    - Application
    - Disk file
    - Exchange folder
    - Lotus Domino
    - Lotus Domino Mail
    - MAPI (Messaging Application Programming Interface)

Printing a Report

1. Generate a report.
2. On the report screen, click the **Print Report** button. (It is the second icon in the toolbar, beside the **Export Report** button.)
3. The print menu will pop up. Select the desired printer and the report will be printed there.

Generating Custom Reports

It is possible to create custom report files on any available statistic you desire. The Deployment Server database is a standard SQL database and can be queried by writing a custom query. Also, it is possible to create additional reports that are built into MobiControl. For more details, please contact us.

Other Tools

These other tools are available through the toolbar:

- The **Stop Loading** button stops the report generation process
- **Refresh** regenerates the report. If parameters were required to generate the original report (e.g. time period), a window will appear requesting the additional parameters
- The **Search Text** button searches the body of the report for a specified text string
- The **View Zoom** field allows the user to select view magnification, page width, and whole page views

Secure Content Library

The MobiControl Secure Content Library allows users to upload files through the web console so that it can be distributed to devices.

With the Secure Content Library we are able to specify file properties when it is uploaded. These properties can range from delivery methods to expiry dates.

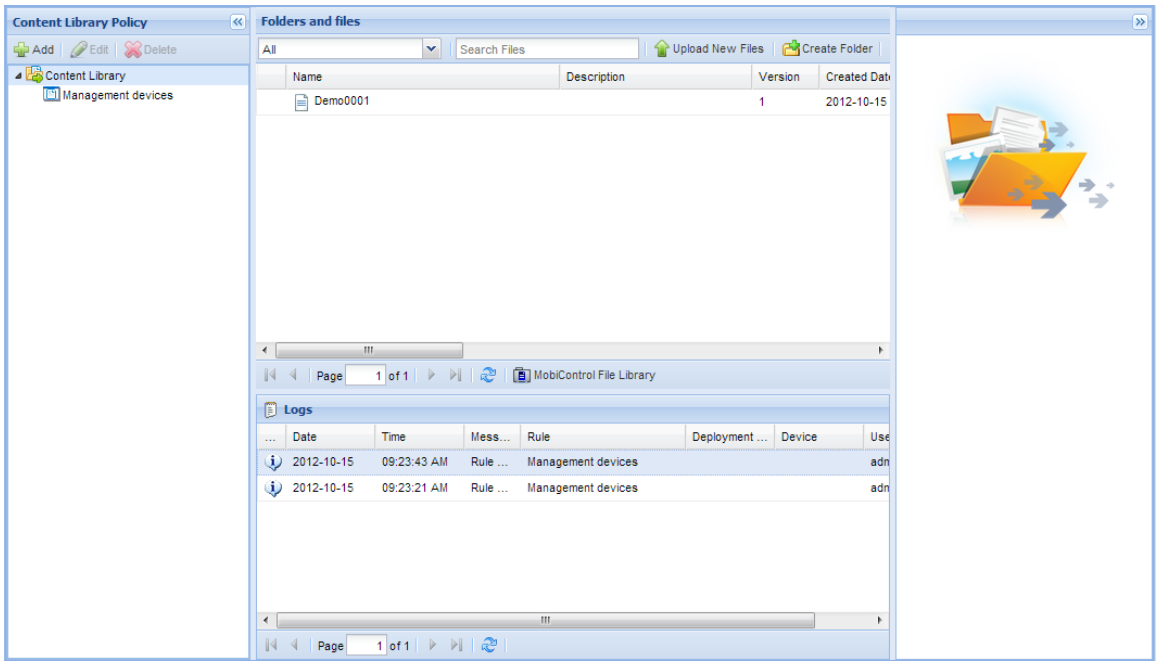
NOTE:

The Secure Content Library is only available for iOS and Android devices.

NOTE:

If the file sync rule is enabled for iOS devices, all those files will appear in the same panel as Content Library files. Files sent by the file sync rule cannot be configured by Content Library settings.

To go to the Secure Content Library, click the Content Library tab at the bottom of the device tab.



Secure Content Library

There are 4 main panels in the Secure Content Library. Starting clockwise, there is the Content Library Policy, Folders and Files, Deployment status, and logs. The Content Library Policy allows us to select which devices get files. Folders and files panel allows us to upload new files and create new folders. The deployment status shows us how many devices downloaded files, and the logs panel shows the logs related to the Secure Content Library.

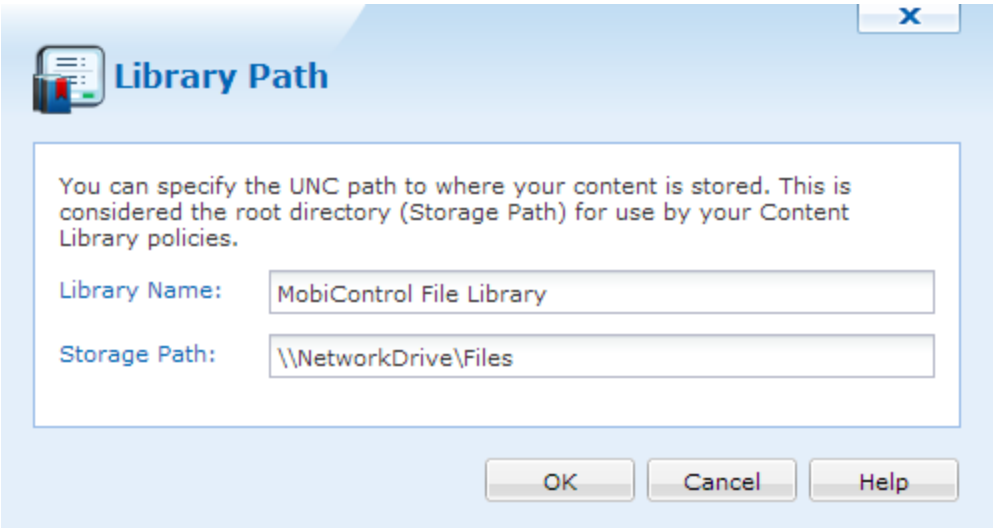
Library Path

When we first open the Secure Content Library tab, we will be prompted with a dialog asking us to name the Content Library and where to store the files.

The Storage Path could be anywhere the deployment has access to. Be it a shared folder on the network, or a folder on the hard drive. All files uploaded will be placed here.

NOTE:

The recommended Storage Path should be a network drive where both the Deployment Service and Management Service have access to.



Library Path

NOTE:

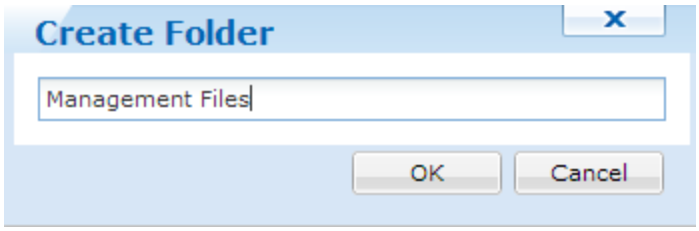
We can change the Library Path at any time. To do this, click the icon at the bottom of the Folders and files panel.

Folders and Files

After choosing the Library name and the Storage Path we are ready to create our folders and upload our first files.

Creating Folders offers a way to organize files. If a folder is wanted to be created, click Create Folder.

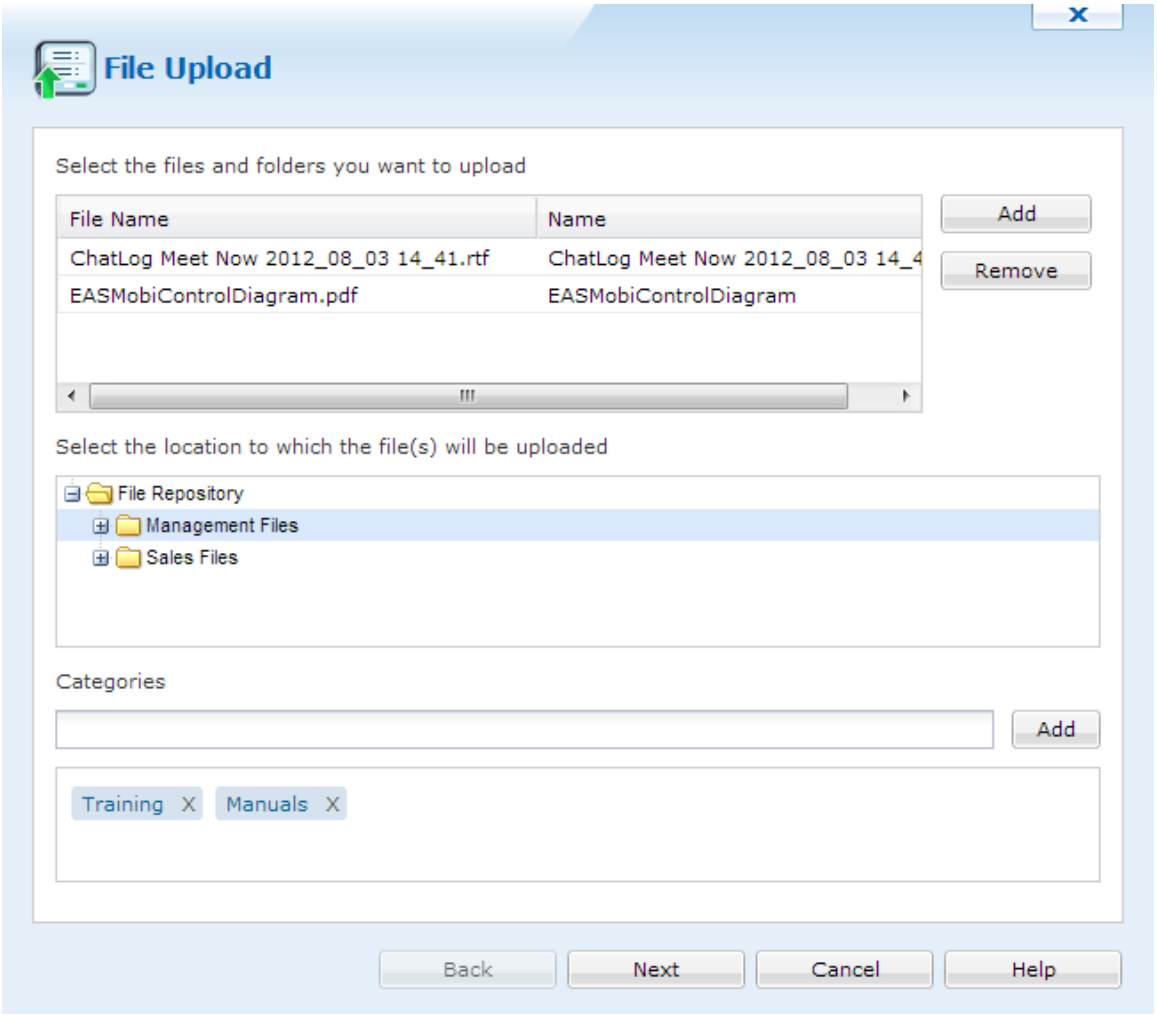
When the Create Folder dialog appears, enter a name and click OK.



Create Folder dialog

File Upload

After creating any folders needed, we can now upload files. To do this, click Upload New Files .



File Upload

Click the Add button to select a file and upload it. We can upload multiple files from here. If a file isn't needed, select it and then click Remove.

After uploading the files, we can select where these files will be placed in the Secure Content Library. File Repository is the root directory, then listing all folders that were created.

When a folder is chosen, we can add categories to these files. Categories are special tags that label each of the files. If we categorize these files for training, we can filter them based on these tags.

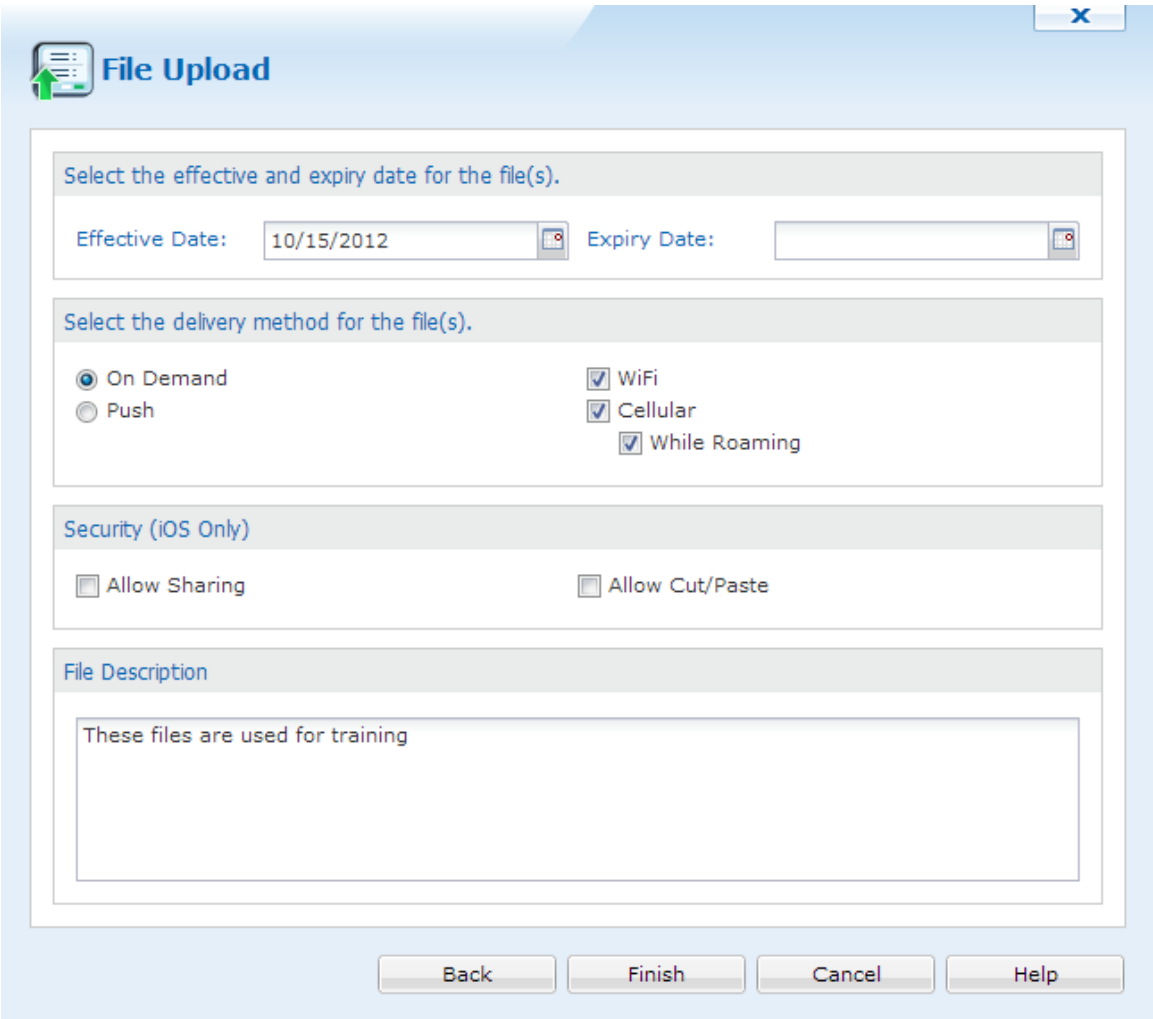
To add a category, just type it into the text field. If categories were created before, MobiControl will find them and we will be able to select them. If a category wasn't created, click Add to create this category.

When everything is configured and set, we can click Next to go to the next page.

File Upload Properties

This panel will allow us to modify the properties of the uploaded files.

We can select the dates the files are effective for, the delivery method, security and description.



File Upload Properties

NOTE:

If the Expiry Date is not needed, please do not click the field. This will ensure that the files will never expire.

If we select On Demand as the delivery method, then files will not be automatically pushed to the devices. Selecting Push will allow the files to be automatically downloaded to the devices.

We can also restrict the way the files are downloaded.

iOS devices offer additional security where these files cannot be shared or cut and pasted.

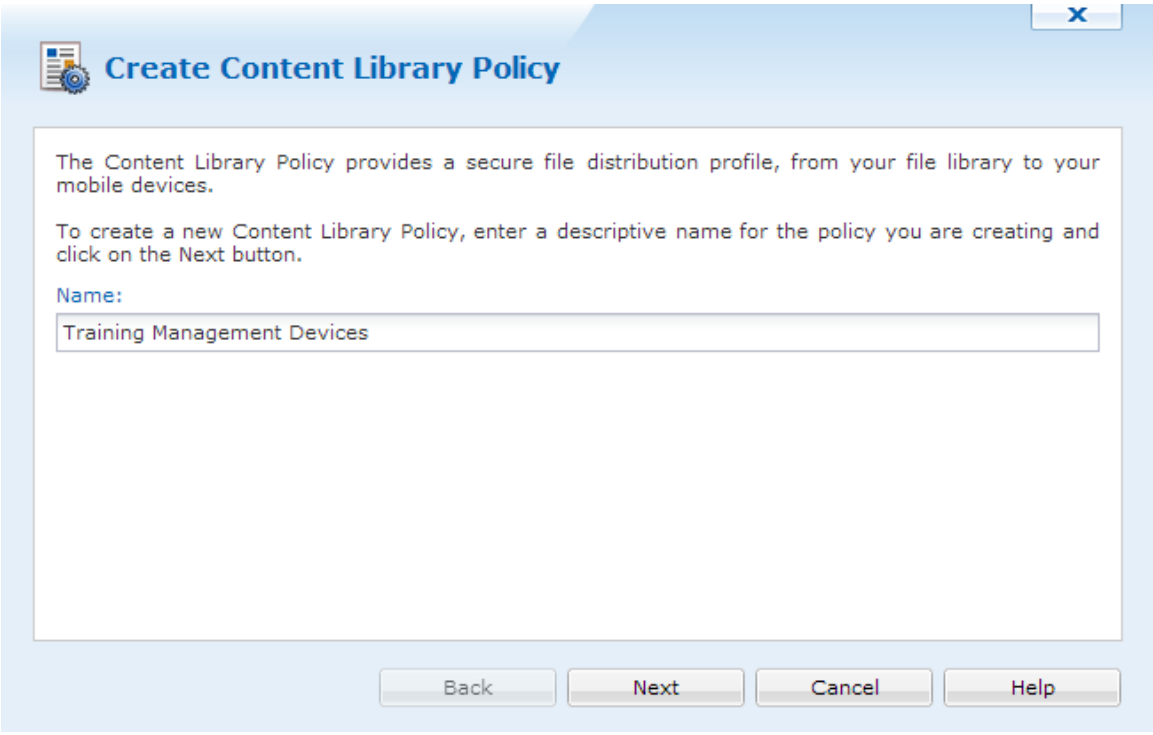
After all properties have been set, click Finish. The files are now uploaded to the MobiControlDeployment Server.

Content Library Policy

The Content Library Policy provides a secure file distribution profile, from the file library to mobile devices.. We can create as many policies as needed. To create a new Content Library Policy, click Add.

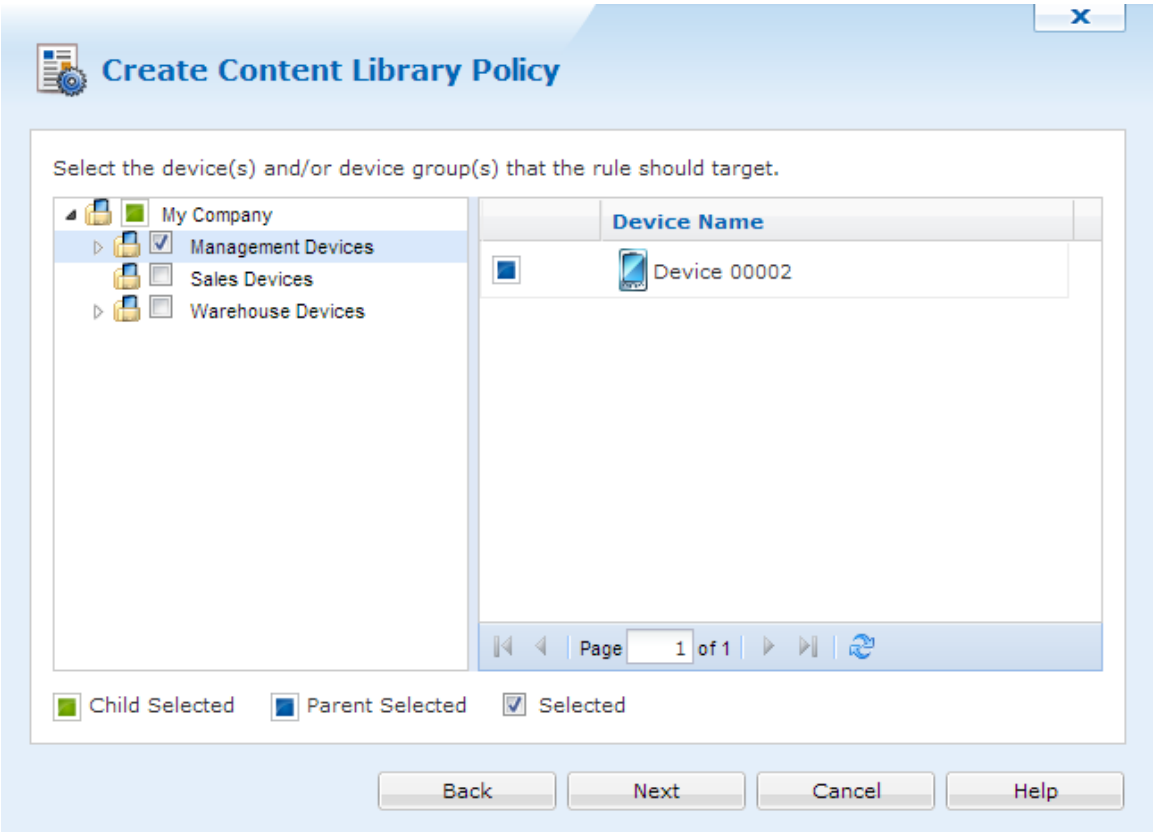
Create Content Library Policy

When we clicked Add, the Create Content Library Policy dialog appeared. In the first panel, enter a name, then click Next.

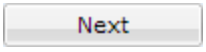


Create Content Library Policy

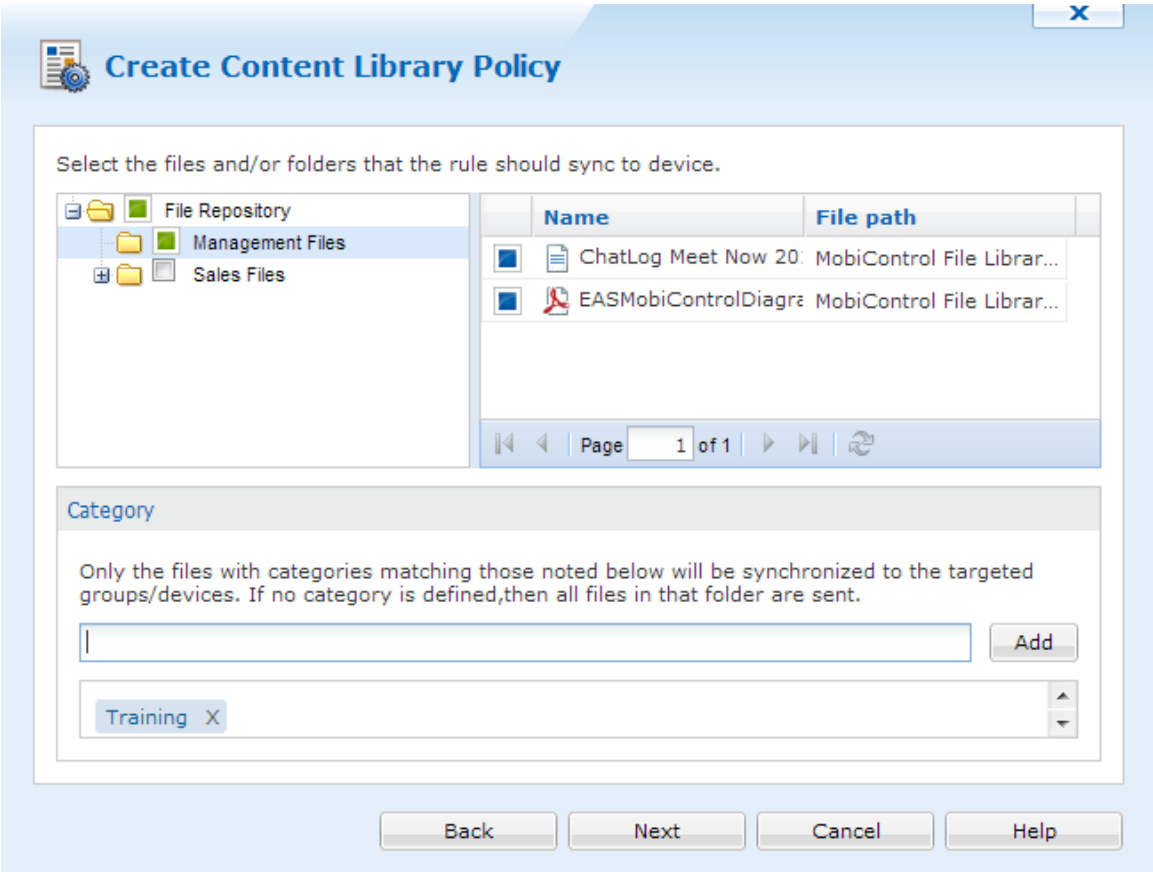
On the next panel, we can select which devices or groups will receive these files.



Select devices and groups

Click  to advanced to the next panel.

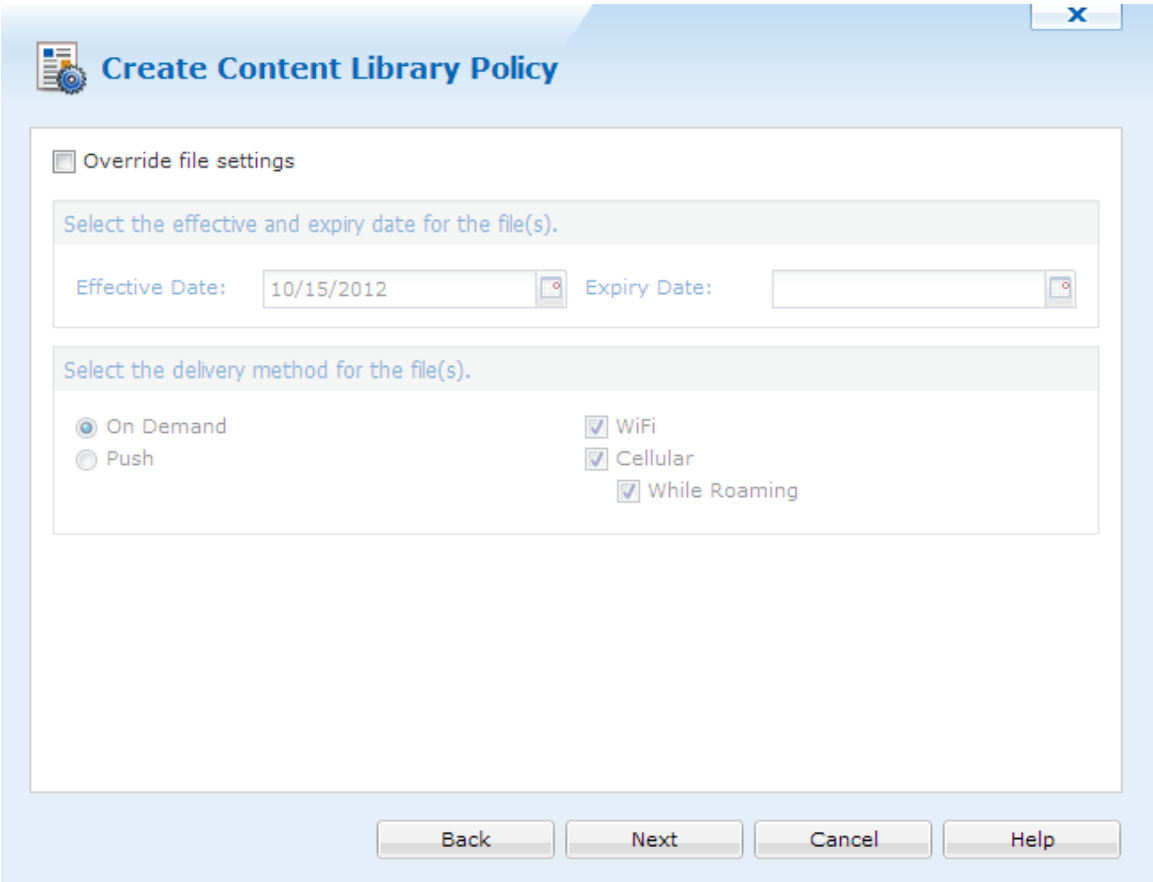
On this panel we are able to select which files are going to be accessible on the devices. If categories were made before, we can just type a category and all files with that tag will be selected.



Source Files

After the files are selected, click Next.

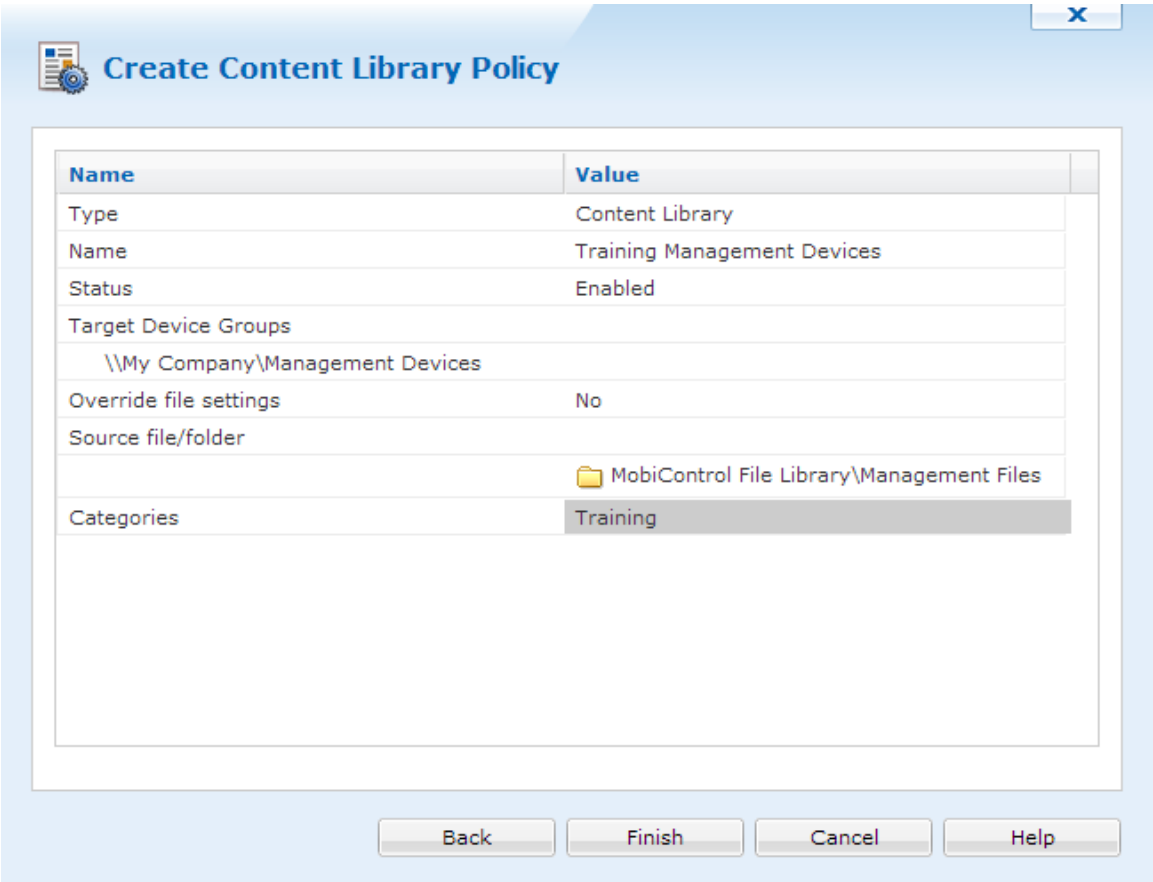
The next panel will allow us to override the file settings. If these settings need to be set, click the Override file settings checkbox.



Override File settings

Once the settings have been set, click Next.

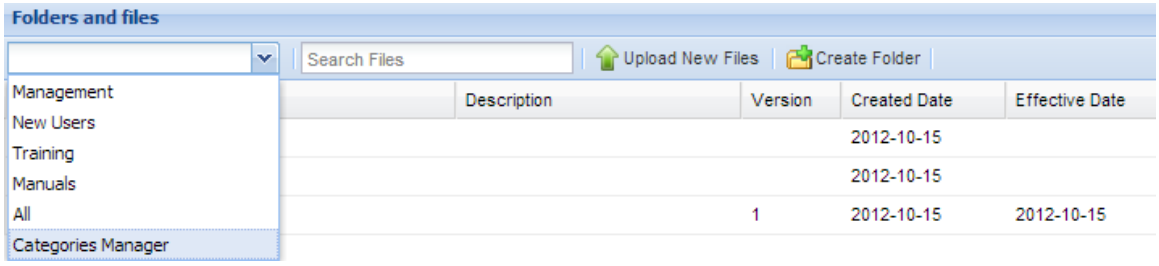
The final panel will show us a summary, click Finish to save and create this policy.



Content Library Policy summary

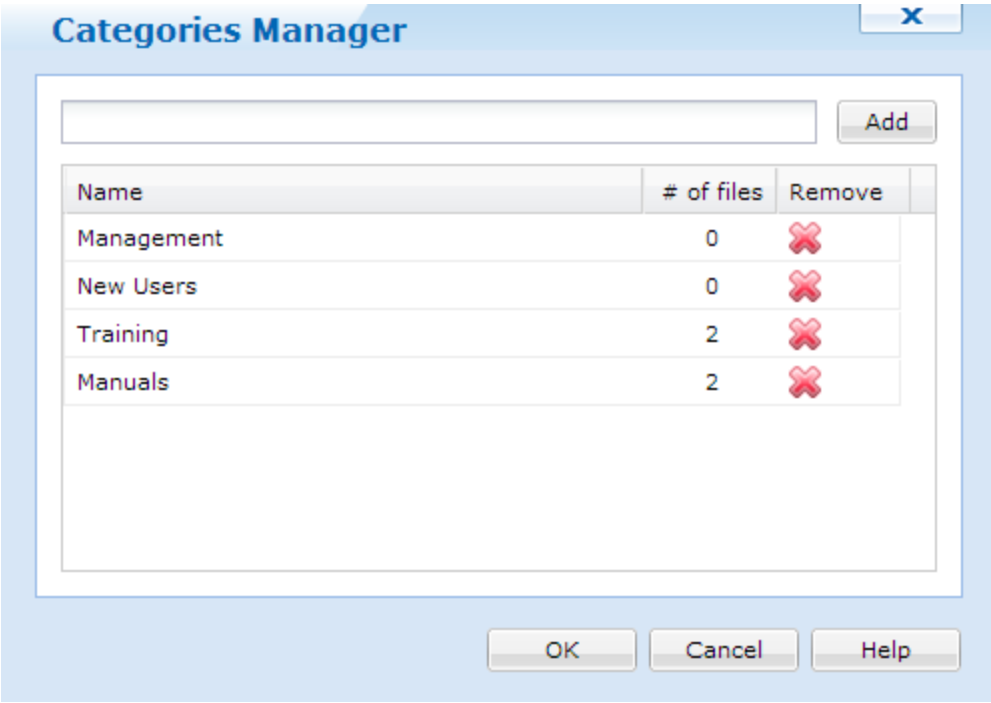
Categories Manager

To gain access to the category manager, click the drop box and select Categories Manager. This drop down list is located in the Folders and Files panel.



Categories Manager selection

Once selected, the Categories Manager dialog will open. Here we can delete previously created categories, and create new ones. We can also see how many files a category was tagged in.



Categories Manager

File Context Menu

When files have been uploaded to the Secure Content Library we are given additional options when we right click a file. Please see the "Secure Content Library - File Context" topic on page 1465 for more information.

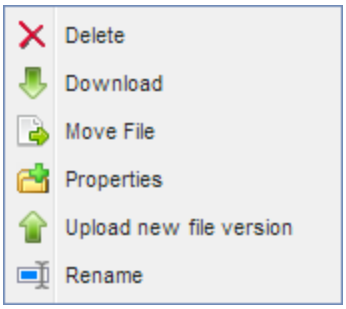
Secure Content Library

File Context Menu

When files have been uploaded to the Secure Content Library we are given additional options when we right click a file.

These options include:

- Delete
- Download
- Move File
- Properties
- Upload a new file version
- Rename

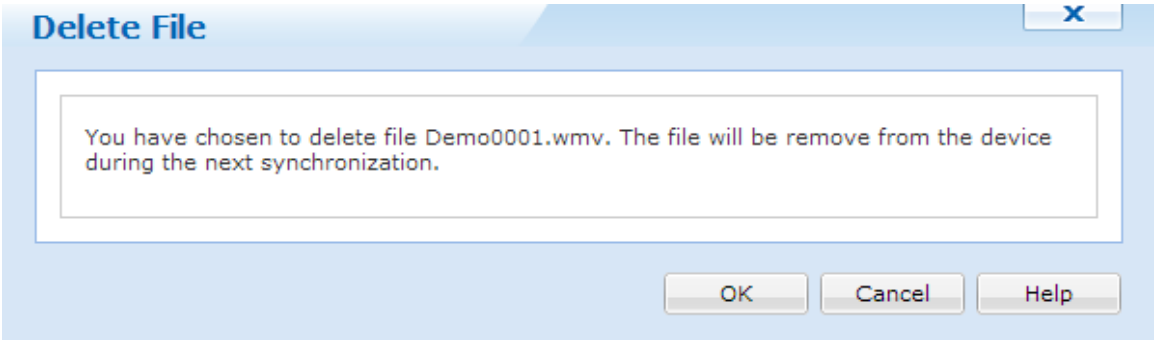


File Context Menu

Delete

Selecting delete will delete the file from the Secure Content Library. A confirmation dialog will appear asking for confirmation.

When a file is deleted from the Secure Content Library and it was already pushed to devices, the file will be removed from devices on the next synchronization.



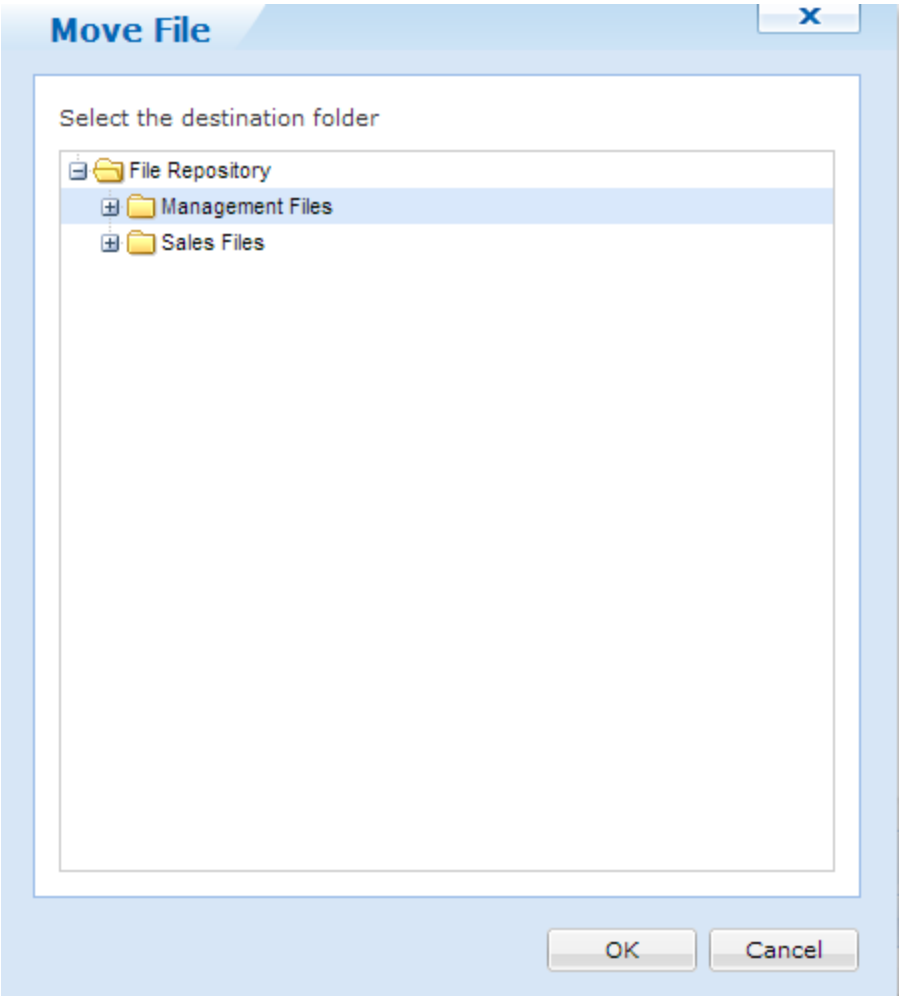
Delete dialog box

Download

Selecting download will download the selected file into the default download directory for your browser.

Move File

Selecting Move File will allow us to move the selected file to a different folder in the content library.



Move File dialog

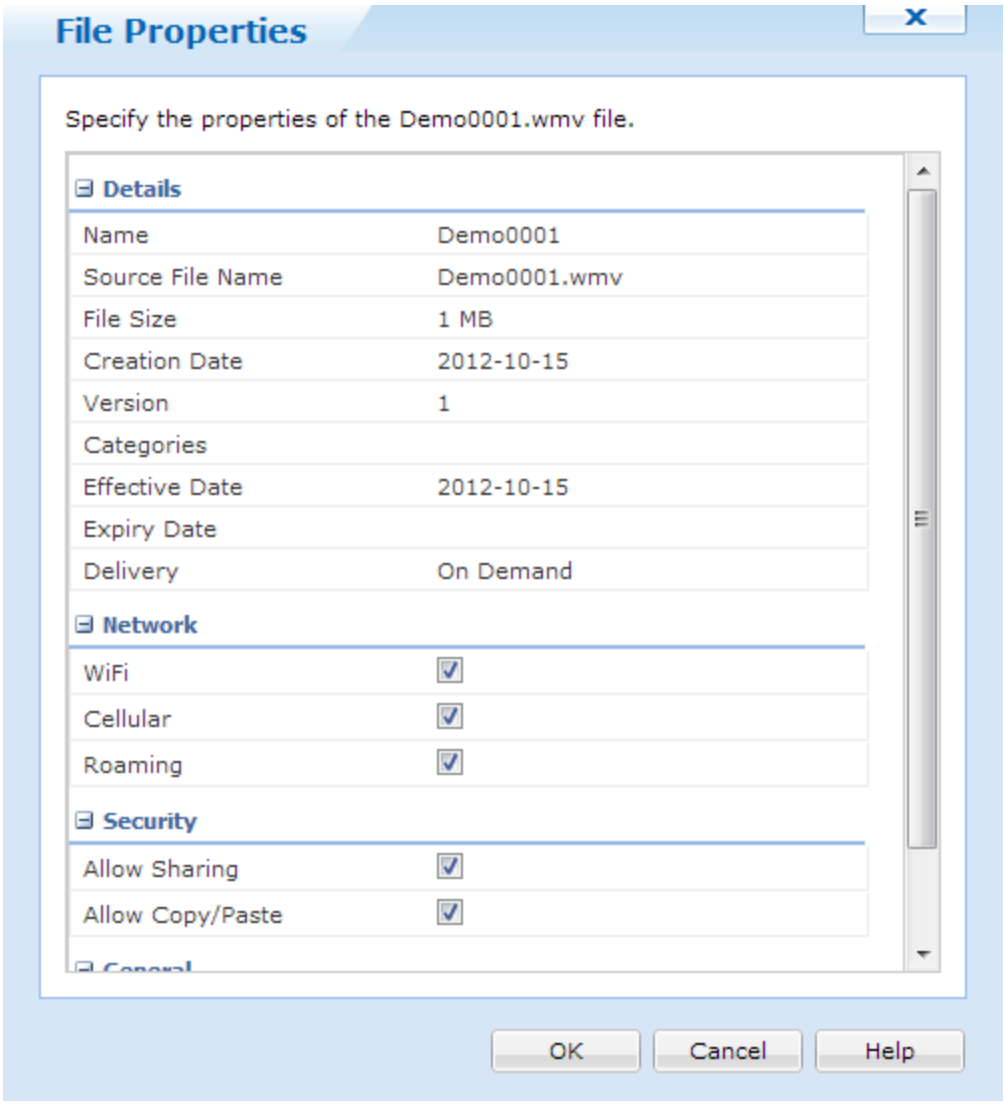
Properties

Clicking Properties will bring up the File Properties dialog. Here we can see all properties that is associated with this file.

Most of the settings here can be configured or edited.

NOTE:

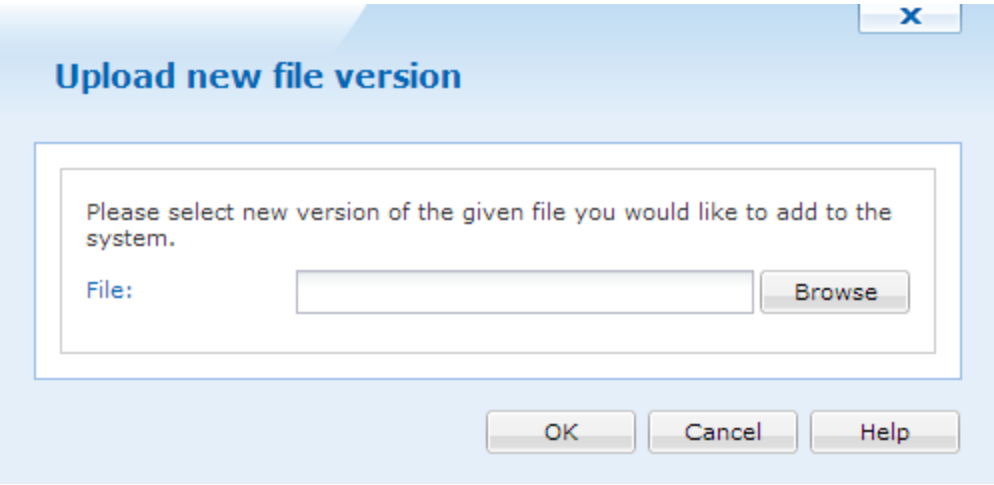
Security settings are only available for iOS devices.



File Properties

Upload new File Version

When we select the upload button, we are given the option to upload a new version of the specified file. When a new file version is uploaded, devices will be able to download the latest version.



Upload New File Version

Rename

Renaming allows us to change the display for the file type. This will not change the actual file name.

Android+ Device Tab

The list of devices currently certified to work with MobiControl's Android+ are as follows:

- **LG (VS950)**
- **Lenovo (ThinkPad)**
- **Pidion (BIP6000)**
- **Huawei (Springboard, MyTouch Q)**
- **Honeywell (7800)**
- **Motorola (ET1)**
- **ZTE (Optik V55)**
- **Any Samsung device running Android 2.3 or higher.**

The **Android+** tab enables you to access the devices connected to the deployment running a Google Android OS and Advanced MDM API's. All functions that affect this operating system are performed such as:

- Location Services
- Device Security
- Device Configuration
- Adding a Device

- Distributing software to a device
- Data collection functions
- Alerts

There are five views within the MobiControl web console. The views can be selected using the tabs at the bottom of the MobiControl Manager user interface.

- The **Devices view (tab)** allows users to view information about configured devices, for instance packages installed, device ID, and IP address. The Devices view (tab) also allows users to control and configure devices, for example, to remote control a device or to change a device's name.
- The **Rules view (tab)** allows users to view information about the configured rules. The Rules view (tab) also allows users to configure rules, for instance, create an add devices rule, a deployment rule, a file sync rule, an enable rule, or a disable rule.
- The **Packages view (tab)** allows users to view information about packages, for instance the packages currently configured or a list of devices onto which a certain package has been installed. The Packages view (tab) also allows users to configure package-related information, for example to add or delete packages.
- The **Reports view (tab)** provides users with a set of reports containing detailed information about the operation of the system. Provided reports include: deployment rule execution summary report, device configuration rule execution summary report, and device activity report.

For more information about the Advanced MDM API's please contact your local Device Sales Representative.

Android+ Device Agent Installation Methods

Android Device Agent Installation Methods

The MobiControl Device Agent is the MobiControl software that is installed onto mobile devices. The Device Agent communicates with MobiControl Deployment Server(s) and carries out the instructions it receives from servers. Device Agents also provide reporting and real-time information to Deployment Servers.

Android Device Agent Installation from Samsung Apps (Samsung devices only)

1. Download the MobiControl Device Agent.
2. Once the Device Agent has been installed, enter the Enrollment ID provided when you create an add devices rule

Please see the "Adding Android+ Devices" topic on page 1389 for More information on creating an add devices rule.

Android Device Agent Installation from Google Play

1. Install the MobiControl Device Agent from Google Play by searching for MobiControl.
2. Once the Device Agent has been installed, enter the Enrollment ID provided when you create an add devices rule.

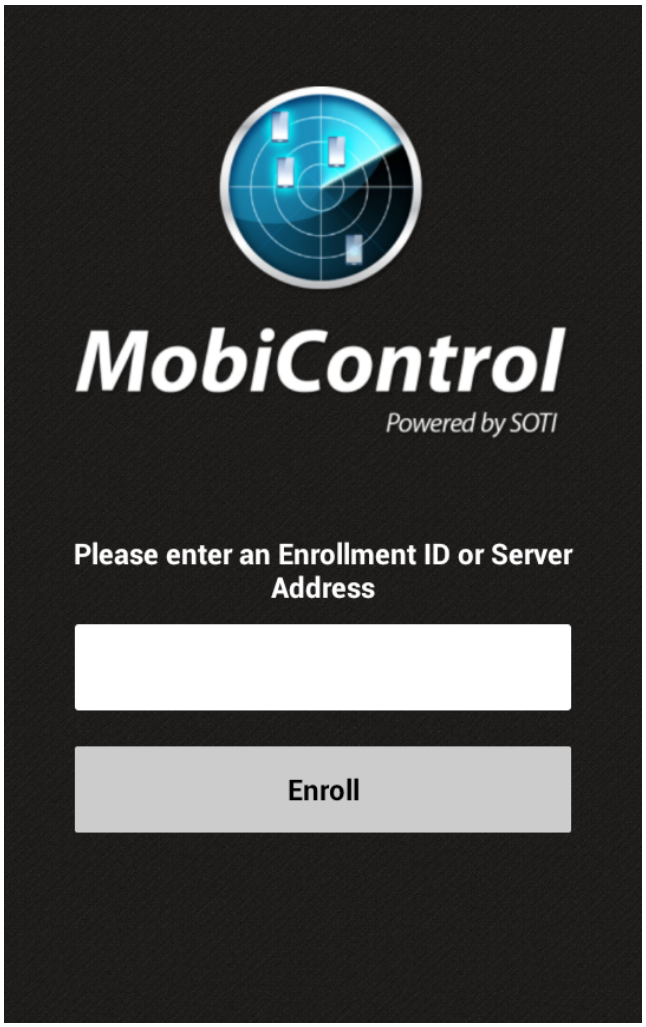
Please see the "Adding Android+ Devices" topic on page 1389 for More information on creating an add devices rule.

Android Device Agent Installation from Internal/External SD Card

1. Create an Add Devices Rule. Please see the "Adding Android+ Devices" topic on page 1389 for more information on creating an Add Devices rule.
2. Download the .APK by right clicking on the Add Device Rule that was created and select **Download Device Agent**.
3. Download the .APK file and the MCSetup.ini and place them both in the root of the SD Card or in the Downloads folder.
4. Ensure that your device can install applications that did not come from Google Play. To do this, go to your device settings, select security and check off **Unknown Sources**.
5. From the device, using a file browser, navigate to the SD Card and select the APK to install it.

When using the MCSetup.ini the user will not be required to enter an enrollment ID as this information is stored within the .ini file.

Device Agent Configuration Applet



Once installed on the Android Device the Device Agent enables the user to connect or disconnect from the Deployment Server Server, as well as view the Application Catalog. Please see the "Android+ Device Agent" topic on the next page for more information on the Android+ Device Agent.

Android Device Agent Uninstallation

The MobiControl Device Agent is installed on the device as a "Device Administrator", first step in uninstalling the Device Agent is to remove the agent as the "Device Administrator".

To remove the Device Agent as the "Device Administrator" and to uninstall the app, please follow these steps:

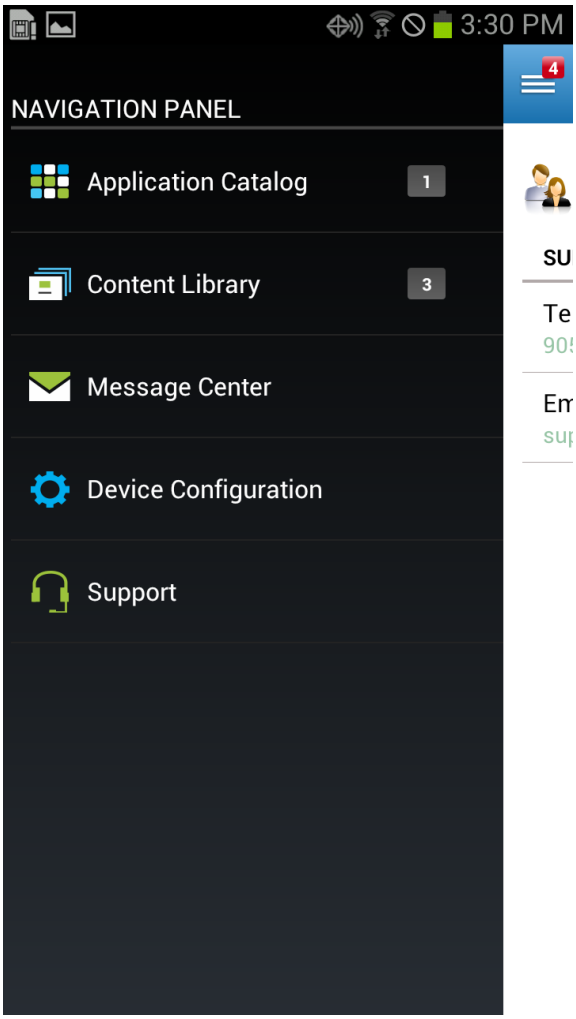
1. Go to your device settings and select **Security**.
2. Once in the Security settings, select **Device administrators**.
3. **Uncheck MobiControl**, this deactivates MobiControl as being a device administrator.
4. Once MobiControl has been deactivated , the app can be uninstalled like every Android app.
5. Go back to Settings and select **Applications**, select MobiControl and uninstall the application.

Android+ Device Agent

Opening the Device Agent will allow us to gain access to specific components of MobiControl. For the AndroidDevice Agent these components will be:

- Application Catalog
- Content Library
- Message Center
- Device Configuration
- Support

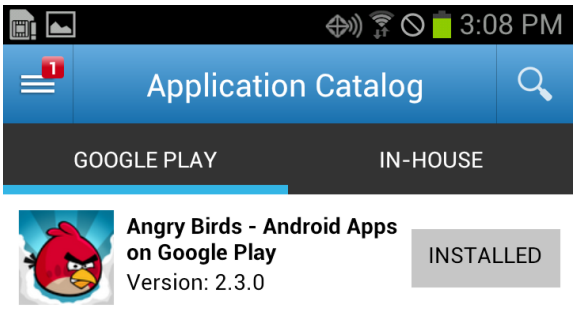
Tapping the menu button will show all these components on the left hand side.



Device Menu

Application Catalog

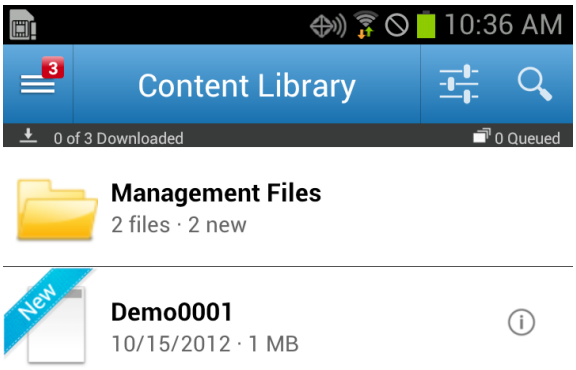
The application catalog menu will show the available applications, (App Store and Enterprise), that the device is able to download. Please see the "Android+ Application Catalog" topic on page 1403 for more information.



Application Catalog

Content Library

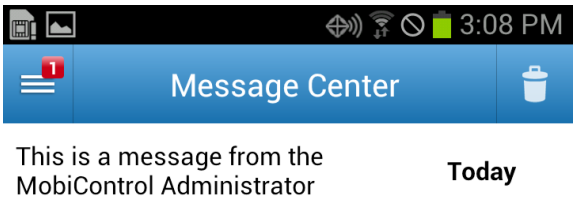
The content library tab will show all files that are available for download from MobiControl. Please see the "Secure Content Library Tab" topic on page 1456 for more information.



Content Library

Message Center

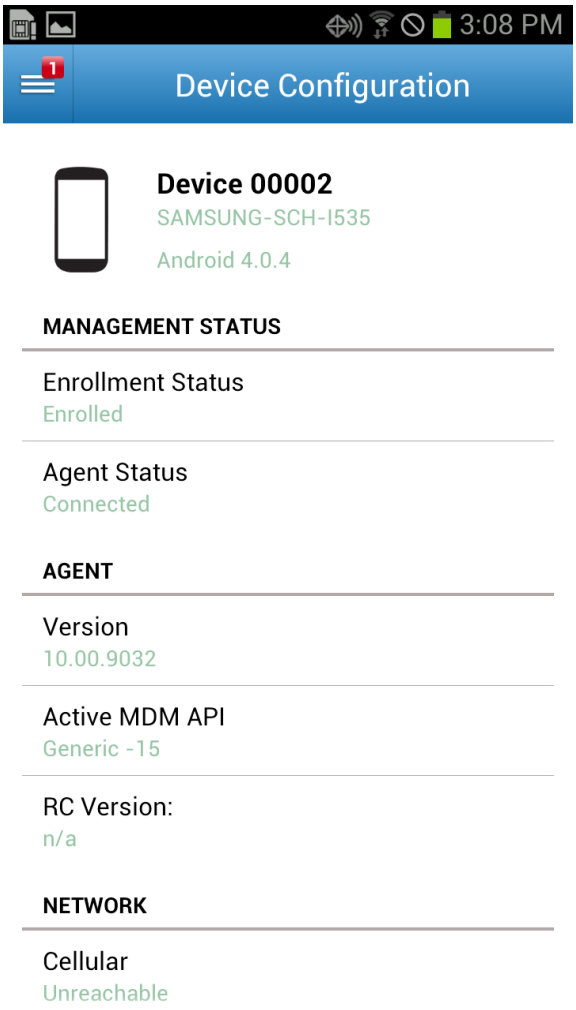
The message center will store all messages that were sent from MobiControl administrators. Users can tap each message to see the whole message.



Message Center

Device Configuration

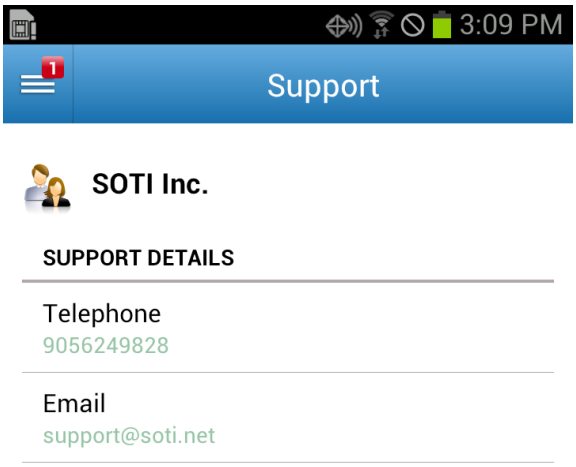
The device configuration menu shows all available information for the device. This includes the model type, Android version, enrollment status and other bits of information.



Device Configuration

Support

The support menu will show the items that were configured from the MobiControl web console. When a user taps either the phone or email items, it will open the respective application to complete the action. For example, tapping the phone item will open up the phone application. Please see the "Android+ Support Contacts Info" topic on page 1356 for more information.



Support

Android+ Devices Tab

The Devices view (tab) is the main view into the status of the devices in the MobiControl system.

Device Tree

The device tree provides a structured view of the devices in the system. The group structure is easily defined by the user by creating new groups and dragging and dropping devices between groups.

Commonly-reported device information can be easily referenced in the device tree window by right-clicking in any open space in the device tree window and selecting the information that you would like to see displayed.

Devices are added to the system by defining an add device rule and creating a MobiControl Device Agent that is installed on the device. Please see the "Adding Android+ Devices" topic on page 1389 for a detailed explanation of how to add devices to MobiControl.

Info Panel

The Info panel provides detailed status information about the group or device that is selected in the device tree. When a group is selected, the displayed information includes the number of subgroups and how many unique, online, offline, or disabled devices are in the group. For devices, the displayed information includes device ID, IP address, battery and memory status.

The content displayed in this panel is stored in the MobiControl database. This information is refreshed when a device establishes a new connection to the MobiControl Deployment Server, and when you click **Refresh** or press F5 on this tab.

Logs Panel

The Logs panel provides a listing of the events occurring in the MobiControl system. This listing is filtered based on the group or device that is selected in the device tree. If only one device is selected, only the events related to that device are displayed. If a group is selected, events for the group and all the devices that belong to that group are displayed.

You have the option to show or hide logging, adjust the maximum number of logs displayed, and the frequency with which the Manager should refresh the log view.

Update Schedule Panel

The Update Schedule panel lists the dates and times when the device is programmed to query the MobiControl system to check for updates. By default, a device will also check for updates whenever it connects to the MobiControl system. Please see the "Android+ Device Update Schedule" topic on page 1359 for more information.

Installed Applications Panel

The Programs panel lists the applications that are installed on the device that is selected in the device tree. This is the same listing that is displayed by the **Manage Application** applet provided by the Android operating system. You can also remove the installed app, view its properties and wipe the app data.

When the app is removed this way, it is silently uninstalled and the user would never be prompted about the uninstall.

The app properties option shows if the app is currently running on the device and whether it is being managed by MobiControl through the app catalog. Please see the "Android+ Application Catalog" topic on page 1403 for more information about the Application Catalog .

Wiping app data will remove all data that is used by the app. For example, when a device is being used by multiple users and it has a email application on it, if you wipe the data from the email app it removes all previous user settings and storage.

Rules Assigned Panel

The Rules Assigned panel lists the file sync rule and Application catalog rules assigned to the group or device that is selected in the device tree. Rules are inherited from parent groups; a rule will apply to a device if it belongs to group to which the rule has been assigned.

The assignment of rules to groups provides a flexible and convenient means for easily configuring devices. For example, once you have set up your rules for software or data distribution, you can automatically provision your devices by simply adding them to the appropriate group within the device tree. Please see the "Android+ Rules Tab" topic on page 1386 for information on creating deployment rules and file sync rules.

Notes Panel

The Notes panel lists the notes that are associated with the selected device. If a group is selected in the device tree, all the notes for the devices that belong to the group are listed. Notes are a convenient way to maintain information about the device such as trouble tickets. Please see the "Device Notes" topic on page 1384 for information on creating device notes.

Packages Panel

The Packages panel lists the packages that are configured on the device that is selected in the device tree. The assignment of packages is directly based on the assigned rules. This panel provides a status column which indicates the state of the package for that device. For example, the status "Pending" indicates that the package has been queued and its installation on the device is pending.

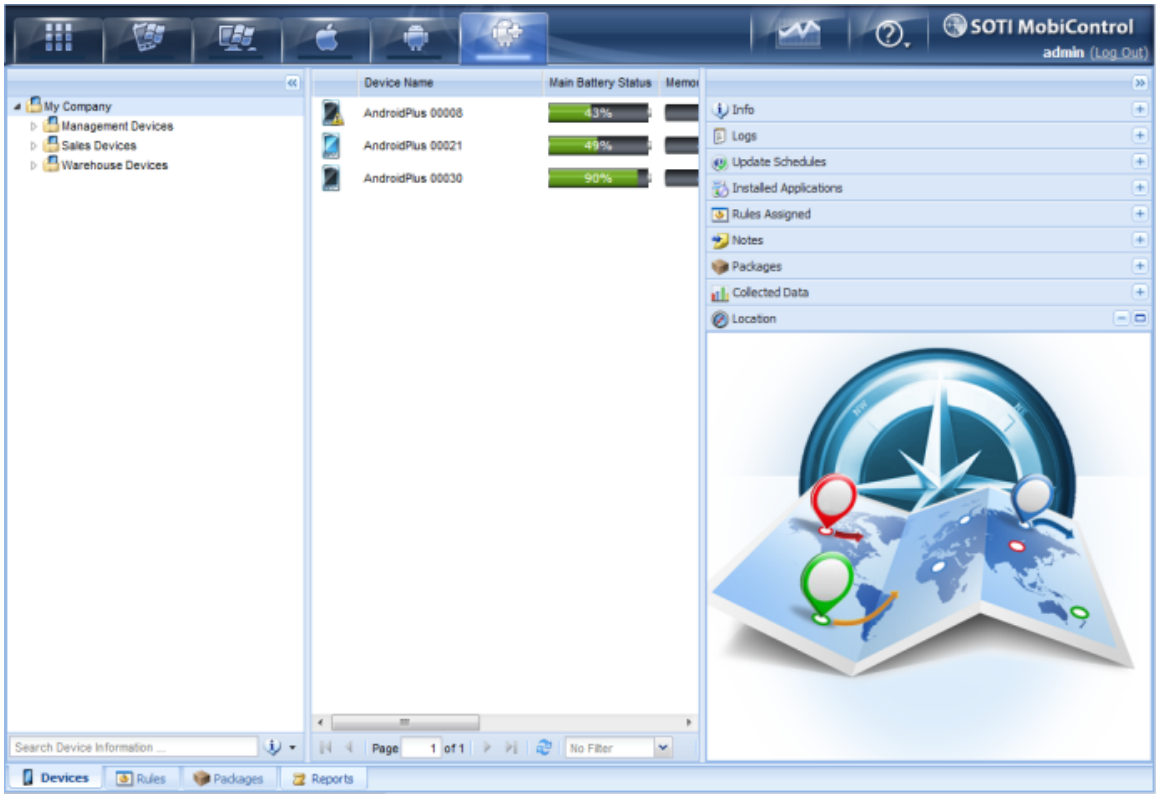
You can force the re-installation of a package on a given device by right-clicking on the package in the Package Panel and selecting **Force Package Reinstall on Next Schedule** or **Force Package Reinstall Now.**

Collected Data Panel

The Data Collection Panel allows you to view the collected historical data for a set of devices. By creating a Data Collection Rule you will be able to specify which items to collect data from, how often to collect them, and when to upload the collected data to the server. Please see the Creating Data Collection Rules page for information on creating Data Collection.

Location Panel

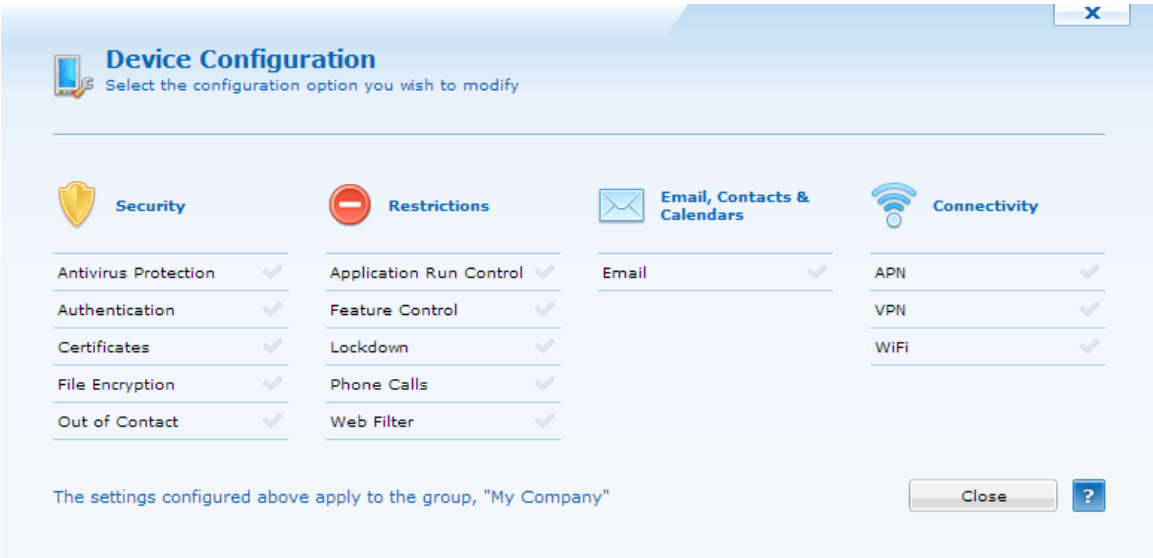
The Location Panel gives the ability to locate, track and gather information on the movement of your GPS enabled devices, no matter where they are in the world which is powered by Microsoft's Bing maps technology. Whether you need to confirm the current location of a particular field-worker, track the progress of an important shipment or collect historical information on the movement of a group of devices or vehicles in order to analyze performance, MobiControl's Location Services can help. Please see the Location Services page for more information.



Android Devices Tab - Devices view (tab)

Android+ Device Configuration

MobiControl offers several device configuration options ranging from password authentication, user interface lockdown (also known as "kiosk"), and the ability to configure the device to automatically react to security threats such as repeated failed login attempts, even if the device is out-of-contact or in an offline state.



Android+ Device Configuration dialog box

MobiControl's security provides powerful features for configuring devices and mobile data, while maximizing usability and making configuration implementation easy, efficient and cost-effective. Salient features of MobiControl's security include:

- Over-the-Air (OTA) security policy distribution
- Policies can be assigned at the individual device, group or global level
- Configuration managed for both online (connected) and offline (disconnected) devices

To access Android Device Configurations, select the device or group of devices for which you want to configure security and then click **Device,** click **Configure Devices,** and click **Security.**

Security

Restrictions

Email, Contacts & Calendars

Connectivity

Android+ Antivirus Protection

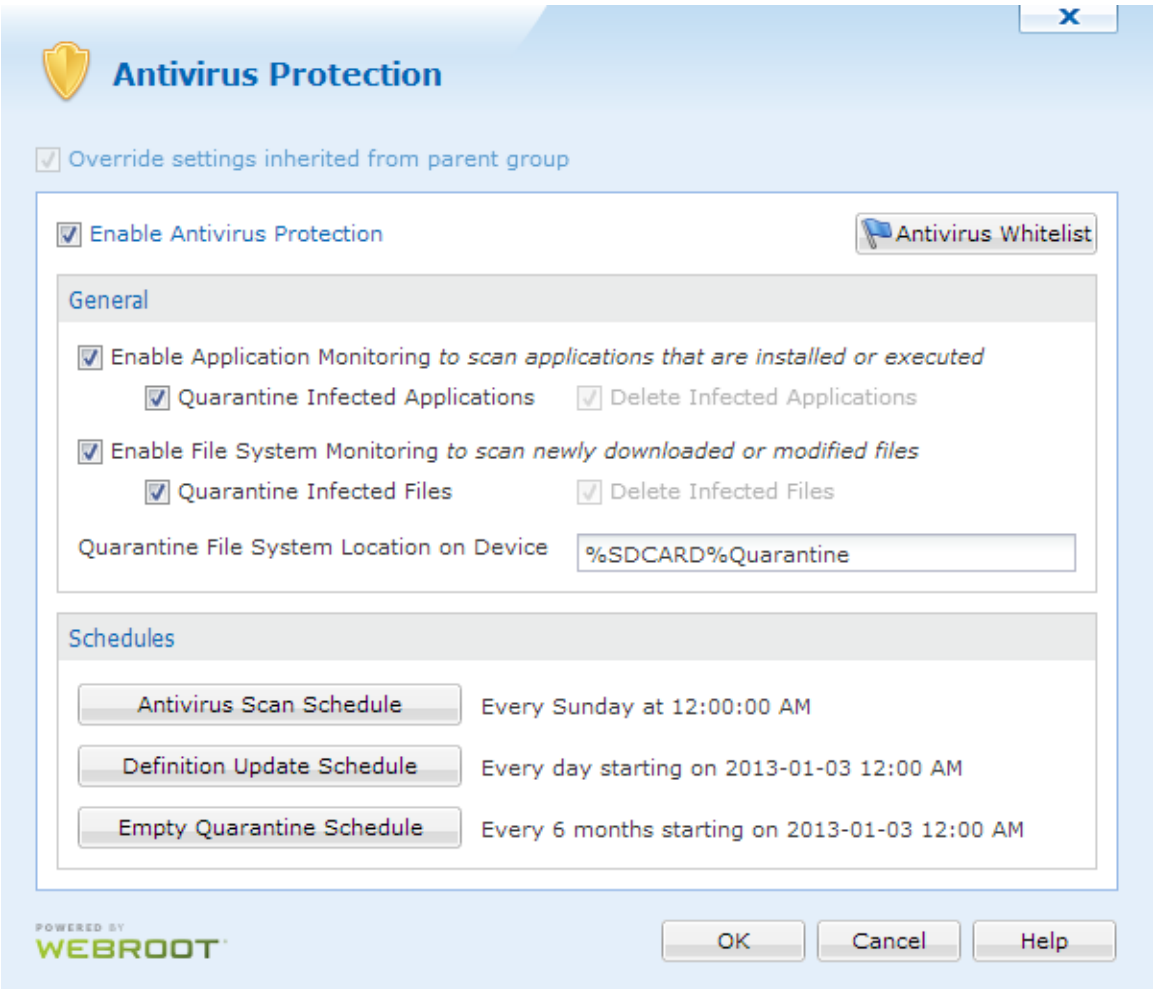
MobiControl's Antivirus protection policy allows us to monitor files and applications on devices. Scans can be configured from every 2 minutes to as much as once a month.

This is done by scanning apps and files against virus definitions, very similar to a Windows desktop antivirus application. Virus definition updates can also be configured to download new definitions based on a schedule.

When an infected file or app is found on the device, MobiControlhas an option to move these files to a special folder on the device's SD card. When it is moved to the folder, it is then deleted from the Android system. This folder can be configured to anywhere that is desired. When infected files or apps are in this folder, we can see a list of all quarantined items in the Web Console.

If a certain application is quarantined by mistake, we can create a whitelist to halt any further quarantines of the application or file.

Click **Enable Antivirus Protection** to enable this feature.



Android Antivirus Protection.

General Settings

If **Enable Application Monitoring to scan applications that are installed or executed** is selected, then MobiControl's Antivirus protection will monitor any applications that are installed. Also, if an application is launched, it will again be scanned. Having **Quarantine Infected Applications** checked will allow MobiControl to move the infected application to the quarantine folder specified.

If **Enable File System Monitoring to scan newly downloaded or modified files** is selected, then any file that is downloaded or modified will be scanned for viruses. If they are infected, they will be moved to the quarantine folder specified.

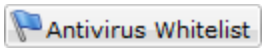
It is recommended to leave the quarantine folder as the default, but it can be changed to any folder needed.

Schedule settings

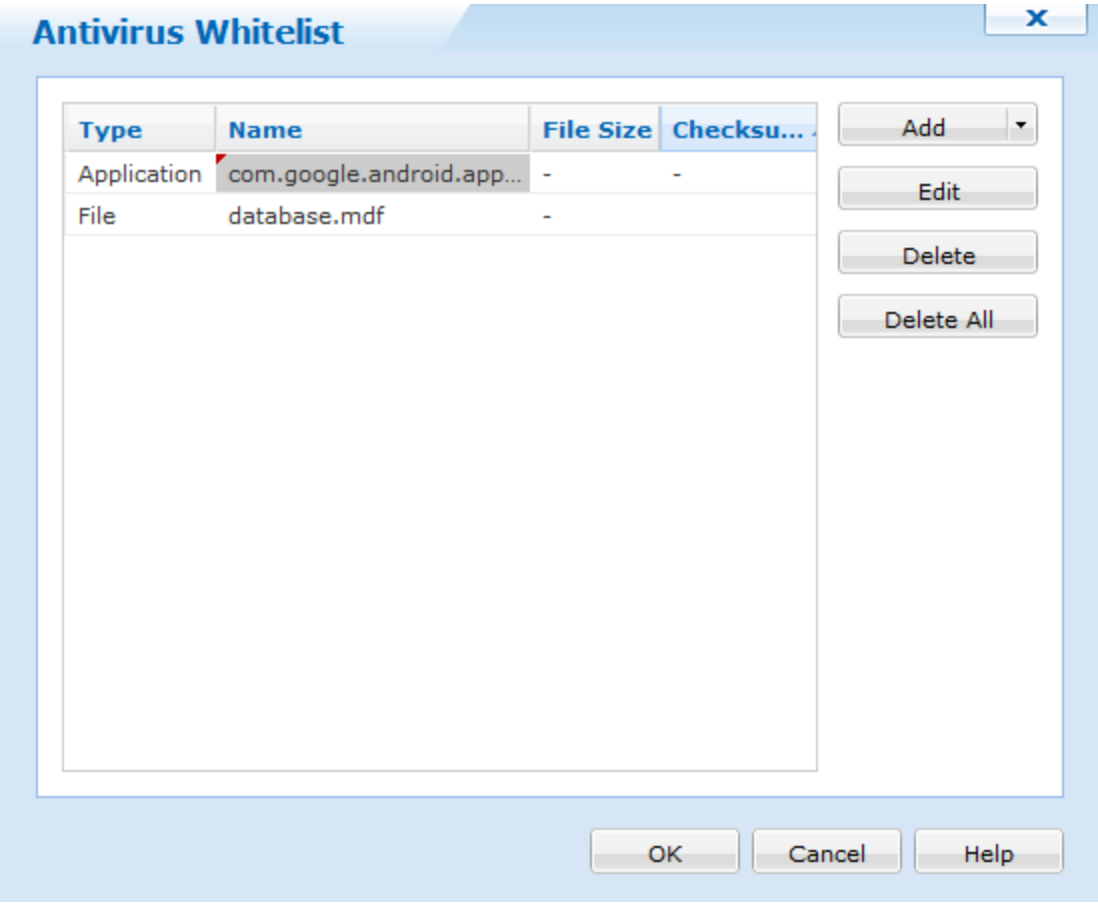
Clicking each of the scheduling buttons allows us to change the frequency of when they are active.

- **Antivirus Scan Schedule**
- **Definition Update Schedule**
- **Empty Quarantine Schedule**

Antivirus Whitelist

The Antivirus Whitelist allows us to exclude certain applications or files from the virus scans. This can be done by clicking the 

button. From here we can specify which applications or files are going to be excluded.



Antivirus Whitelist

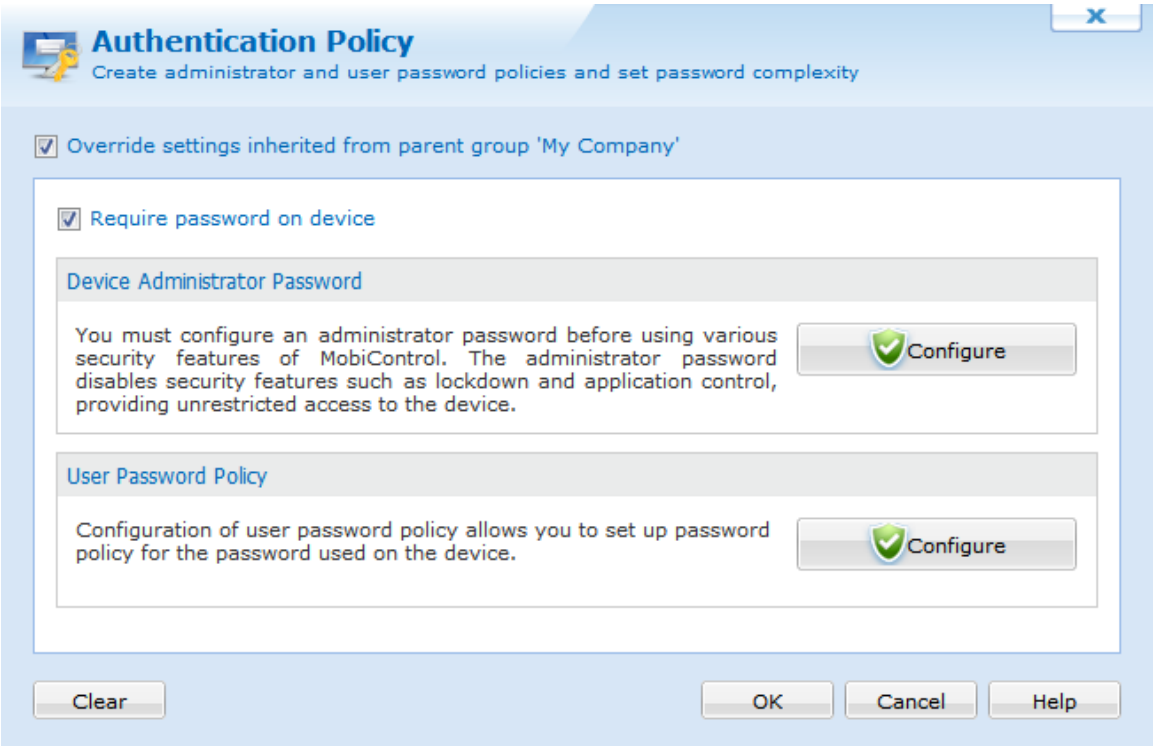
Configuring the Antivirus Whitelist

After all configurations are done, click OK to apply the configurations.

Android+ Authentication

The Authentication Policy option in the **MobiControl Security Center** dialog box allows administrators to manage device-side, password-based user authentication.

To enable Authentication Security for a device or group of devices, select **Authentication Policy** from the MobiControl Security Center. (Please see the "Android+ Device Configuration" topic on page 1292.)



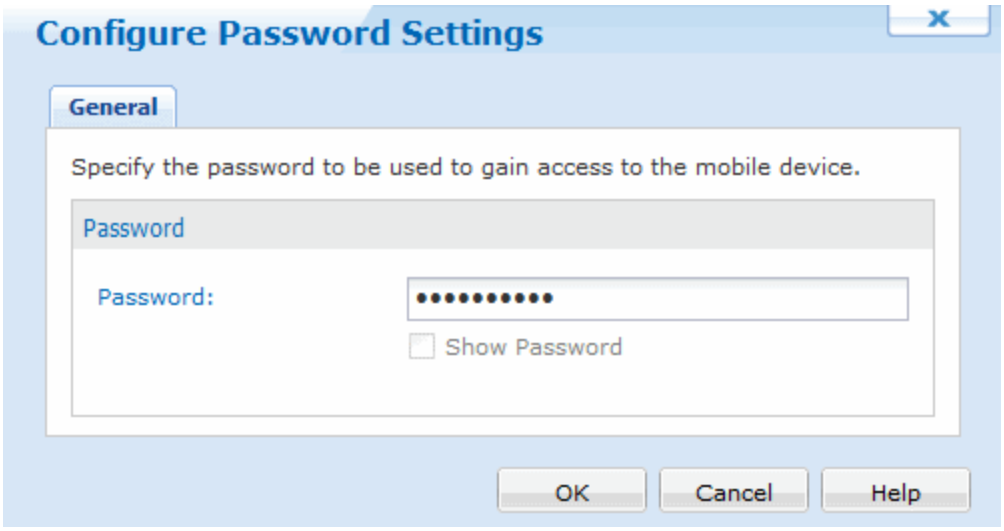
Device Authentication Configuration dialog box

Administrators can configure an administrator password and a user password. When the administrator password is entered, the device is unlocked so that the administrator has complete access to the device. When a user password is entered, the user will have access to only those programs that the administrator has configured. An administrator can allow users to run all programs or only specific programs. Please see the "Android+ Device Lockdown" topic on page 1312 and "Android+ Application Run Control" topic on page 1307 for more details.

Field Name	Description
Device Administrator Password	Configures the Administrator password for the Android+ devices.
User Password Policy	Configures the User password policy for the Android+ devices.

Device Administrator Password

To specify an administrator password, first ensure that the **Require password on device** box is checked, and then click the **Configure** button in the administrator password section. This will bring up the dialog box below. Enter the desired password in the two provided text boxes and click **OK**. The configuration of the Administrator password is a prerequisite for all the other security configurations. To get to this screen you must click on the **Options** button, then select **Administrator** and click **OK.**



Administrator password settings dialog box

Device User Password

To specify a user password, first ensure that a **Device Administrator Password** has been setup, and then click the **Configure** button in the use password policy section. This will bring up the dialog box below. Enter the desired password policy configuration in the provided sections, as displayed below, and then **OK**.

User password policy settings dialog box

Complexity Requirements

To configure a user password, first ensure that the **Enable Password Authentication** box is checked. The **Complexity** dialog box allows you to specify the password complexity requirements for the user password on the Android device.

Field Name	Description
Minimum Password Length	Specify how long the user password must be on the Android Device.
Minimum Password Quality	Specify the password quality by requiring Numbers, Letters, or Number and Letters.
Minimum number of complex characters allowed	Specify how many special characters are required for the user password.

History

The **History** dialog box allows you to specify the password history requirements for the user password on the Android device.

Field Name	Description
Maximum password age	Specify how long the user password can be used on the Android device before it must be changed.
Number of unique passwords before reuse	Specify how many passwords will be remembered until the user can use that password again.

Policy

The **Policy** dialog box allows you to specify the password policy requirements for the user password on the Android device.

Field Name	Description
Time lapse before device auto-locks	Specify how long the device will stay unlocked while off. The device will automatically lock again after the expired time.
Maximum number of failed password attempts before device wipe.	Specify how many times an incorrect password can be entered on the device before it automatically wipes itself.

Android+ Certificates

With MobiControl's certificate policy, we are able to install certificates on devices on behalf of authenticated users or devices.

To get here, right click a device/device group, and select Device Configuration. Once the Device Configuration window appears, click **Certificates**.

Here, we are able to upload certificates, or generate new ones based on Templates.

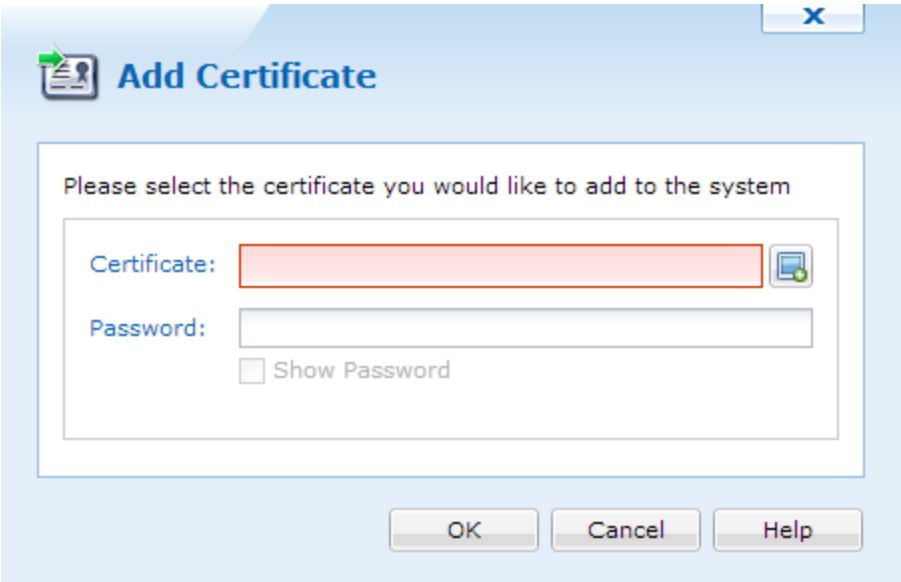
NOTE:

To set up certificate templates, Certificate Authorities must be set up. Please see the Certificate Authorities page for more information.

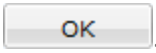
Certificates

Device Configuration - Certificates

When the Certificates window is open, we can upload new certificates by clicking New.



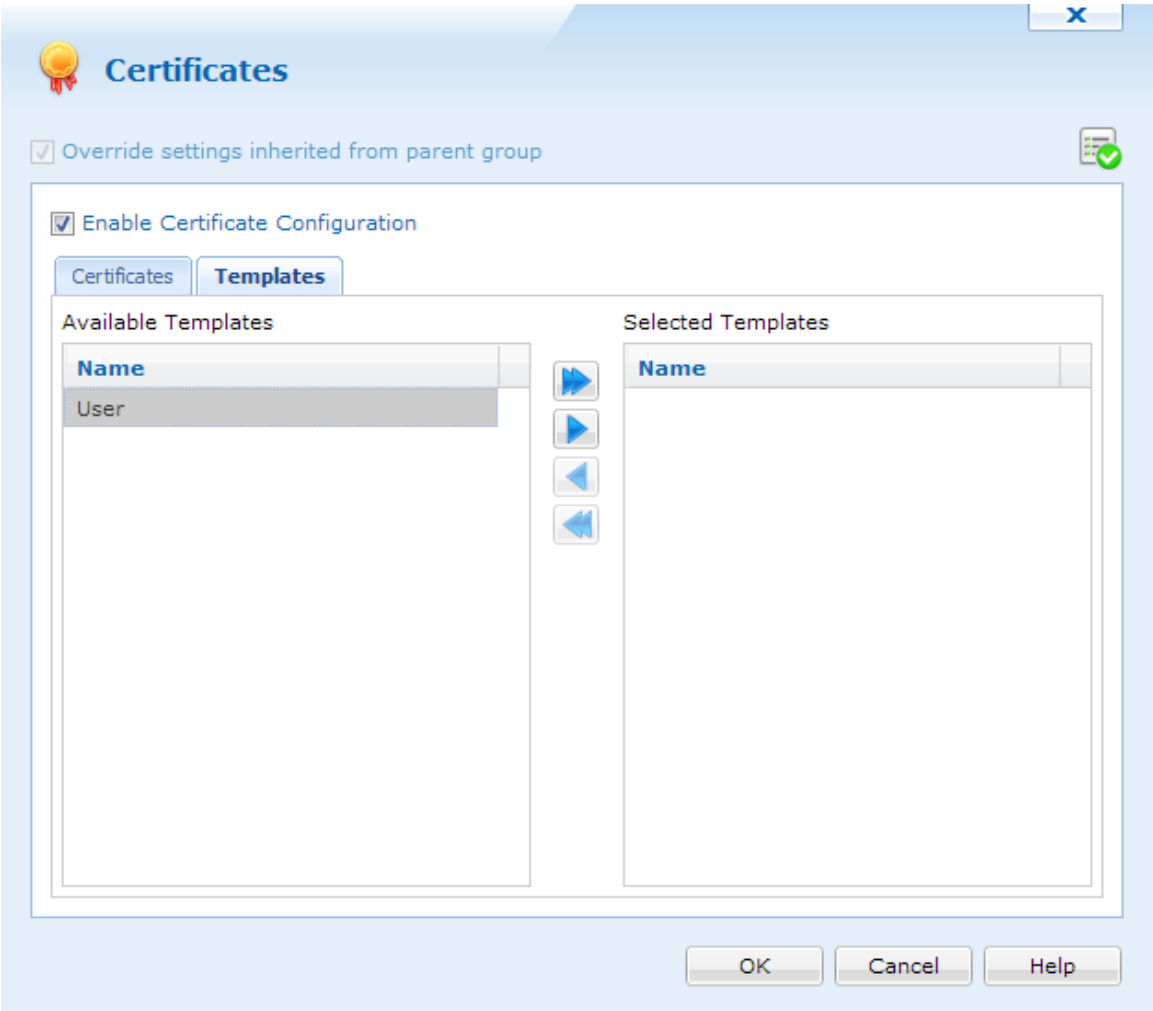
Adding new certificates

Click  to select a certificate. When uploaded, type the password associated with it, and click  .

When the certificate is added, we can select it and click any of the right arrows to move it to the *Select Certificates* panel. This will now install the certificate on the device or device group it is configured for.

Templates

Templates allows MobiControl to request a certificate on behalf of a user or device, and install it. This allows for dynamic certificates.



Selecting Certificate Templates

Certificate Templates are based off the templates configured in Certificate Authorities. Please see the Certificate Authorities page for more information about certificate templates.

When templates are configured, we can select one or many, and move it to the **Selected Template**s panel.

After all certificates have been selected, clicking OK, will close the window and apply the settings.

Android+ File Encryption

Due to the portable nature of data stored on mobile devices, there always exists the possibility of this data being found by someone other than the intended user. For instance, if a device is lost or stolen, sensitive business information (contacts, emails, spreadsheets, documents or other confidential data) may be found. Data can be easily retrieved from the device using a variety of file transfer methods (i.e. USB cradle, Bluetooth or Wi-Fi file transfer, or infrared beam).

MobiControl helps secure data stored on the mobile device and SD memory cards or storage media to help businesses achieve compliance with strict data storage and processing regulations. The file encryption feature allows encrypting data stored on a device or memory card so that it can not be accessed by an unauthorized person. This protects sensitive data if an attempt is made to extract it from the mobile device and access it on another mobile device, computer or data reader by an unauthorized person.

NOTE: SUPPORTED DEVICES

Only Android+ devices with Android 3.0+ are able to utilize file encryption.

File Encryption Policy dialog box

MobiControl's policy-based file encryption uses FIPS 140-2 validated AES-256 encryption algorithms to secure mobile data. On-the-fly file encryption is implemented easily and transparently without affecting the end users experience and allows data to be encrypted and decrypted in memory when needed by mobile applications on the device. MobiControl provides granular control allowing encryption of the devices external storage card or Internal Storage Card.

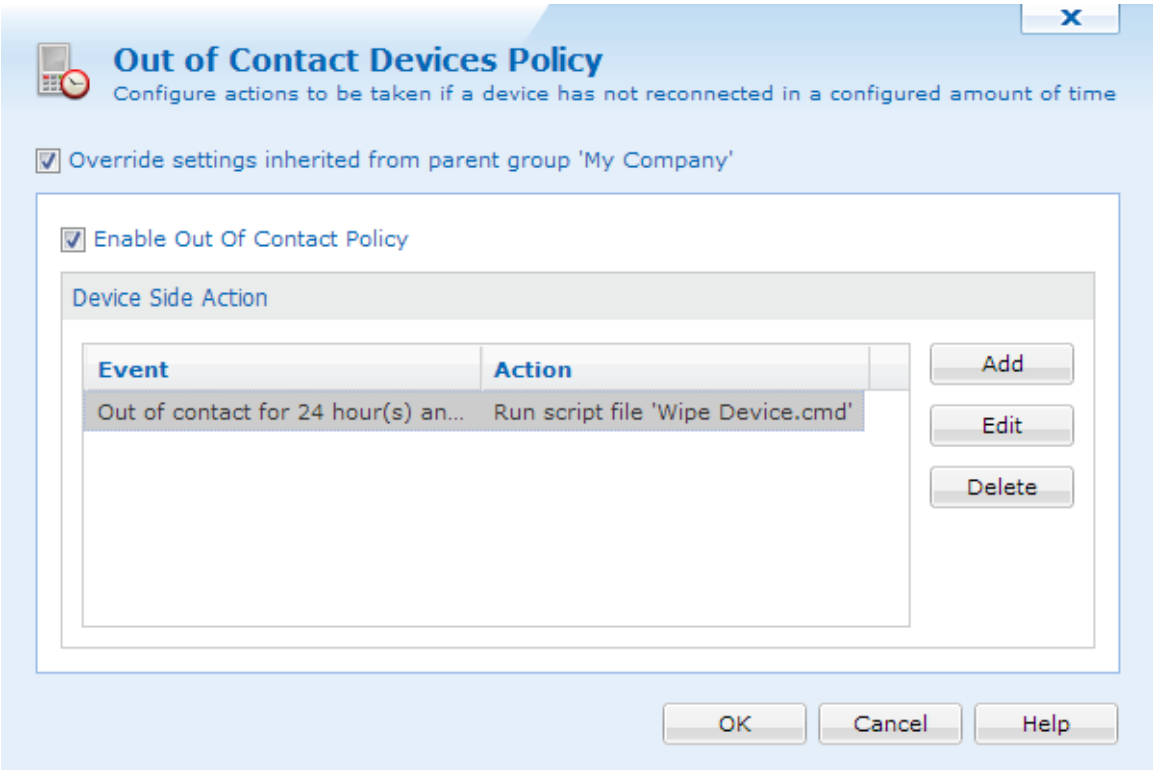
To enable file encryption for a device or group of devices, select **File Encryption Policy** from the MobiControl Security Center. User authentication must be enabled prior to enabling file encryption. (Please see the "Android+ Device Configuration" topic on page 1292 and "Android+ Authentication" topic on page 1296 for more information.)

Android+ Out of Contact Devices

The out-of-contact devices policy dialog box allows you to manage "out-of-contact" devices which are not able to connect to the MobiControl Deployment Server. This feature can be used to define security actions that can be triggered if a device has not contacted the MobiControl server for a specified time

interval, or has been lost or stolen and appears as offline in the device tree.

To enable the out-of-contact devices policy for a device or group of devices, select **Out of Contact Devices Policy** from the MobiControl Security Center. (Please see the "Android+ Device Configuration" topic on page 1292.)



Out of Contact Device Security Policy dialog box

EXAMPLE:

If a device does not contact the server for two days, you can configure it to be wiped to avoid losing any sensitive data on the device. Other actions and standard script commands can also be executed.

To add an event for which security actions can be specified, click the **Add** button. Click on the **Edit** button to modify an existing event or an action. Click on **Delete** to remove an event and its corresponding action from the list.

Action	Description
Add	To add an event for which security actions can be specified.
Edit	To modify an existing event or an action. Clicking this button presents the option to edit an action or the corresponding action.
Delete	To remove an event and its corresponding action from the list.

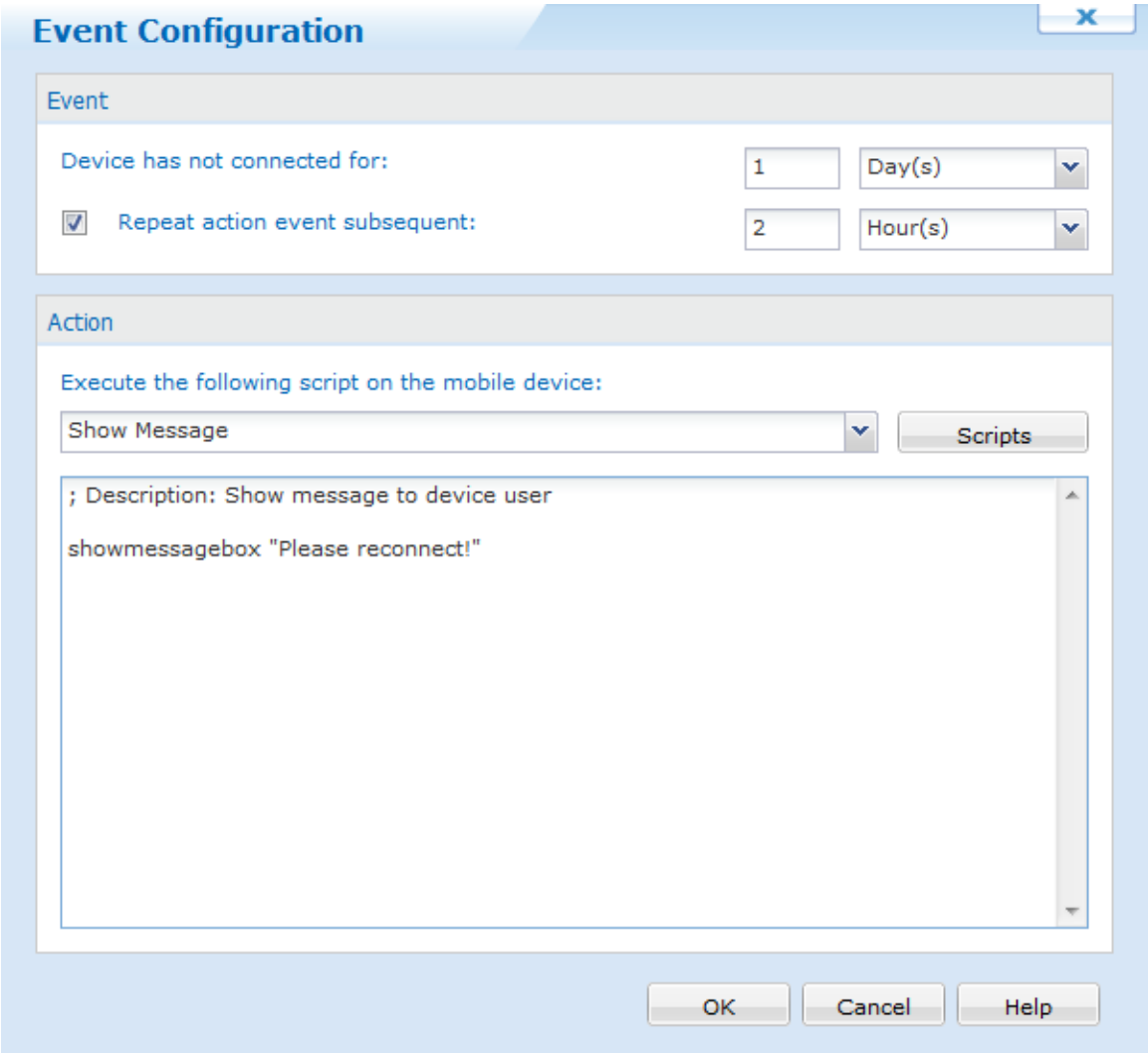
Add Event

To add an event, click the **Add** button to bring up the **Out of Contact Event Configuration** dialog box. Specify the time interval after which an action (or a script) should be triggered if the mobile device has not connected to the MobiControl Deployment Server (which is indicated by the device appearing as online in the device tree). This can be in minutes, hours, days or weeks.

If **repeat action event subsequent** is selected, actions can be repeated after the initial time out.

EXAMPLE:

If the out of contact policy is to be triggered if the device hasn't connected for 1 day, and repeat action event subsequent is configured for 2 hours, the out of contact policy action will be triggered every 2 hours after the initial trigger.



Out of Contact Event Configuration dialog box

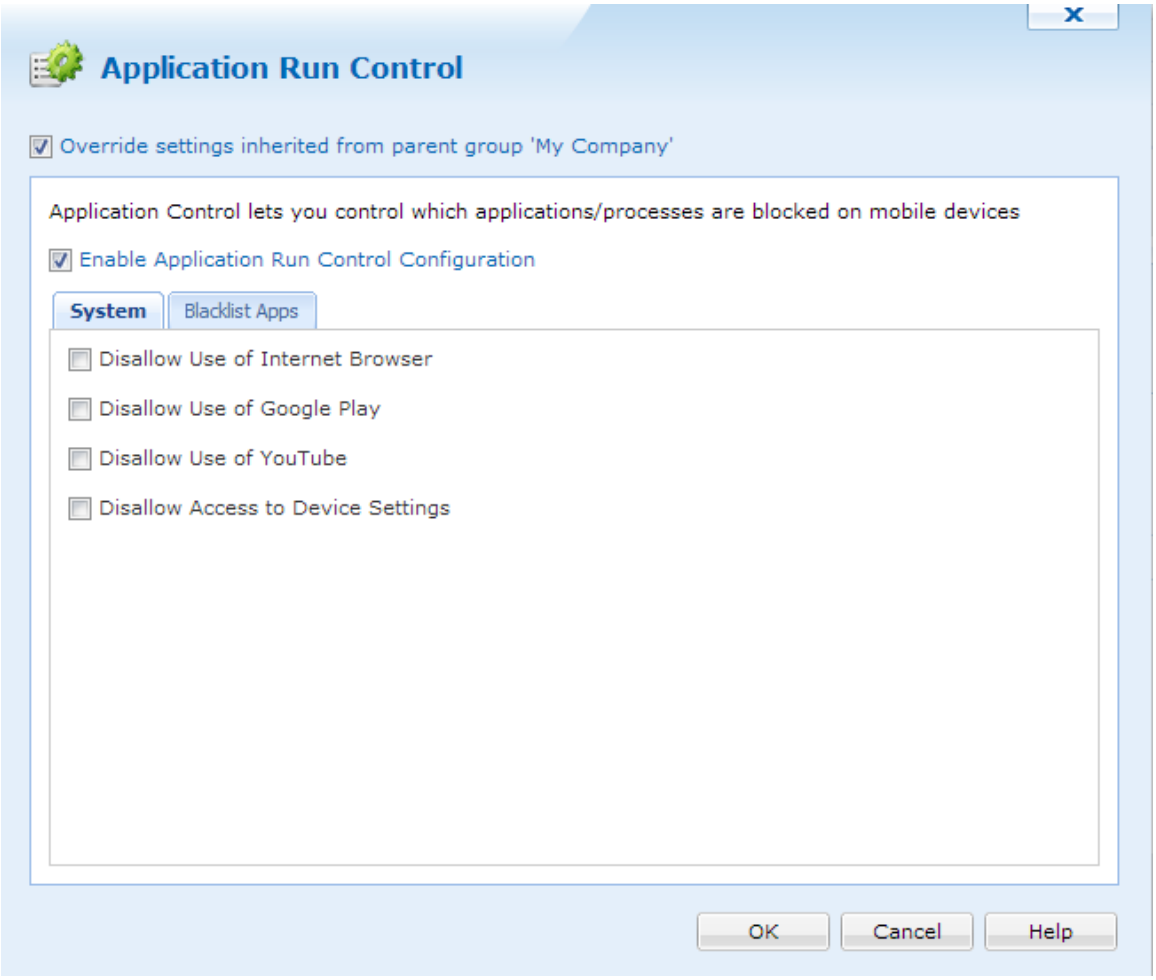
After you have specified the time interval, select a script to execute, or click **Scripts** to bring up the **Manage Scripts** dialog box. Please see the Script Manager page for further details.

Once everything is configured, click **OK**.

Android+ Application Run Control Policy

The easy availability of applications—games, consumer-oriented utilities and third party tools—for mobile devices results in end users installing and running unauthorized personal programs and recreational software on devices meant for business use. In addition to contributing to memory and battery life overhead, this situation also contributes to productivity losses. The installation of unauthorized and unapproved non-business applications contributes to a significantly higher volume of support calls, increasing the IT help desk's support burden. Most critically, it is imperative for security-conscious users to control and restrict the unauthorized installation of personal applications to ensure compliance with strict mobile data protection requirements.

MobiControl's application run control features reduce the risk of leakage of sensitive data and complement the existing network security model by preventing the introduction of malware and viruses into the network through the mobile devices. Additionally, it also allows memory management on the mobile devices to free up resources taken up by unnecessary processes, and allowing for better device performance. MobiControl integrates tightly with the operating system to prevent restricted applications from running entirely on the mobile device, making it much more efficient than competing white list and black list solutions which use CPU and battery-consuming processes to monitor for and destroy restricted applications.



Application Run Control dialog box

Block System Apps

MobiControl has the ability to block certain system apps. These apps include the default Internet Browser, Google Play, Youtube and accessing the device settings.

If more applications are needed to be blacklisted, please see below.

Blacklist Mode

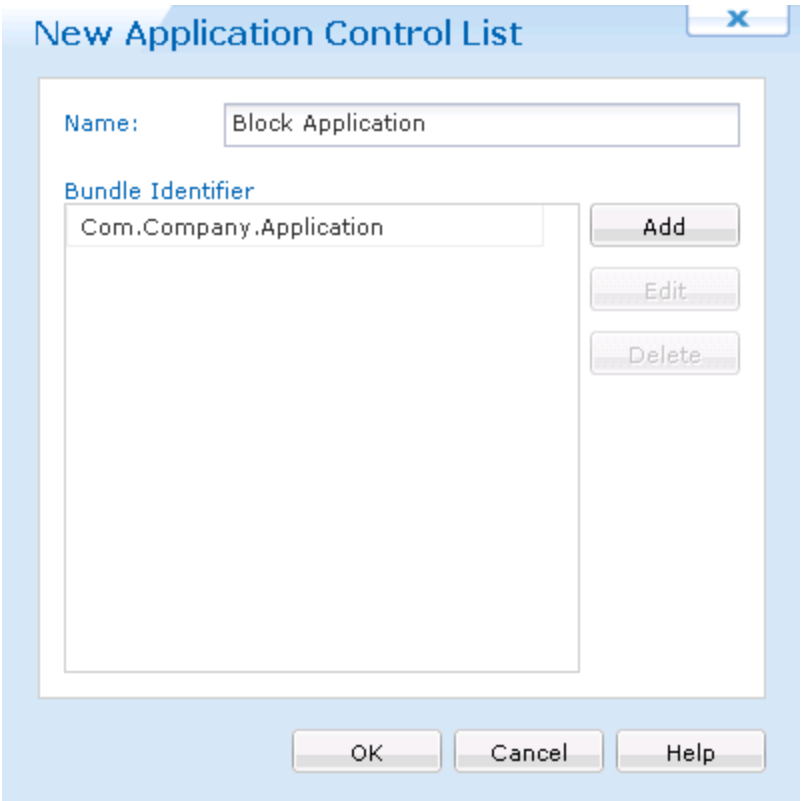
The **black list**, or list of restricted applications, allows IT administrators to ensure that an application will not be allowed to execute on the device. The MobiControl Device Agent prevents any black-listed processes from executing on the device.

To enable application run control for a device or group of devices, select **Application Run Control Policy** from the MobiControl Security Center.

> **NOTE:**
>
> If an application is being run from the lockdown, and it is blacklisted on the device, the application will still run as the lockdown takes precedence over the blacklist.

Control List Creation Methods

Configuration of application run control begins with the creation of an application control list. An application control list is simply a listing of the names of the Package ID's (Bundle Identifiers) that correlate to the application you wish to disallow on the mobile device. For example, `com.google.android.talk` corresponds to Google Talk, and `com.android.providers.calendar` corresponds to Google Calendar for Google Android.



Application Run Control Learning Mode list

You can manually create a new application control list by clicking the **New** button in the **Application Run Control** dialog box, and then choosing the **New** option in the **Select Control List Creation Method** dialog box. The **New Application Control List** dialog pops up, allowing you to specify the application that you want to add to the list.

Now the application run control list has been created, you may assign it to various devices and groups.

IMPORTANT:

Application run control can adversely impact the operation of the mobile device if configured incorrectly. After you have developed a control list, apply it to one or two select devices for extended field testing before expanding it to the general deployment. As a general rule, if you don't know what the application or package ID does (e.g. `com.company.application`), allow it to run instead of blocking it as it might be critical for the device's proper operation. You do have the potential to brick the device by blocking incorrect package IDs.

Modifying or Deleting a Control List

An application control list can be edited whether it is currently in use or not.

An application control list can only be deleted if it is currently not selected for any devices or device groups. A control list that is listed in the **Selected** field is considered in-use, even if the application run control is disabled for the given group or device.

NOTE:

If you edit an application control list that is shared among device groups that are not subgroups of the group you are configuring, the changes will not be propagated to the other devices. The modified control list will

NOTES:

- When logged in as Admin on the mobile device, application control enforcement is suspended.
- Certain processes and applications are critical and necessary for stable device operation and normal execution of the MobiControl Device Agent.
- Applications that are included in a lockdown program menu are automatically on an accept list, and cannot be put on a black list.

OTA Upgrades

To block Over The Air upgrades on your Samsung Android+ devices, block the following:

- Application Name: Software Update - Package Name: com.wssyncmldm
- Application Name: FOTA Client - Package Name:com.sec.android.fotaclient
- Application Name: SDM & Sync Service - Package Name: com.samsung.sdm & com.samsung.syncservice

Whitelisting Applications

If only one or two applications need to be allowed, and black listing every other application seems impractical, we can create a white list for Android+ devices. The whitelist will remove the appearance of all applications from the app drawer except for Settings, Mobicontrol, and the apps that are whitelisted.

To do this, we will need to send a script down to the device or device group. This script consists of turning on the whitelist and then adding the applications to it.

The script to be sent:

```
writeprivateprofstring PRCList
 appcontrol -s
 writeprivateprofstring PRCList PRC0 package.name.1
 writeprivateprofstring PRCList PRC1 package.name.2
 appcontrol -w
```

Example of the script, to allow only the default Android browser:

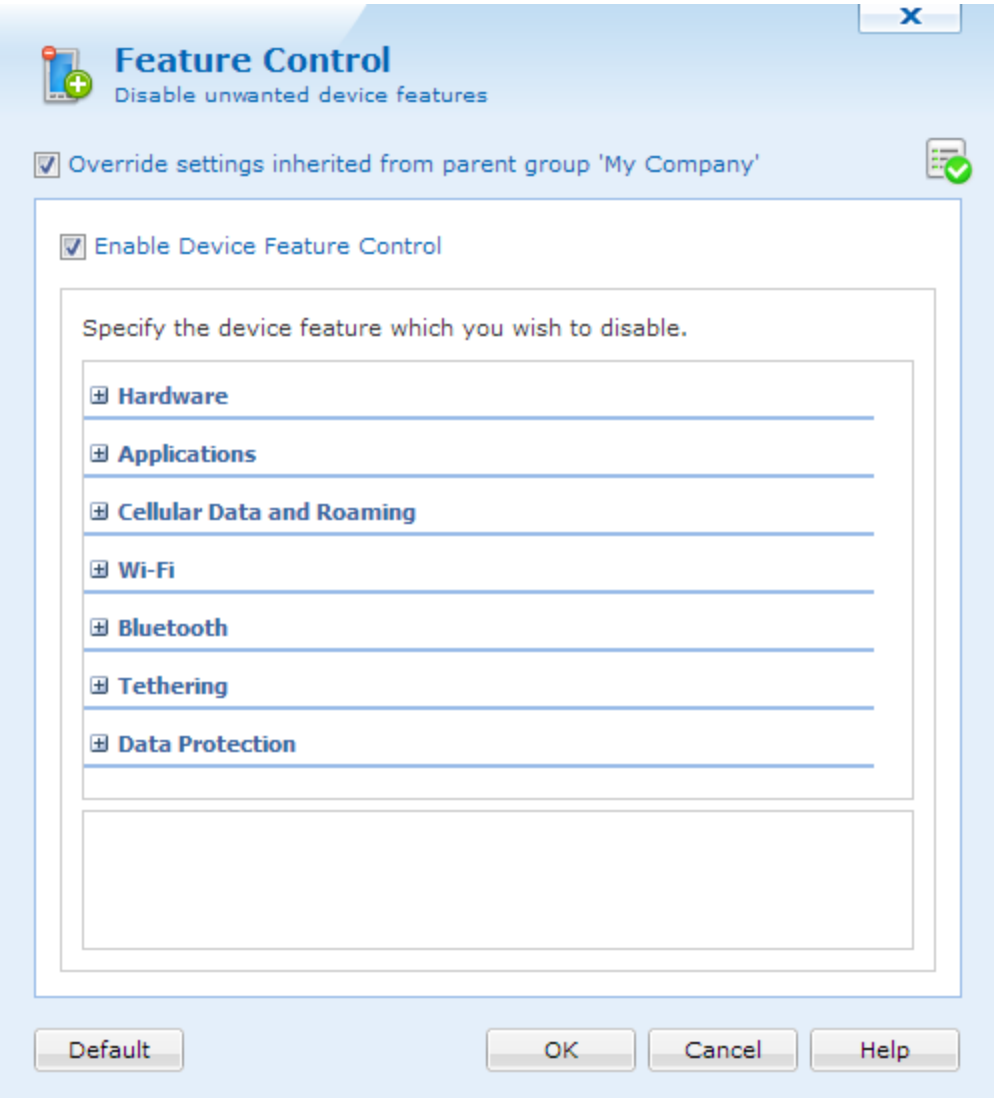
```
writeprivateprofstring PRCList
 appcontrol -s
 writeprivateprofstring PRCList PRC0 com.android.browser
```

```
appcontrol -w
```

Android+ Device Feature Control

For security-conscious organizations and environments where privacy and information security concerns require controlling the unauthorized transfer of mobile data out of the mobile devices, MobiControl provides various on-device feature controls including the capability to block various device communications, similar to firewall functionality. MobiControl's device features control policy allows IT administrators to selectively disable device features. Applying the policy at the individual or group level allows custom profiles for different users and locations in an organization. The ability to disable or enable Bluetooth and infrared ports allows controlling whether end users can beam business cards, applications or documents to one another.

To enable the device feature control, right click a device or group of devices, and select **Device Configuration**. Once the Device Configuration dialog appears, click **Feature Control**.



Device Feature Control Policy dialog box

NOTE:

Some device feature controls may not work with all MDM versions. To see what MDM version is on your device, select the device in the web console and expand the info panel. Scroll down until you see Supported APIs.

To see which features are supported by your MDM version, click 

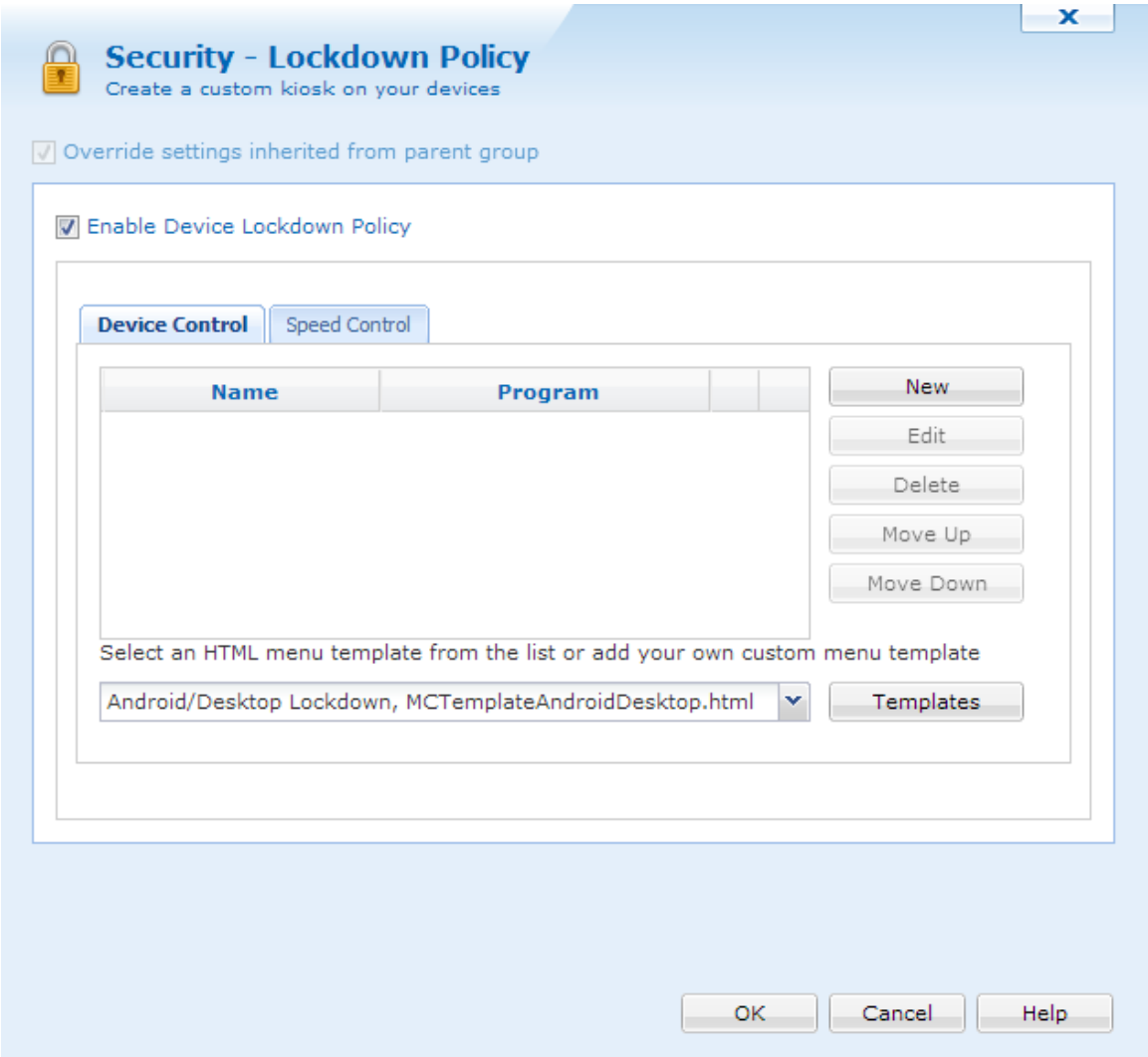
The following features can be enabled or disabled using the device feature control policy. The list is organized by OEM's certified for MobiControl:

- **LG**
- **Lenovo**
- **Pidion**
- **Huawei**
- **Honeywell**
- **Motorola**
- **Panasonic**
- **Samsung**

Android+ Device Lockdown

Device lockdown replaces the standard device home screen with a customizable home screen. Users have access only to authorized applications and websites, and are prevented from accessing all other applications and device controls.

Please see the "Android+ Speed Lockdown" topic on page 1316 for more information about the Speed lockdown.



Lockdown Policy dialog box

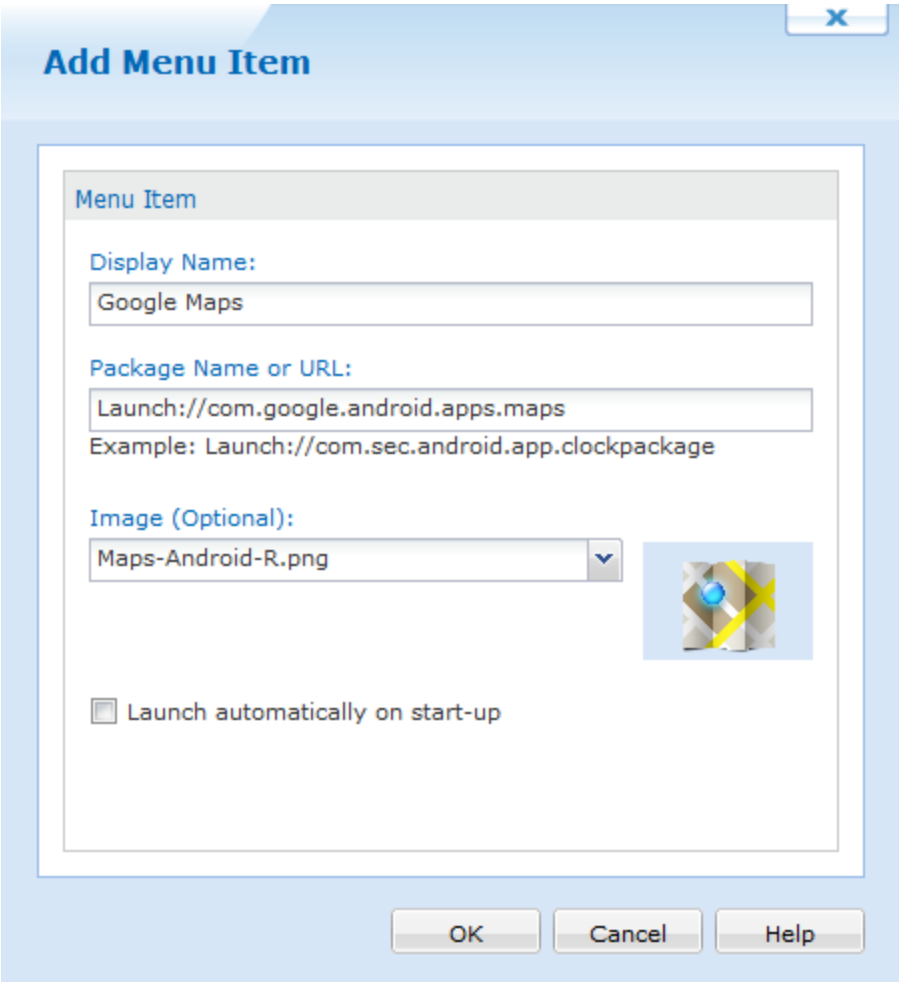
By locking down devices, organizations can minimize the risk of unauthorized persons accessing information on their mobile devices. Administrators can control exactly which programs users are allowed to run, and which websites they are allowed to visit. This decreases the amount of down-time caused by users changing settings that may adversely affect the operation of the device or application software, and also decreases support costs. MobiControl allows running the mobile devices in a kiosk mode with a read-only access to provide critical information to the end users, without giving them access to change the settings.

The lockdown menu can only be dismissed by an administrator. Specification of a user password is optional. If not configured the device user can access the lockdown menu directly after turning on the device. If a user password is defined, then the password must be entered in order to access the lockdown menu.

To configure lockdown settings for a device or group of devices, select the target device or group in the device tree view in the main console window and select **Security** from the **Configure Device(s)** submenu.

Field Name	Description
Enable lockdown menu	Use this checkbox to enable or disable the device lockdown menu.

Field Name	Description
Device Program Menu	The device program menu is a list of programs and websites to which the user has access. There are pre-configured HTML menu templates that can be edited or applied to the menu, and an option to enable or disable the launching of a menu item with keyboard shortcuts. Please see the Device Program Menu section below for details.
HTML menu template	Select a menu template from the drop-down list. Please see the Templates section below or the "Customizing Android+ Lockdown Menu Templates" topic on page 1319 for more information.



Add New Menu Item dialog box

TIP:

- If you link to a search engine the end user will gain full access to the Internet.

Device Program Menu

Use the **New** button to add menu items. Each entry consists of a user-friendly name and a complete file path to the executable, `.lnk` shortcut file, `.cmd` script file, or website address (URL). To adjust the position of the menu items, use the **Move Up** and **Move Down** buttons.

Field Name	Description
Display Name	This is the displayed name of the menu item which will appear on the device.
Program Path	This is the path for the web address, or Package ID (Bundle Identifier) on the device. For instance, the Package ID (Bundle Identifier) for Google Maps is `com.android.apps.maps`. The Package will automatically be prefixed with the Launch:// URI. If you are attempting to navigate to a web page, simply enter the URL, http://www.Company.com. Movie:// - Allows videos to be played on the lockdown. Dial:// - This will open the dialer, with a specified number. (e.g. dial://5555555555) Launch:// - Launch applications based on package ID. File:// - Opens a file on the device (e.g. file:///%sdcard%content/document.pdf) http:// - Opens a webpage from within the lockdown. https:// - Opens a secured webpage from within the lockdown. ftp:// - Opens FTP from within the lockdown. browser:// - Opens a url in browser using the HTTP protocol browsers:// - Opens a url in browser using HTTPS protocol Intent:// - Opens an Android intent (e.g. to open Google Navigation - google.navigation://?q="2%20Greenway%20Plaza%20Houston%20TX%2077046") action:// - Executes a MobiControl action (e.g. to change device password, action://CHANGE_DEVICE_PASSWORD. To configure WiFi, action://CONFIGURE_WIFI)
Image (optional)	This is the name of the image file that you want to display in the lockdown menu with this menu entry. By selecting the image in this dialog box, it will be automatically delivered to the device along with the lockdown configuration. Select an image from the drop-down list, or click the image to select an image from your desktop computer. In order to display this image in the lockdown menu, it is necessary for the HTML template to have a special `<MCDispImgN>` tag. Please see the "Customizing Android+ Lockdown Menu Templates" topic on page 1319 for instructions on how to make this image appear in the Lockdown menu.  **NOTE:** If you wish to replace an image that had been previously imported, upload the new graphic file, maintaining the same file name as the old one. You will be asked to confirm the overwrite of the old file. Click **Yes,** and the new image will be in effect.
Use Application Icon	Use the application icon in the lockdown. In order to display this image in the lockdown menu, it is necessary for the HTML template to have a special `<MCEXEIconN>` tag. Please see the "Customizing Android+ Lockdown Menu Templates" topic on page 1319 for instructions on how to make this image appear in the Lockdown menu.
Launch automatically on startup	When this option is checked, the selected program will be automatically executed on startup (i.e. after a soft reset, or restart of the lockdown process).

Templates

The lockdown program menu is displayed as an HTML web page to the user. The Template drop-down box allows you to select an HTML template from a list of built in templates and your own customized templates.

You can easily create a customized lockdown template by copying an existing template and directly modifying HTML code in the built-in Lockdown Menu Template Editor available in MobiControl. (Please see the "Customizing Android+ Lockdown Menu Templates" topic on page 1319.) You can also use your favorite HTML editor. When editing the HTML file, be sure to preserve the special MobiControl Menu tags. These special tags are automatically replaced with the appropriate Program Menu entries by MobiControl.

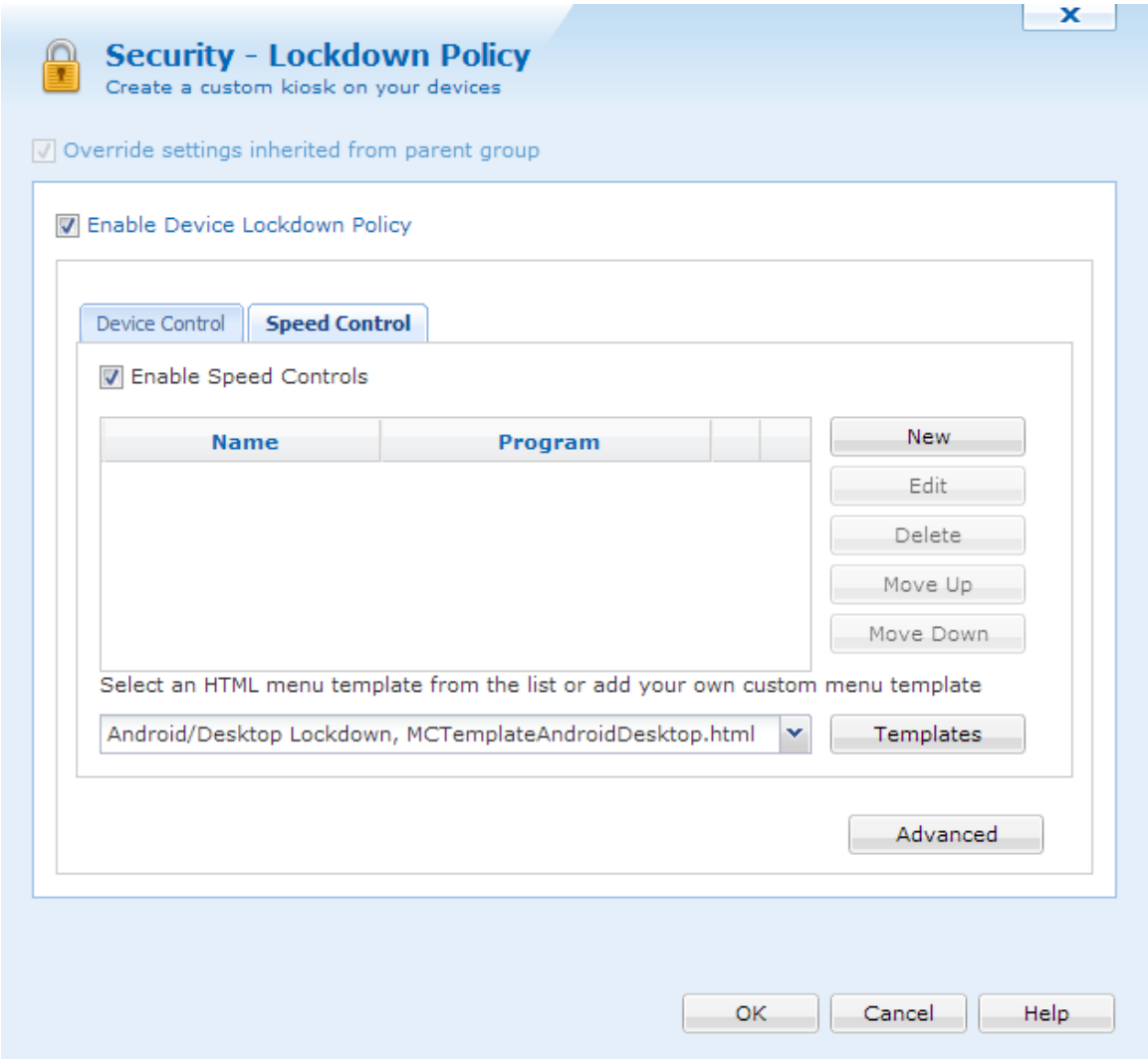
Once you have selected the desired template and clicked the **OK** button, MobiControl will merge the menu items that you have configured with the selected template and generate a custom HTML menu page.

For further assistance, please contact us.

Device lockdown page

Android+ Speed Lockdown

Device lockdown replaces the standard device home screen and Windows **Start** button with a customizable home screen. Users have access only to authorized applications and websites, and are prevented from accessing all other applications and device controls while on the road. This promotes greater safety by disabling distracting features on a mobile device while workers are on the road.

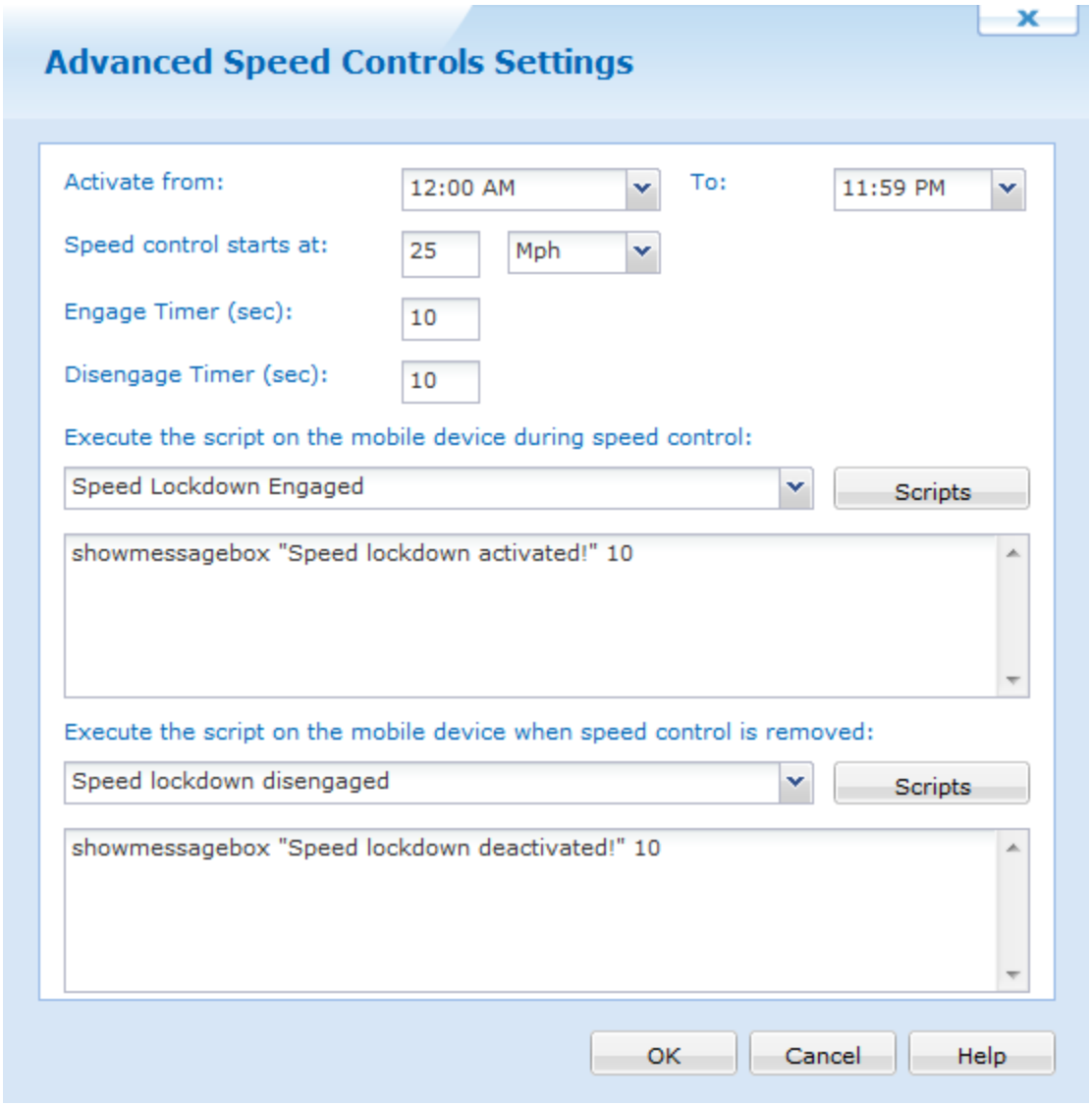


Lockdown Policy dialog box

For information on how to set up menu items and configuring lockdown templates, please click here.

Speed Lockdown triggers when the device is going a certain speed, as set in the Advanced settings. The speed of the device is determined by utilizing the device's GPS unit. Using the device's GPS unit, MobiControl periodically checks the location of the device along with the time. It will then check again and determine the distance between the two points and calculate the device's speed.

Since there are times where there could be traffic, or stop lights, having the speed lockdown disengage and re-engage constantly will cause distraction to a driver. Because of this, the speed lockdown has engage and disengage functionalities. These and other settings can be configured by clicking Advanced.



Advanced Speed Control Settings

Below are brief descriptions of each feature in the Advanced Speed Control settings.

Field	Description
Activate From, to	Here we can set when the speed control should activate. We can set it for the whole day or even 15 minutes.
Speed Control starts at	This is where we decide what speed the device should be travelling before the engage timer starts counting. We can change the speed measurement to either Mph or Km/h.
Engage Timer	The amount of time the device should stay on or above the speed control

Field	Description
	before the lockdown activates.
Disengage Timer	The amount of time the device stays below the specified speed control before disengaging.
Execute script on the mobile device during speed control	When the speed control lockdown is activated, send this script to the device.
Execute script on the mobile when speed control is removed	When the speed control lockdown is deactivated, send this script to the device.

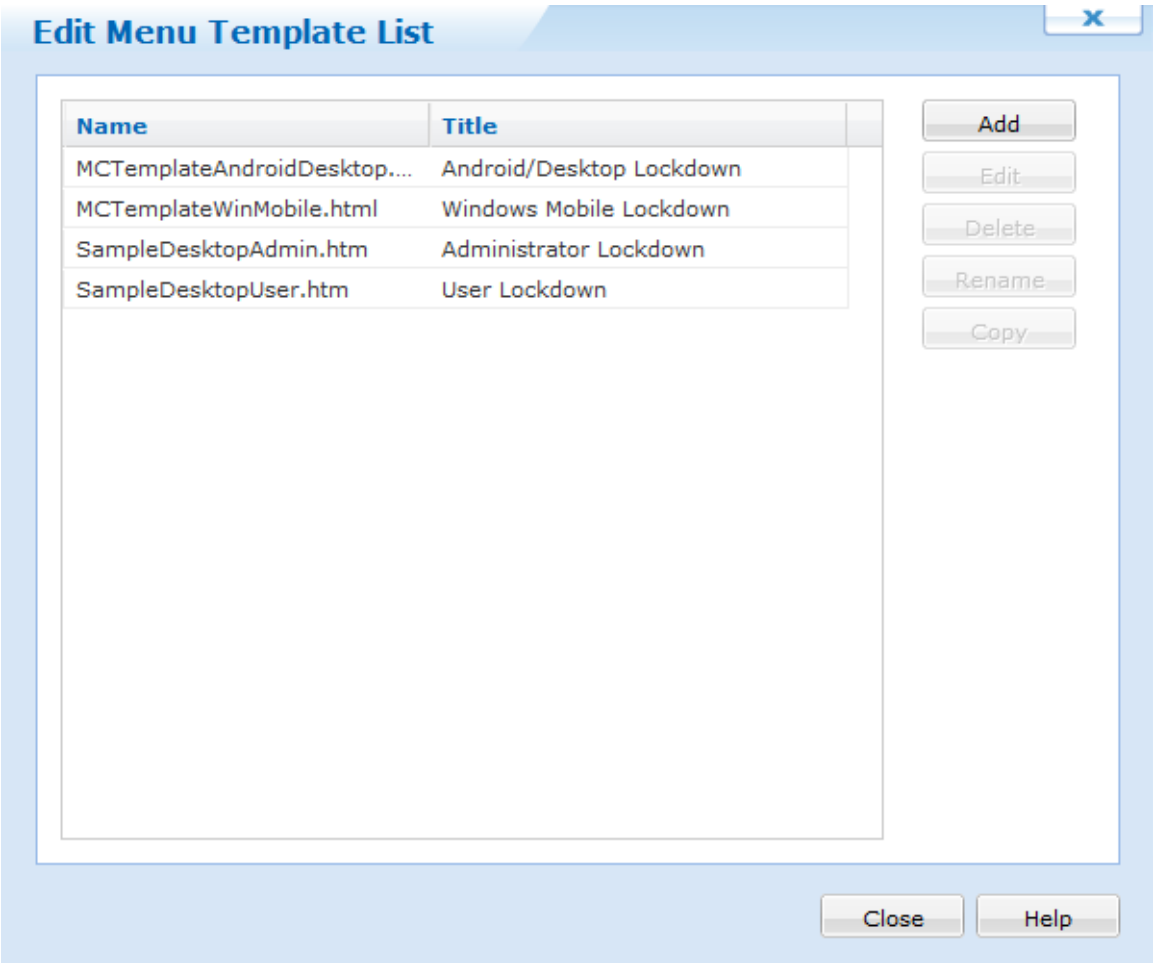
Using the above screen shot, the speed lockdown is activated the whole day, should engage when the device is travelling at 25 Mph or higher for at least 10 seconds. If it falls below the specified speed, wait 10 seconds before disengaging the speed control. When the speed control is activated, send a message box to the device, and when the speed control is removed, send another script.

Customizing Lockdown Menu Templates

MobiControl allows you to modify pre-configured HTML menu templates or to build your own HTML menu templates. A menu template is an HTML file with special menu tags that get replaced by MobiControl when it generates the menu. Essentially, the menu tags get replaced by the menu item links that you configure for your program menu. The table below describes the special menu tags that get replaced in the HTML file.

The easiest way to create a custom program menu template is to make a copy of one of the default templates, customize it, and then add it to the list of available templates:

1. Select **Edit** in the **Lockdown Configuration** dialog box.
2. Create a copy of one of the default templates listed in the **Templates** dialog box. (Copy and paste it into another folder, e.g. My Documents.)
3. Edit the copied file according to the guidelines below and name the file appropriately.
4. Add the new template by selecting the **Add** button in the **Templates** dialog box.



Edit Menu Template List dialog box

The following table describes menu tags:

<table>
<tr><th>Tag Name</th><th>Description</th></tr>
<tr><td><MCMenuFull></td><td>This tag gets replaced with the full menu list that the user has configured. The menu items are separated by carriage returns.
Sample Menu Entries:
MobiControl Device Agent(launch://net.soti.mobicontrol)
My Website (http://www.mywebsite.com)
<table>
<tr><th>Template</th><th>Resultant Menu</th></tr>
<tr><td><html>
<body>
<MCMenuFull>
</body>
</html></td><td><html>
<body>
MobiControl Device Agent

My Website

</body>
</html></td></tr>
</table></td></tr>
<tr><td><MCMenuN>
where "N" is the menu item number</td><td>This tag allows you to place each complete menu item where you want it in the HTML.
Sample Menu Entries:
MobiControl Device Agent(launch://net.soti.mobicontrol)
My Website (http://www.mywebsite.com)
<table>
<tr><th>Template</th><th>Resultant Menu</th></tr>
<tr><td><html>
<body>
1. <MCMenu0>

2. <MCMenu1>

<body>
</html></td><td><html>
<body>
1. MobiControl Device Agent

2. My Website

<body>
</html></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Tag Name</th><th>Description</th></tr>
<tr><td><MCLinkN> and <MCDispN>
where "N" is the menu item number</td><td>These tags let you further separate the menu item to be inserted into the "link" and the "display" text and control where in the HTML template they will be inserted.
Sample Menu Entries:
Android Calendar (launch://com.android.calendar)
Browse mywesbite (browse://www.mywebsite.com)
Report.pdf (file://mnt/sdcard/report.pdf)
<table>
<tr><th>Template</th><th>Resultant Menu</th></tr>
<tr><td><html>
<body>
1. <a href="<MCLink0>">
 <MCDisp0>

2. <a href="<MCLink1>">
 <MCDisp1>

3. <a href="<MCLink2>">
 <MCDisp2>

</body>
</html></td><td><html>
<body>
1. <a href=
"
launch://com.android.calendar
"> Calendar

2. <a href=
"browse://www.mywebsite.com">
Browse
mywebsite

3. <a href=
"
file://mnt/sdcard/report.pdf
"> Report.pdf

</body>
</html></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Tag Name</th><th>Description</th></tr>
<tr><td><MCExeIcon N>
where "N" is the menu item number</td><td>This tag lets you display the built-in icon for an application executable that is in the program menu.
Sample Menu Entries:
Android Calendar (launch://com.android.calendar)
Browse mywesbite (browse://www.mywebsite.com)
Report.pdf (file://mnt/sdcard/report.pdf)
<table>
<tr><th>Template</th><th>Resultant Menu</th></tr>
<tr><td><pre>
<html>
 <body>
1. <a
href="<MCLink0>">
<img src="
<MCExeIcon0>">

2. <a
href="<MCLink1>">
<img src="
<MCExeIcon1>">

3. <a
href="<MCLink2>">
<img src="
<MCExeIcon2>">

 </body>
</html>
</pre></td><td><pre>
<html>
 <body>
1. <a href=
"launch://com.android.calendar">
<img src= "
SDCard\Lockdownimage\MCLD_
Calendar.bmp">
2. <a href=
"browse://www.mywebsite.com> <img
src= "
SDCard\Lockdownimage\MCLDBrowse.bmp
">
3. <a href=
"file://mnt/sdcard/report.pdf">
<img src= "
SDCard\Lockdownimage\MCLD_
report.bmp">
 </body>
</html>
</pre></td></tr>
</table></td></tr>
<tr><td><MCDispImg N>
where "N" is the menu item number</td><td>This tag lets you associate a picture with an entry in the lockdown screen.
Sample Menu Entries:
MobiControl Device Agent (launch://net.soti.mobicontrol)
My Website (http://www.mywebsite.com)
<table>
<tr><th>Template</th><th>Resultant Menu</th></tr>
<tr><td><pre>
<html>
 <body>
1. <a href=
"<MCLink0>"> <img
src
="<MCDispImg0>">

2. <a href=
"<MCLink1>"> <img
src=
"
<MCDispImg1>">

</body>
</html>
</pre></td><td><pre>
<html>
 <body>
1. <a href=
"launch://net.soti.mobicontrol">
<img src =
"\SDCard\Lockdownimage\Logo.png">

 2. <a href=
"http://www.MyWebsite.com"> <img
src=
"SDCard\Lockdownimage\website.jpg">

</body>
</html>
</pre></td></tr>
</table></td></tr>
</table>

Including Pictures in Menu Templates

You can insert images into your template by simply using the Insert Image feature in the built-in HTML Template Editor. MobiControl will deliver the image to the device. Alternatively, if you do not want to use MobiControl to deliver the image, you can simply specify in the HTML template the full path to the graphic for where it will be found on the mobile device (e.g. `<img src="file:///SDCard/images/CompanyLogo.jpg">`).

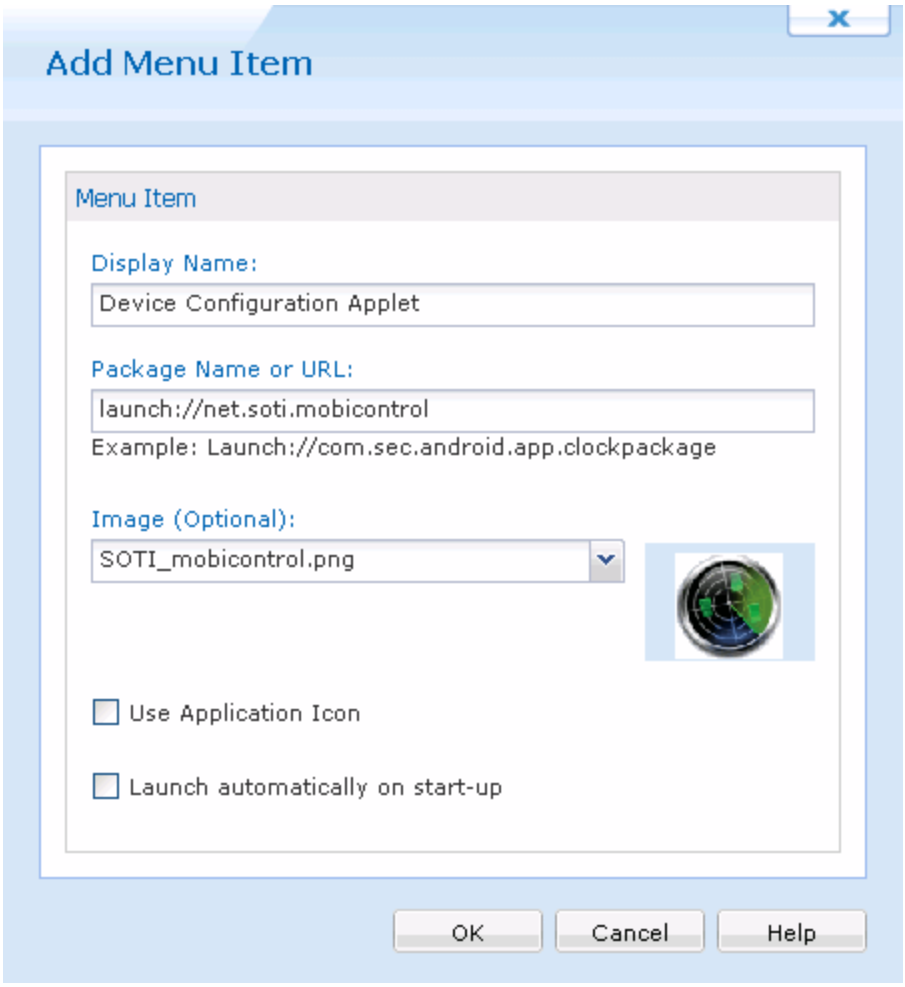
URI's

Uniform Resource Identifier (URI) is a string of characters used to identify a name or a resource on the Android Device. Such identification enables interaction with representations of the resource using specific protocols. Schemes specifying a concrete syntax and associated protocols define each URI. The MobiControl Lockdown on Android devices allows you to use custom URI's. Such URI's include Launch://, Http://, Https://, File:// and Browser://.

Linking to the MobiControl Device Configuration Applet

The MobiControl device applet that is normally accessed by tapping on the MobiControl icon on the Today screen or system tray of the device contains a bounty of useful status information. This information can be very useful when trying to troubleshoot a problem in the field, for example resolving connectivity issues between the device and the MobiControl Deployment Server.

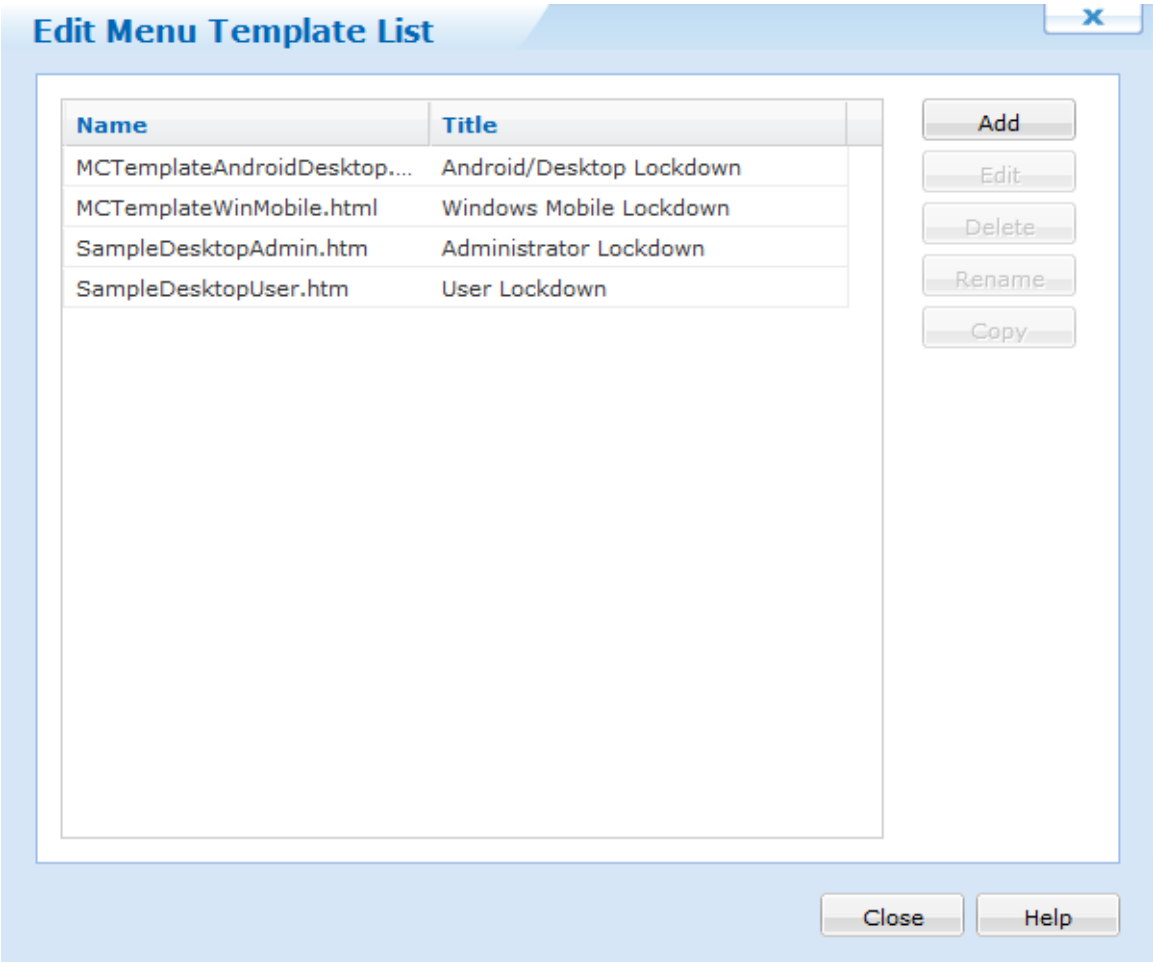
To create a link to the applet from the lockdown program menu add a program entry to the following path: `net.soti.mobicontrol`



Program menu entry for MobiControl Configuration Applet

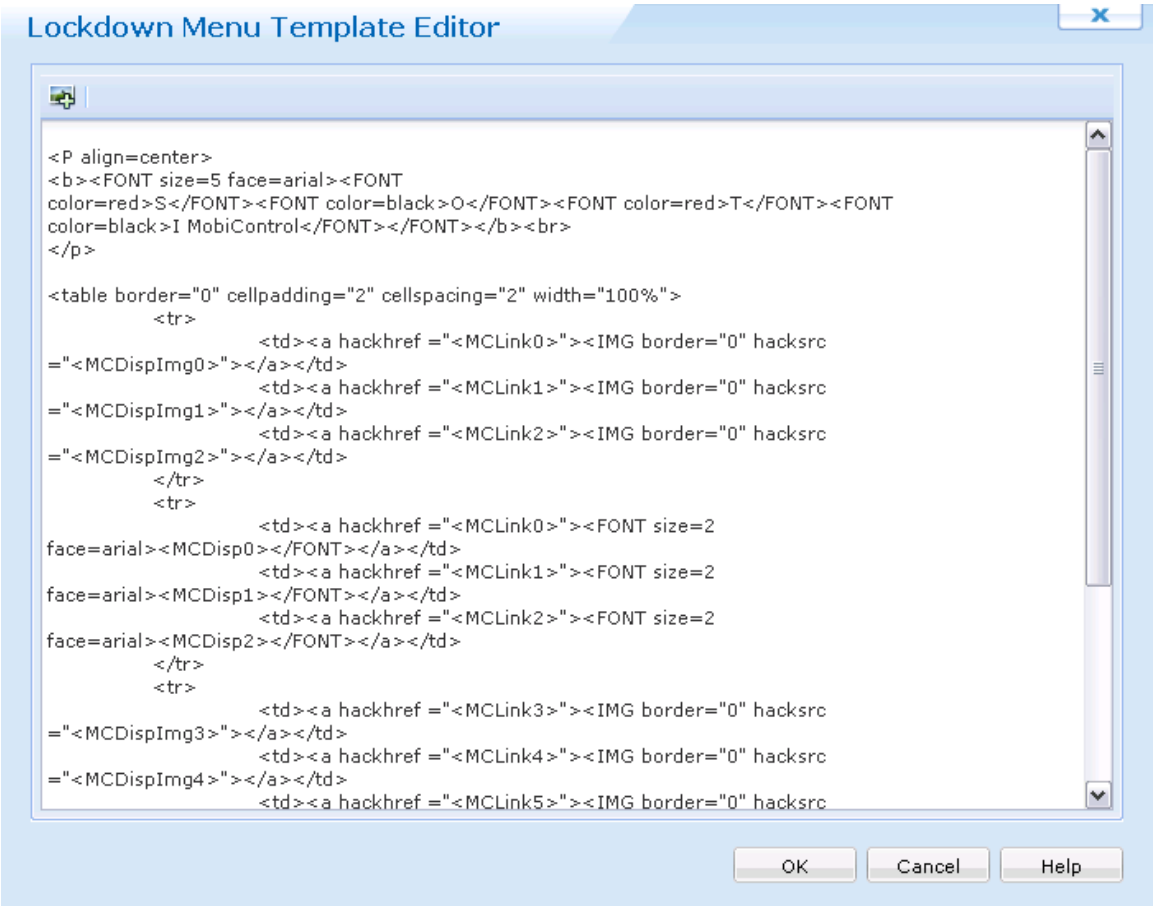
Edit Menu Template List

In the **Edit Template Menu List** dialog box, click **Add** and navigate to the location of your customized lockdown page and select it. You will see the customized menu template in this list now. You can chose to edit this template further by clicking on **Edit** and launching the lockdown menu template editor, or click on **Close** and then select the template from the **Lockdown Menu**.



Edit Menu Template List dialog box

You can edit the lockdown menu templates using the built-in HTML editor. After saving a modified template, be sure to select the template file in the combo selection box on the main **Lockdown Configuration** page. Basic HTML, Java, and Flash are supported in the lockdown.



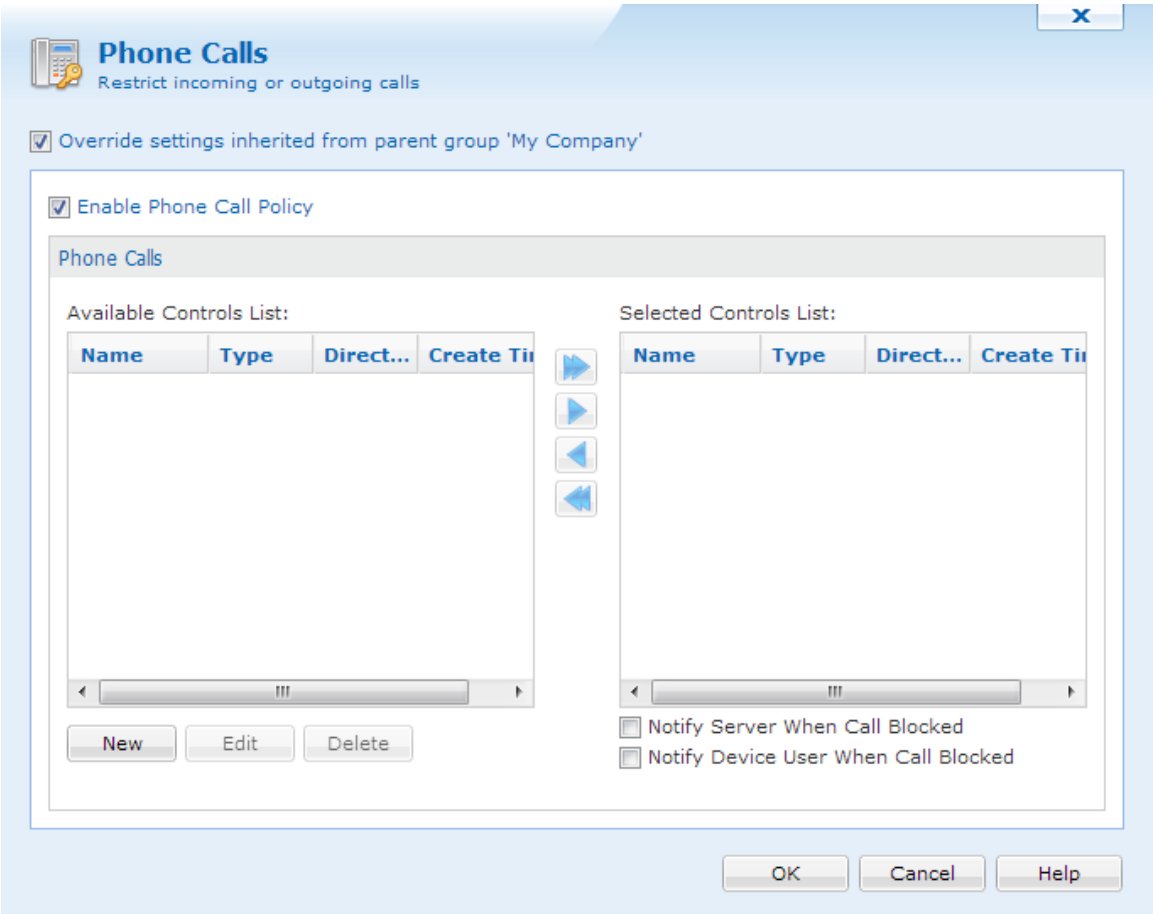
Lockdown menu HTML editor

TIP:

You can easily include a graphic in your HTML template by selecting the **Insert Image** menu option in the HTML Editor.

Android+ Phone Call Policy

MobiControl provides various on-device feature controls including the capability to block various device communications, including what numbers a device is able to call or receive calls from.



Phone Call Policy dialog box

Phone Call Policy Control Lists

MobiControl allows you to specify the numbers to which users may place calls to and receive calls from:

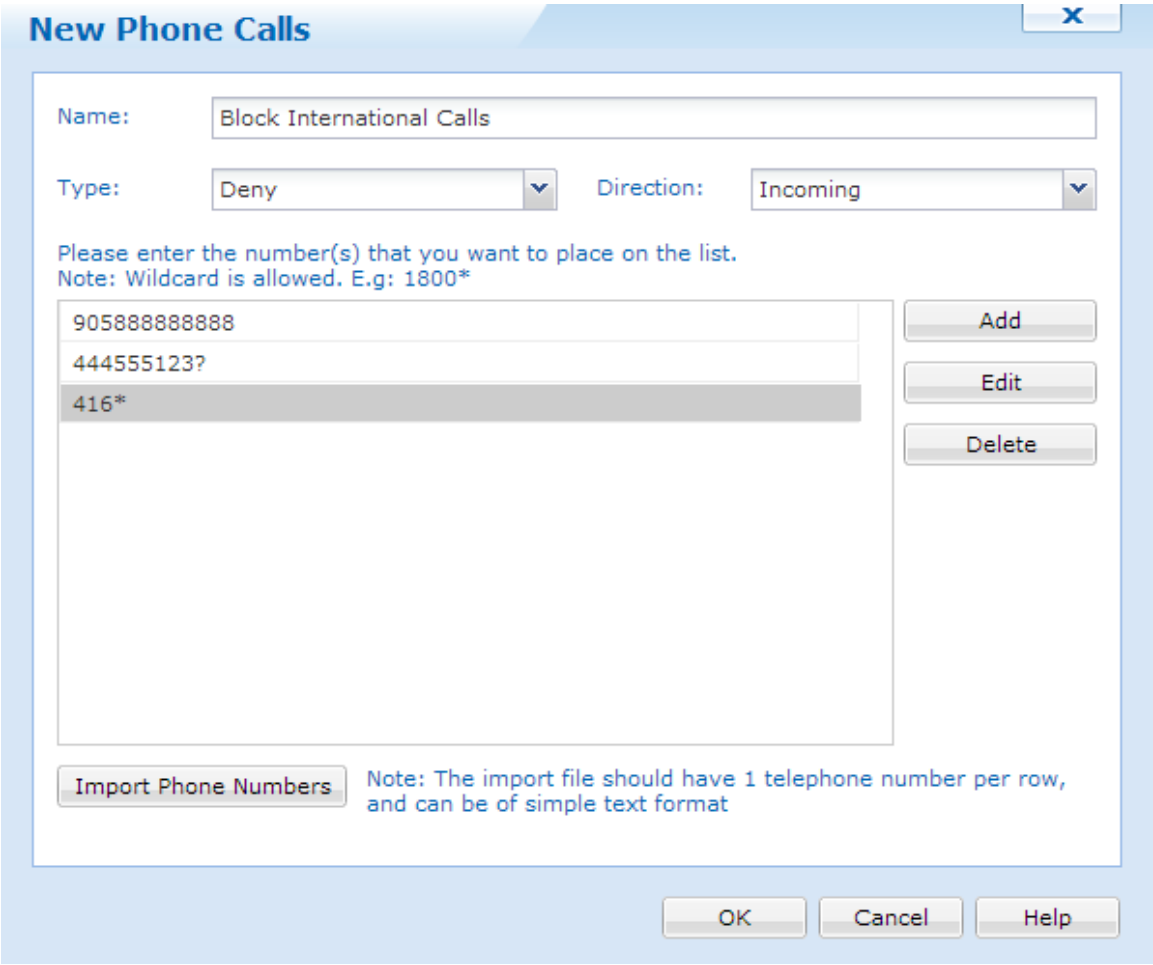
1. The **Available Control Lists** displays all control lists that have been defined, but currently are not in use. Administrators are able to create several different phone call policies without having them be activated on the devices.
2. The **Selected Control Lists** displays all currently activated control lists. Only the control lists included in the selected control lists are allowed to execute on the device. This provides an added layer of security for organizations concerned about unknown phone calls that may be placed from or received by the device. This can potentially happen without the end user being aware of it, as is frequently the case with viruses, spyware and other malicious applications.

> **NOTE:**
>
> There cannot be both deny and allow control lists activated at the same time. All control lists for a particular direction must be the same type.

> **IMPORTANT:**
>
> If the allowed list is not set up correctly, you may end up blocking or not allowing a potential system critical phone call. Emergency numbers will always be allowed even if they are not part of a whitelist.

3. When the **Notify Server on Call Blocked** check box is checked, the server's log file will output all calls that were blocked, along with the phone number that was trying to call in or out for the particular device.
4. When the **Notify User on Call Blocked** check box is checked, and the user receives an incoming call from a phone number that was blocked, a message box will be displayed

To enable phone call policy control for a device or group of devices, select **Phone Call Policy** from the MobiControl Security Center. (Please see the "Android+ Device Configuration" topic on page 1292.)



New Phone Call Policy entry dialog box

Field Name	Description
New	Clicking on this button allows you to create a new phone call policy with the dialog box as shown above. Assign a meaningful name to help distinguish between the various phone call policies you may setup.
Type	The available options allowed are either Allow or Deny. The type Allow indicates the phone calls that can either be placed from the phone or received by the phone or both based on Direction set for this policy. The type Deny indicates the phone calls that can not either be placed from the phone or received by the phone or both based on Direction set for this policy. If attempting to block restricted or unknown callers simply add **<unknown>** and/or **<restricted>** to the deny list.
Direction	The available options are Incoming, Outgoing, or Both. Incoming indicates that this policy is for calls received by the device. Outgoing indicates that this policy is for calls placed by the device. Both indicates that the policy is for both incoming and outgoing calls. For example, you may want to allow all communication to and from your device to your IT Support team and hence you would select both in this case with the appropriate phone numbers that can be dialled to work with your support team.

Once you have configured the Name, Type and Direction, click on **Add...** in order to enter in the phone number(s) that the policy monitors.

MobiControl will compare the number either received or placed with the list of numbers mentioned in the policy and compare the exact phone number displayed with the list of numbers you provide. If you have a series of numbers that you would like to enter in, there are a few options available, which can be used in combination with each other:

1. Leverage the wild card character, which is the asterisk, or '*'. The asterisk indicates any number of digits. For example, you may want to only allow calls coming from a particular area code. In this case, you can enter in '<area code>*' as the number.

   EXAMPLE:

   416* would match all calls that start with 416.

2. Leverage the single wild card character, which is the question mark, or '?'. The question mark indicates any single digit.

   EXAMPLE:

   You may want to allow communication to a list of phone numbers that only vary by a single digit. In this case, you can enter in as an example, 444555123?. This indicates the policy applies to the following list of numbers:
   444-555-1230
   444-555-1231
   444-555-1232
   444-555-1233
   444-555-1234
   444-555-1235
   444-555-1236
   444-555-1237
   444-555-1238
   444-555-1239
   Combinations of the two wild card characters can also be used if required. For example, 4??-555-12* would succeed if the phone number is 432-555-1234, but not if the phone number is 432-432-1234

When the **Import CSV** button is selected, a dialog box will appear to import the list of phone numbers using a CSV file. MobiControl assumes that the input file format is **one phone number per line**. To view a sample CSV file, click here.

EXAMPLE:

9058888888
519222*
416*
Upon reading in the file, the individual numbers will be added to the list control, just as though they were individually typed in using the Add button.

IMPORTANT:

The file being imported must not contain more than 2000 lines.

Android+ Web Filter

The Android+ Web Filter allows us to block certain types of websites. MobiControl uses a highly sophisticated filter to determine which web pages are safe and which are not. If a user stumbles across a web site that is blocked by the filter, they are then redirected to a predetermined safe site.

To enable the Android Web Filter, right click a group or a single Android device, click **Device Configuration**. After the Device Configuration dialog appears, click **Web Filter**.

IMPORTANT:

Webroot's SecureWeb Browser must be installed on the device for the web filter to function. It is recommended to include the SecureWeb Browser in an Application Catalog so that it can be installed on the device. Please see the "Android+ Application Catalog" topic on page 1403 for more information on the Application Catalog.

Android Web Filter dialog box

When the Web Filter is enabled, MobiControl will push down a secured browser to the configured devices. This browser has the advanced web filter technology that allows us to block categorized websites.

The Web Filter has an option to redirect users to a trusted website if they do come across a filtered website.

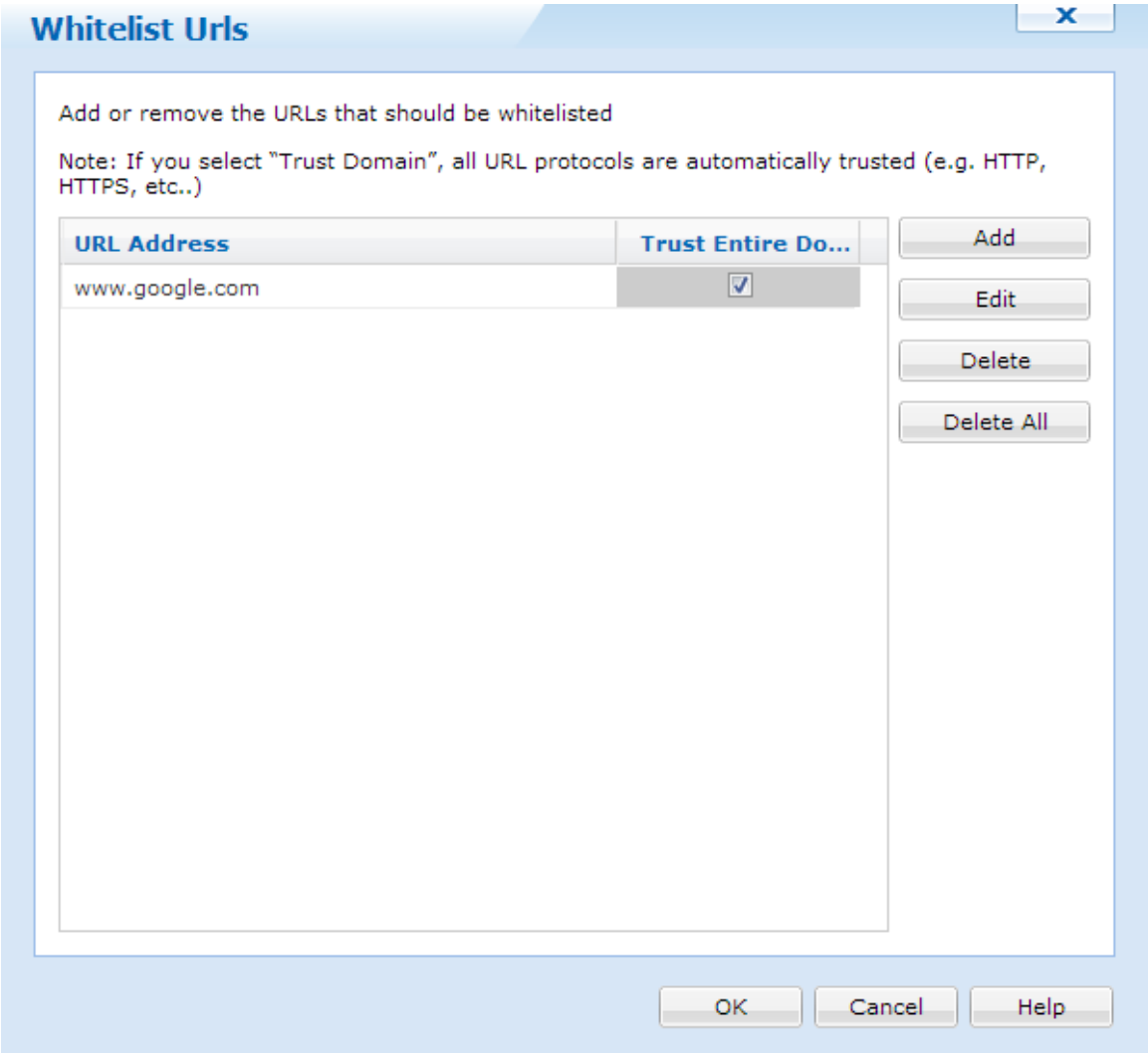
Below, we will go over each of the categories that included with this filter (Click each title to see sub categories):

- **Adult**
- **Business and Economy**
- **Education**
- **Entertainment**
- **Government/Politics**
- **Hacking and Proxy Avoidance**
- **Health**
- **Life Style**
- **Other**
- **Spam**
- **Technology**

Website Whitelist

If certain websites are blocked by the filter, we can enable a Website Whitelist to ensure that these sites do not get blocked. To do this, click the 

button.



Website Whitelist

Clicking Add allows us to enter a URL address. These addresses are the websites that will not be blocked by the filter.

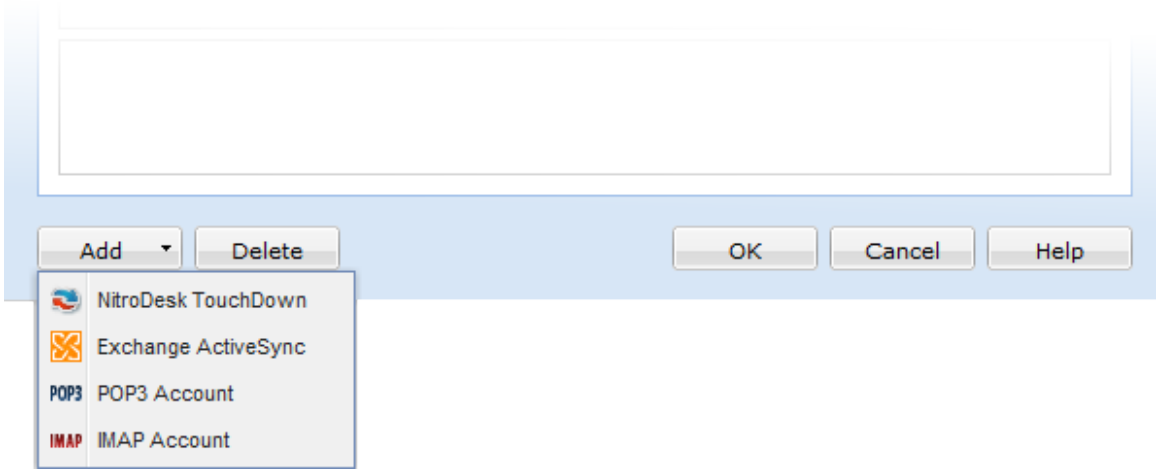
Checking off **Trust Entire Domain** will ensure that all protocols, and sub domains are trusted.

If a URL is not needed anymore, click Delete.

After all configurations are set, click OK to save everything and close.

Android+ Device Email Configuration

With MobiControll, you can now configure Microsoft Exchange ActiveSync, NitroDesk TouchDown, POP3 and IMAP account settings for your mobile device. To arrive at this configuration menu, select the device or the group, right-click, select **Configure Device(s)**, and click **Email Configuration**.



Add allows the use of multiple exchange profiles to be configured on the device. If the Android+ device has Nitro Desk installed MobiControl can also configure those email settings. For more information on Nitro Desk on Android please See "Android Device Exchange ActiveSync via NitroDesk TouchDown".

NOTE: SUPPORTED DEVICES

Only Samsung devices and the LG VS950 are able to configure Exchange, IMAP and POP email through the default email application. All other devices must use Nitro Desk to configure Exchange ActiveSync email.

For more information on how to configure Exchange ActiveSync on Android+ devices please See "Android+ Exchange ActiveSync Email Configuration"

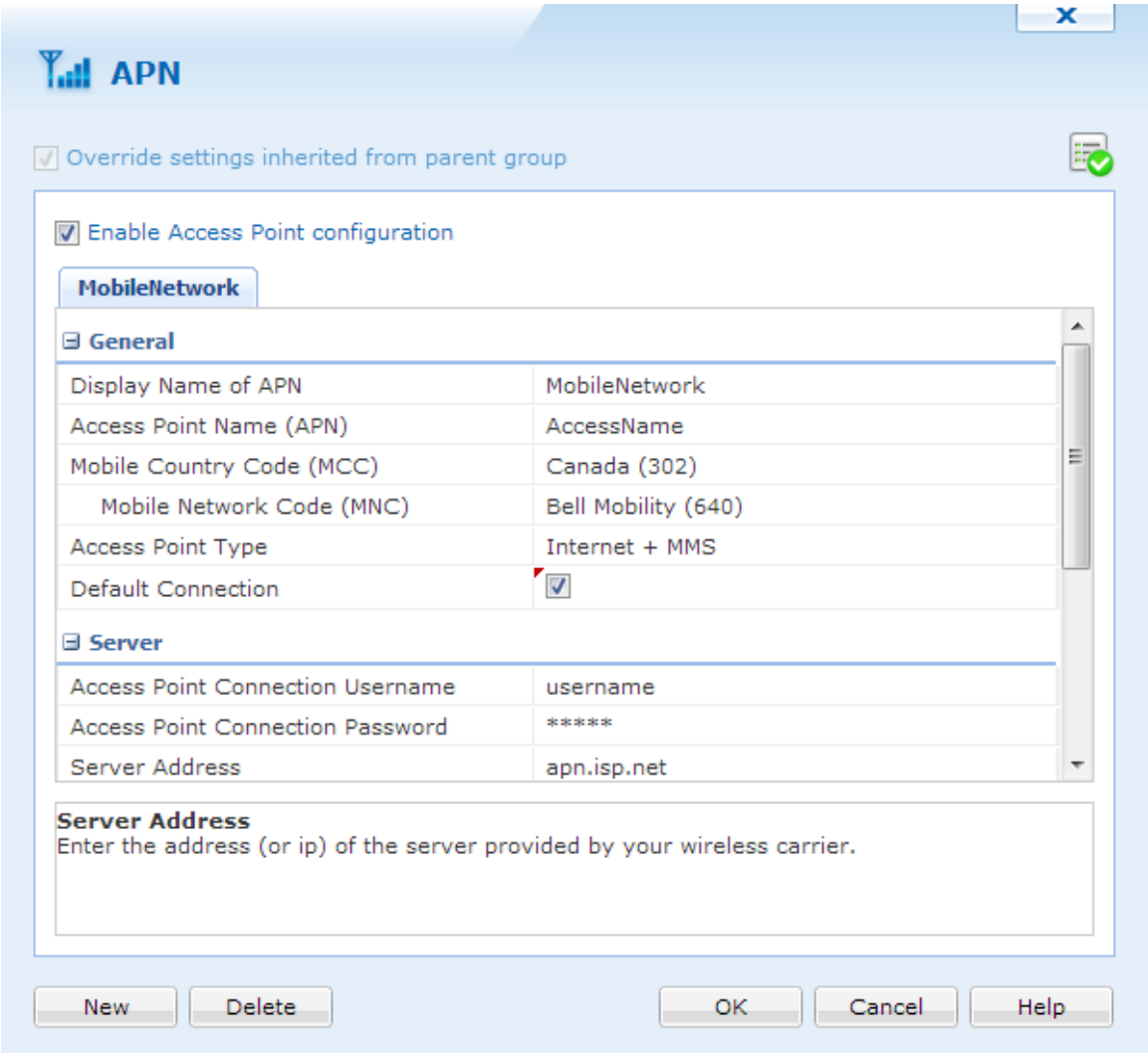
For more information on how to configure IMAP on Android+ devices please See "Android+ Device IMAP Email Configuration"

For more information on how to configure POP on Android+ devices please See "Android+ Device POP3 Email Configuration"

Android+ APN Configuration

If a cellular company has given specific APN connection settings to allow devices to connect to the Internet, MobiControl allows us to centrally manage these settings through a special configuration.

To access this configuration, right click a device (or group) and click **Device Configuration**. When the Device Configuration panel appears, click **APN** under Connectivity.



Configure SSL device settings dialog box

General

Field	Description
Display Name of APN	This will be the display name that appears on the device
Access Point Name (APN)	The name of the APN
Mobile Country Code (MCC)	The country code for the APN. This is a drop down that lists every available country.
Mobile Network Code (MNC)	The mobile network code for the selected country. This is a drop down that lists all available mobile networks in the selected country
Access Point Type	The account point type. We can choose Internet, MMS, or Internet + MMS

Field	Description
Default Connection	If selected, devices would use this as the default connection

Server

Field	Description
Account Point Connection Username	The username provided by the wireless carrier
Account Point Connection Password	The password provided by the wireless carrier
Server Address	The address or IP of the server provided by the wireless carrier
Port	The port number for the server

Proxy

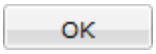
Field	Description
Proxy Server Address	The server address of the proxy server provided by the wireless carrier
MMS Proxy Server Address	The address of the MMS Proxy Server
MMS Server Address	The address of the MMS server
Port	The port number for the server

Security

Field	Description
Authentication Type	The authentication type for the APN connection. We can choose PAP, CHAP, PAP/CHAP, or none

Clicking 

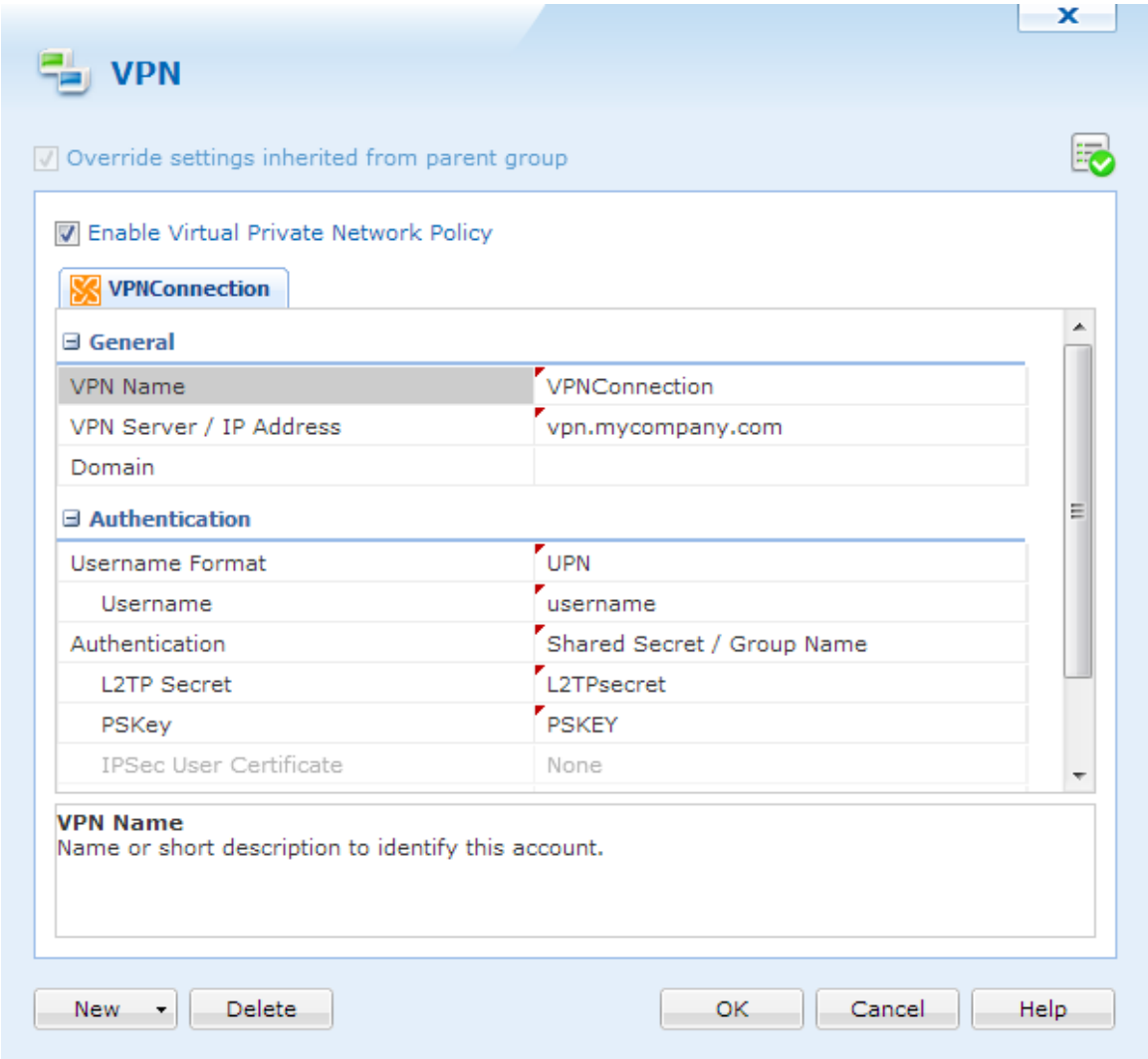
allows us to create multiple APN profiles.

After everything is configured, click 

to save and close the window.

Android+ VPN Configuration

MobiControl's Android+ VPN Configuration allows us to set up the VPN settings for devices. We are able to set up VPN for L2TP or PPTP. To access the VPN configuration page, right click a group or device and select **Device Configuration**. When the Device Configuration dialog appears, click **VPN**.



Configure VPN device settings

To create a new VPN connection for either L2TP or PPTP, click New and select either one. Below we will go through each of the configurations for L2TP and PPTP. Click the titles to reveal the information:

L2TP

PPTP

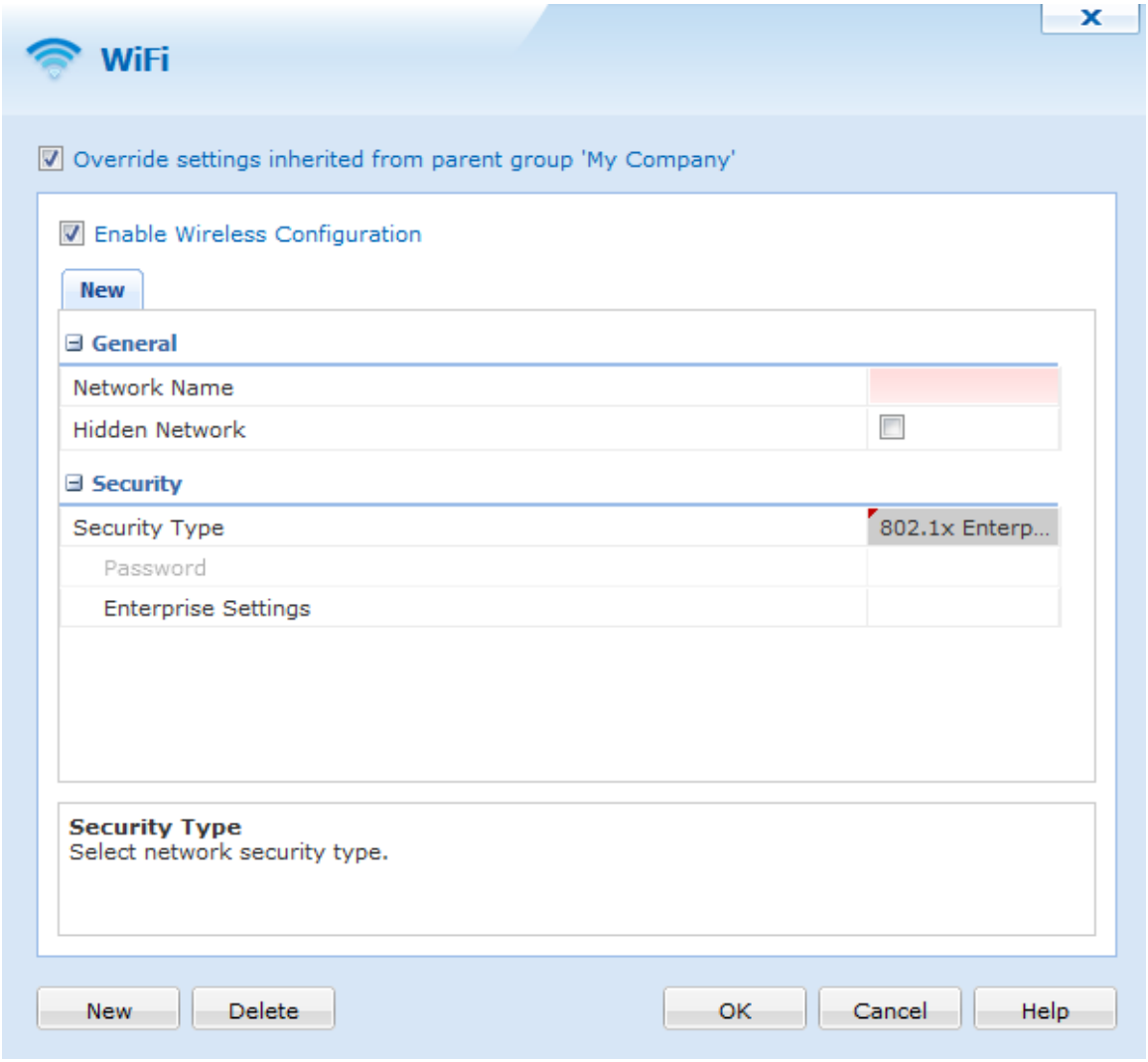
If a VPN connection is not needed any more, click Delete.

After all settings have been configured, click OK to save and close.

Android+ WiFi

With MobiControl's WiFi policy, we are able to configure the WiFi connection on Android devices. This offers a way to safely and quickly configure the wireless connection on one or hundreds of devices.

To enable the Wireless Policy for a device or group of devices, right click a device or group, and select **Device Configuration**, from there, click **WiFi**.



Device Feature Control Policy dialog box

If more than one network is needed to be configured, selecting 

will create an additional profile.

Field Name	Description
Network Name	The name of the network which the device should connect to. Also is the name of the Wireless Policy.
Hidden Network	Select whether the network is hidden or not.
Security Type	The security protocol currently being used on the network. We can select WEP, WPA/WPA2, 802.1 Enterprise or None.
Password	The password to connect to the network.
Enterprise Settings	If 802.1x Enterprise is selected as the security type, clicking the text box will bring up the 802.1x Enterprise settings page. See below for more information on the 802.1x Enterprise settings panel.

802.1x Enterprise Settings

If a wireless configuration is not needed anymore, just select Delete. After all configurations are done, click OK.

Android+ Advanced Settings

There are eight main aspects to Android+ Advanced Settings. Each of these settings can be configured for a single device or applied at the device group level thereby configuring a set of devices. When the devices are moved from one device group to another in the device tree, the settings for the new device group are applied automatically to the devices.

Custom Attributes

Custom Attributes allows us to create custom information that appears on the information panel on the right hand side of the web console. Please see the "Custom Attributes" topic on page 1343 for more information.

Custom Attributes

Custom data allows us to pull information for Android+ devices and show this information in the web console's info panel. MobiControl can pull information from .ini files. Please see the "Android+ Custom Data" topic on page 1346 for more information.

Connection Settings

This option allows you to configure connection settings for your mobile device(s), via. configure connection security by enabling or disabling SSL, select connection mode between persistent, scheduled and manual, change connection retry interval and set log file management, among other options. Please see the "Android+ Connection Settings" topic on page 1350.

Deployment Server Priority

This option allows you to specify the Deployment Server preferences for the devices. When a device is configured with more than one Deployment Server, it will try to connect to highest priority one first and if this server is not accessible, then it will try to connect to the next server available. Please see the "Android+ Deployment Server Priority" topic on page 1353.

Remote Control Settings

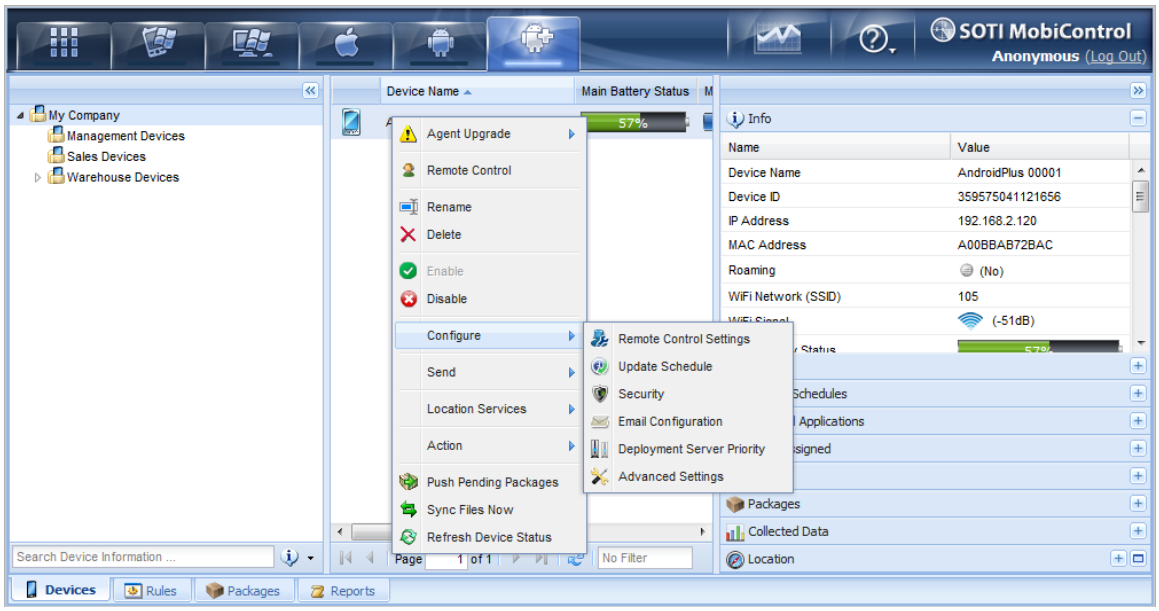
Select a device skin to display in the MobiControl Remote, and choose the connection profile to use when remote controlling the device. This allows for customized remote control settings, optimised for different types of connections, for instance, high-speed Wi-Fi or low-speed cellular connections). Please see the "Android+ Remote Control Settings" topic on page 1355.

Support Contacts Info

If users call support for their mobile device needs, configuring this option allows them to find the contact information reliably. Since this information is set centrally all information is updated once it's changed. Please see the "Android+ Support Contacts Info" topic on page 1356 for more information.

Update Schedule

Adjust the interval at which the mobile devices contact the Deployment Server for new updates, configuration changes and packages. Please see the "Android+ Device Update Schedule" topic on page 1359.

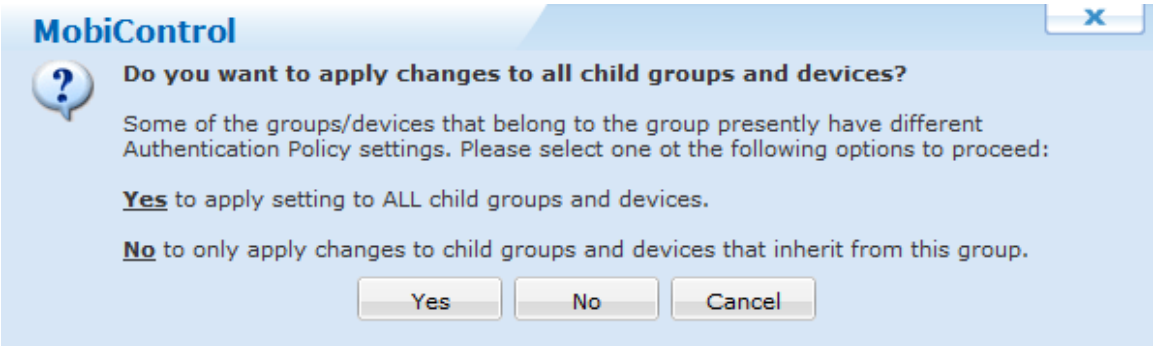


Device Configuration Menu options

Configuration Override Settings

Override settings allows you to create unique configuration settings at the current level which you have selected. This will override the settings that the device or group was previously inheriting from the parent group.

If the configuration settings are different at any sublevel (be it device or subgroup) then a confirmation prompt will allow you to choose whether the current setting(s) should be applied to all sub devices and groups or only the level that inherit configurations from this group.



Custom Attributes

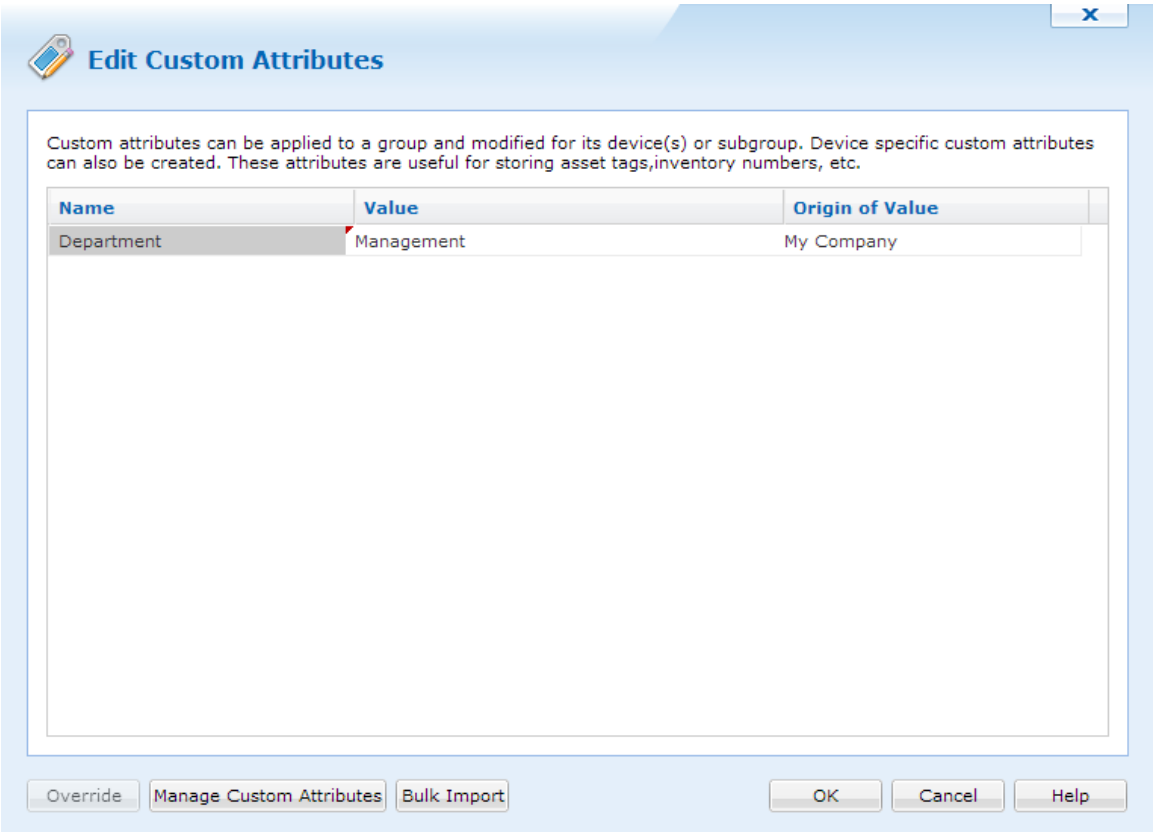
Custom Attributes allows us to create attributes to show in the information panel with our own data. This offers custom organization and labelling. For example, we can create a department attribute and put a different department for each device or device group.

Custom Attributes can also be propagated to devices so that they can be used in other applications and information.

NOTE:

Custom Attributes are available for all device types.

To set up Custom Attributes, right click a device or device group, go to Advance and click **Custom Attributes**.



Custom Attributes panel

The Custom Attributes panel has 3 columns: name, value and origin of value.

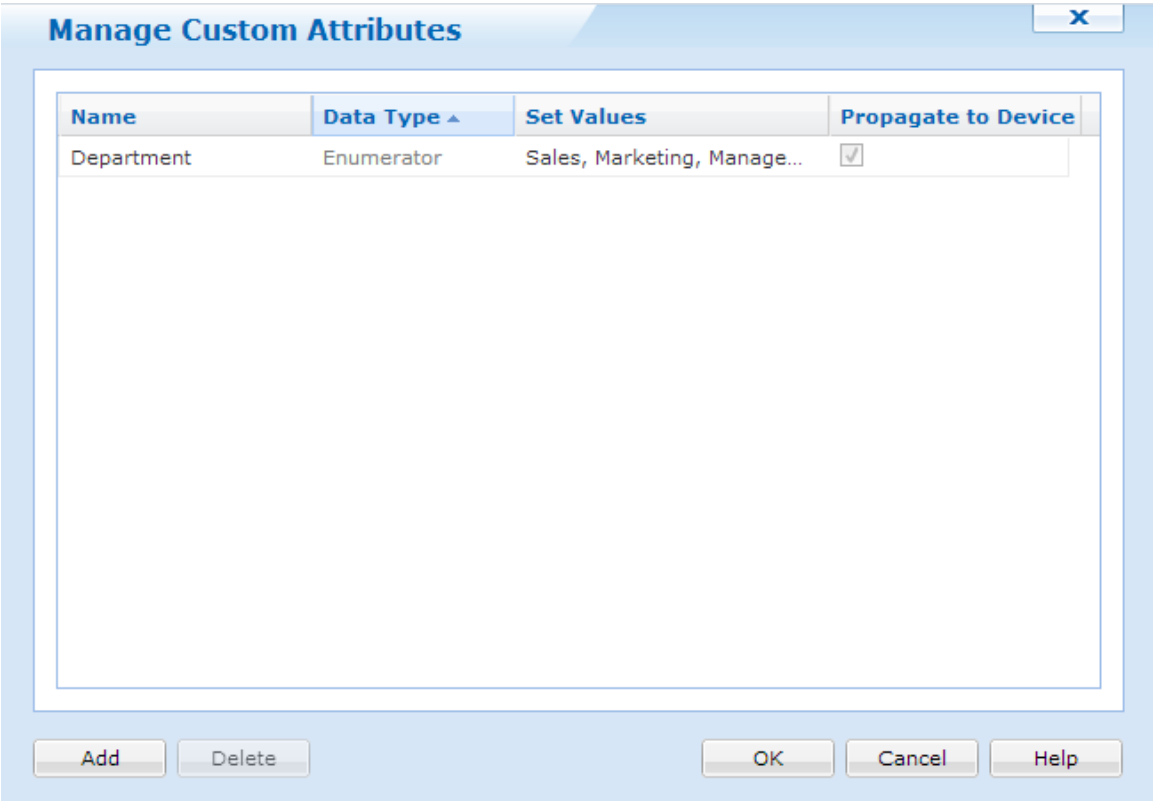
The name column shows the name of the Custom Attribute that will be shown in the info panel. Value contains the actual attribute for this field. Origin of value shows us where this field came from. For example, if Custom Attributes were set at the root level of the device tree, the origin of value will show the root level device group.

Clicking **Override** will change the origin of value to that where the device resides. This is useful if attributes change for each device. The Override button will change to **Remote Override** if we want to inherit the value from a parent group.

To create new attributes, click **Manage Custom Attributes**.

Manage Custom Attributes

When Manage Custom Attributes is clicked we a new dialog box appears. Here we will be able to create the Custom Attributes.



Manage Custom Attributes

Click Add to add a new attribute.

When Add is clicked, a new row will appear. Clicking the field under name will allow us to name this attribute.

Data Types

There are 5 available data types to have for Custom Attributes:

- Text
- Numeric
- Date
- Boolean
- Enumerator

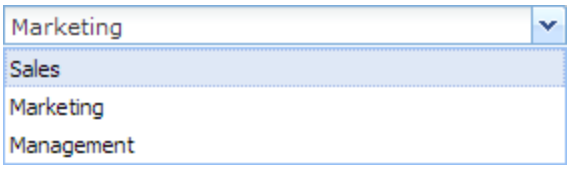
Text will allow us to create values with **letters and numbers**.

Numeric will allow us to create values with **only numbers**.

Date will allow us to set dates.

Boolean will create a checkbox for **yes or no / true or false**.

If we select enumerator, this allows us to create a drop down list when we set the attribute. To create the list, click the field in **Set Values** column. Here we can type the items we want in the drop down list. **Each value must be separated with a comma (,)**. For example, if we want to create a department attribute, we can have Sales, Marketing, Management. When we set this attribute, we will be presented with the drop down.



Enumerator Example

Propagate to Device

Checking this off will have MobiControl create the Custom Attributes in the pdb.ini file on the device. Applications can then read this file and pull the Custom Attribute value.

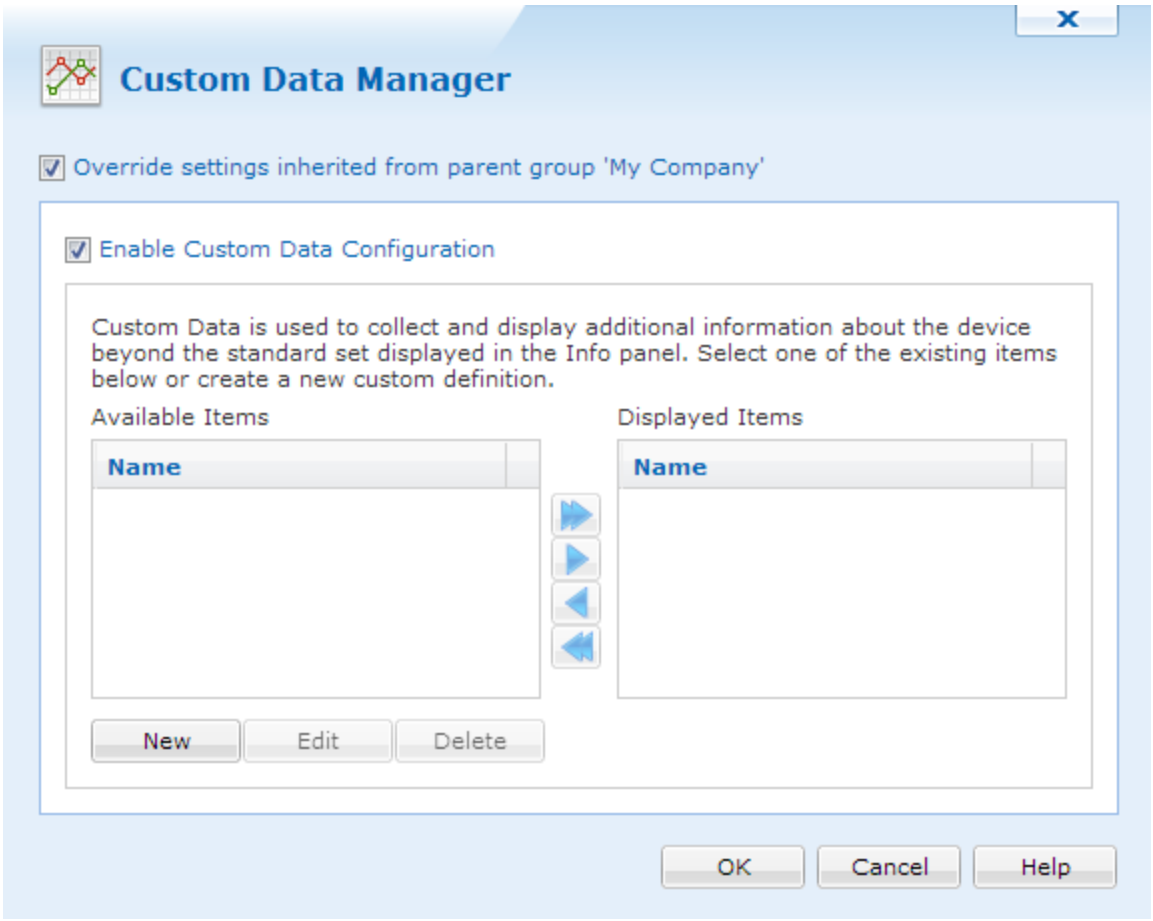
Bulk Import

If there is a large amount of Custom Attributes to be inserted, we can do a bulk import so that everything is added at once.

Once everything is set, click OK to save and close the Custom Attributes.

Android+ Custom Data

The custom data feature in MobiControl allows users to create their own monitoring fields to be shown in the **Device Info** window. This can be useful for monitoring various aspects of third-party applications. Custom data values are refreshed from the device when the device reconnects to the MobiControl Deployment Server and periodically, while the device status is Online, based on the device update schedule.



Custom Data Manager

The Custom Data Manager is accessible by right-clicking on a device or group, then selecting **Advanced Settings** and clicking **Custom Data**.

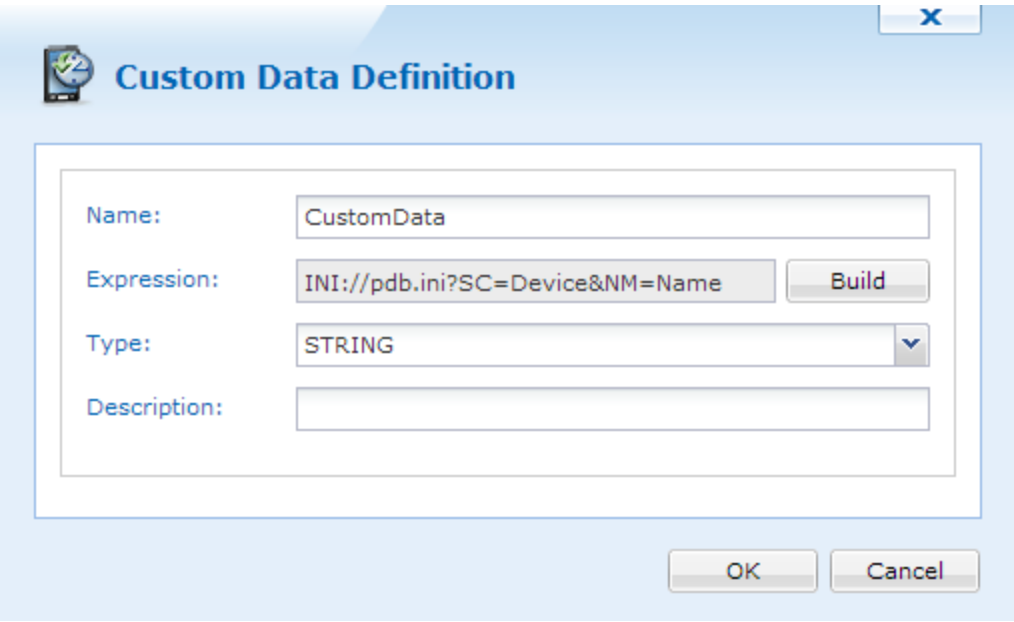
The following custom data type is available for Android+ devices:

Type	Format and Description	Example
.INI File	`<Key>=INI://\<FileName>?SC=<SectionName>&NM=<ValueName>` Get a value from a Section in an `.ini` file.	`INI://\%SDCARD%SOTI\pdb.ini?SC=Device&NM=DeviceName`

Editing Custom Data

Configuration of custom data entries is performed through the Custom Data Manager which can be accessed by highlighting the device or the device group and selecting **Custom Data** from the **Advanced Settings** option in the **Device** menu.

You can use the buttons in the **Custom Data Setting Manager** dialog box to add new entries, edit existing entries and change the order position of the custom data entries as displayed in the **Info** window.

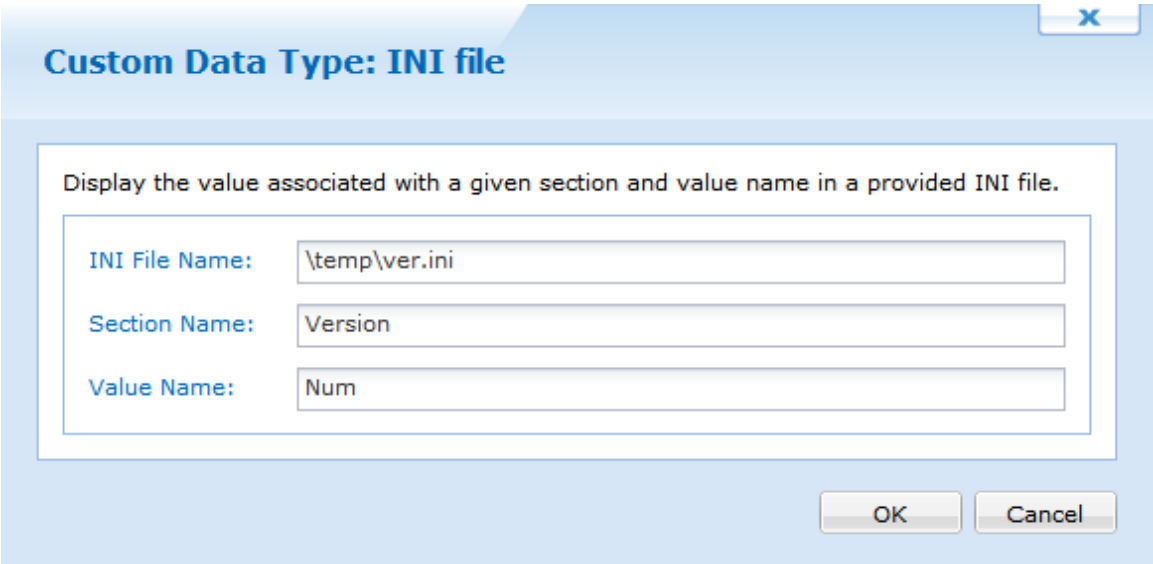


Custom Data Definitions window

The following table describes the fields in the **Custom Data Definition** dialog box.

Field Name	Description
Name	Name of the custom data field that you want to show in the device info pane
Expression	The build button can be used to create a definition which will be used to collect the custom data values.
Type	"STRING" is the setting recommended when doing custom data collection. Other options are "FLOAT" and "INTEGER."
Description	A brief note describing the nature of the custom data query and its purpose. This description is shown in the device info pane when the custom data field is selected.

Custom Data: .ini File



The following table describes the fields in the **Custom Data Type: INI File** dialog box.

NOTE:

To target the device storage card, type %SDCARD% before the location of the file.

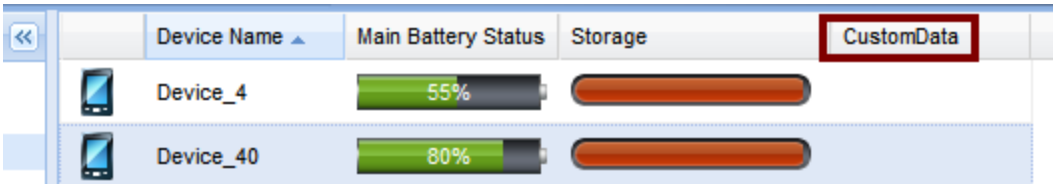
Field Name	Description
INI File Name	Location of the `.ini` file on the mobile device
Section Name	Section from which the value should be read
Value Name	Value that should be read from the `.ini` file and displayed in the custom data field in the Device Info panel

Limitations

- All result values are limited to 250 characters. They will be truncated if this limit is exceeded.
- All Query Key Names are limited to 80 characters.
- All query strings (URLs) are limited to 250 characters.

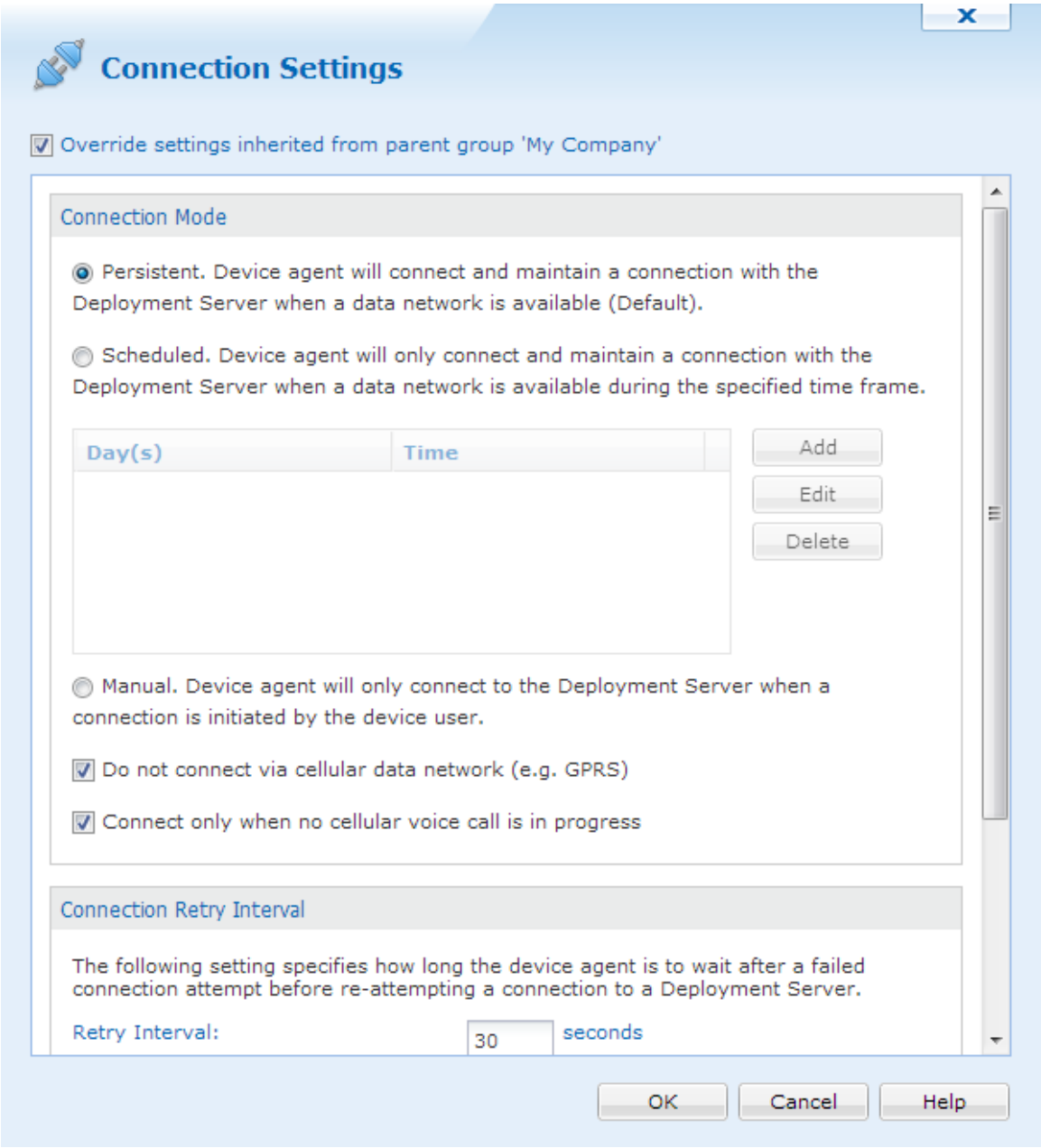
Custom Data Device Column

Once custom data has been configured, you can display or hide these custom data. Right-click on the device tree header or white space in the device tree and select **Custom Data**. You can also choose to display or hide the predefined data values displayed in the list.



Android+ Connection Settings

To access the **Connection Settings** dialog box, right-click on a device or device group, point to **Advanced Settings,** and select **Connection Settings.**



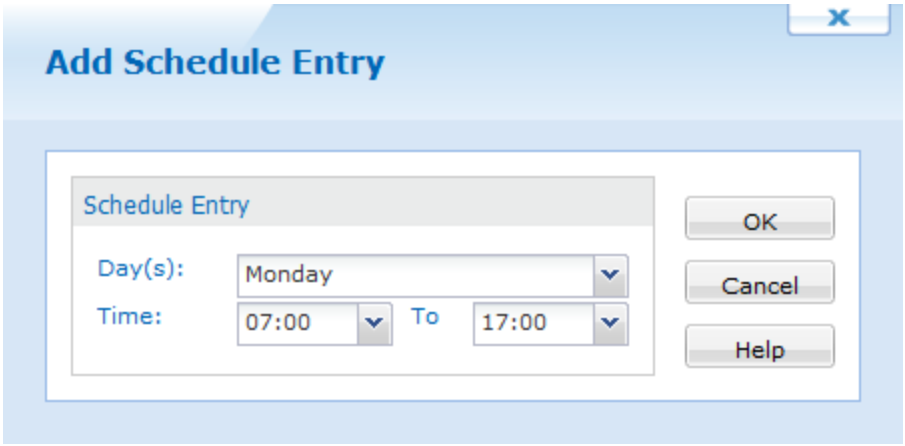
Connection Settings tab

Connection Mode

In any connection mode, the Device Agent does not force the mobile device to establish a network connection; it only takes advantage of an existing network connection.

Option	Description
Persistent	In this mode of operation the Device Agent will persistently try to establish and maintain a TCP/IP connection with the Deployment Server. This maximizes the amount of time the device is connected to MobiControl, ensuring that it is able to quickly receive updates and available for remote control.

Option	Description
	This is the recommended mode of operation for most installations.
Scheduled	In this mode of operation the Device Agent will only attempt to establish and maintain a TCP/IP connection with the Deployment Server during the defined time periods. Within the set time periods, the Device Agent operates in a "persistent" mode. Outside of the set time periods, the Device Agent will remain disconnected from the Deployment Server unless a connection is manually initiated by the device user. This is the recommended mode of operation for installations where it is not necessary for the device to always be connected to the Deployment Server. It is important that the time frame configured takes into consideration the device update schedule, and file synchronization schedules. These schedules can only be executed when the device is connected to the Deployment Server. **TIP:** If you are experiencing aggressive battery consumption with the persistent connection mode, switch to the Scheduled mode, and specify a narrow time frame (e.g. 1–2 hours)
Manual	In this mode of operation the Device Agent will never automatically attempt to establish a connection to the Deployment Server. Connections must be initiated by the device user via the device configuration applet. This is the recommended mode of operation for installations where only the remote help desk facilities of MobiControl are being used (not using deployment rules or file sync rules), and it is acceptable and/or required that the device user initiate the connection to the Deployment Server.



Add Schedule Entry settings dialog box

Connection Retry Interval

This setting determines how long the Device Agent should wait before trying to contact the Deployment Server again after a failed attempt. If your device will experience long periods disconnected from the Deployment Server, you should set this value high in order to prevent battery drain.

Option	Description
Allow Inbound TCP/IP(DIRECT) Remote Control Connections	This box needs to be checked if you intend to connect to your mobile device using the **TCP/IP (DIRECT)** connection mode. This option will enable the **Allow Inbound TCP/IP Connections** option in the Device Agent on the mobile device.

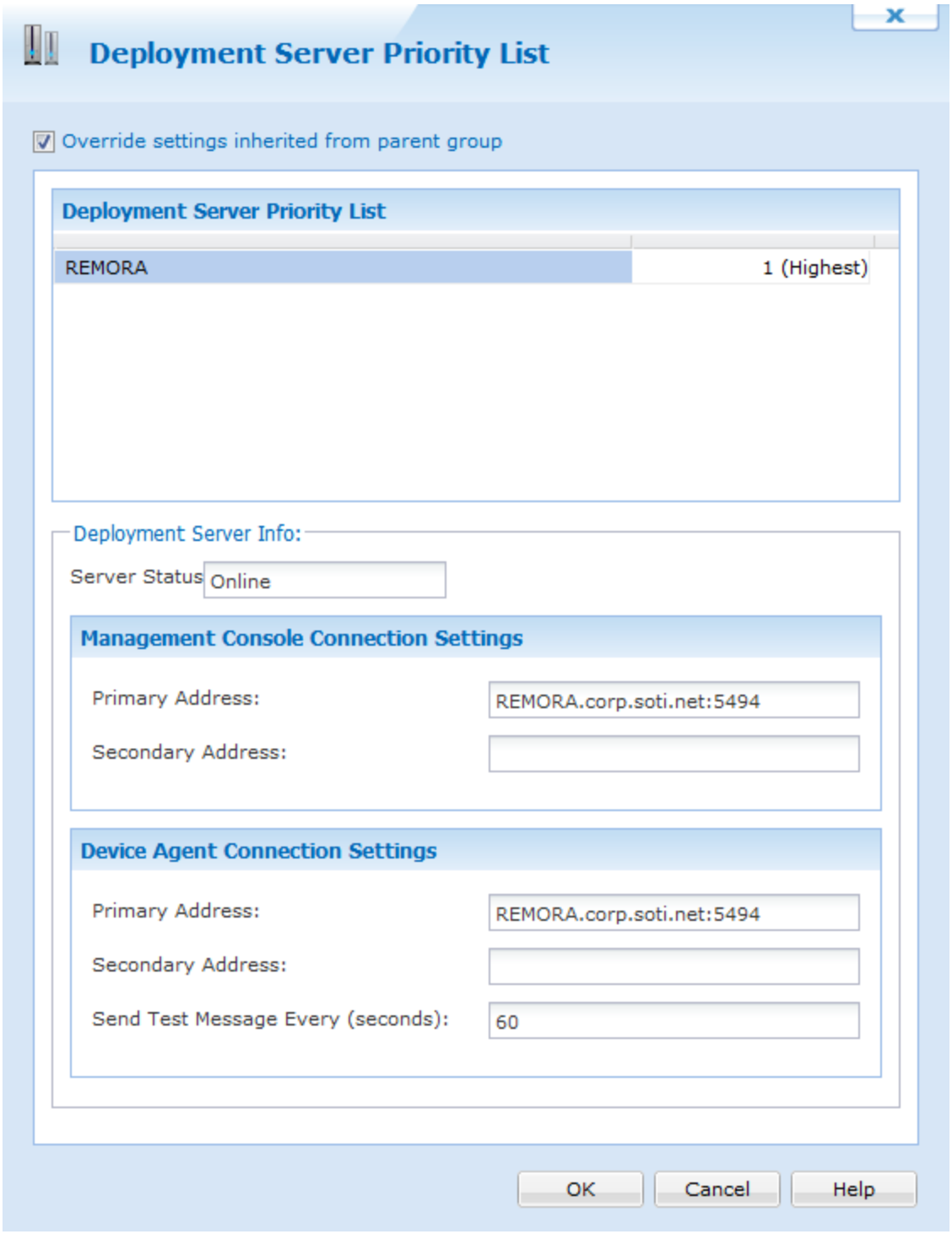
Log File Management

This set of options allows you to tune how the debug log files are managed on the device. Log management works by waiting for the log file to grow to a maximum threshold. Once the given threshold is met, the log file size is reduced down to the given minimum threshold by purging all the older entries.

Option	Description
Minimum Log File Size	Threshold size up to which the log file will be purged.
Maximum Log File Size	Threshold size, reaching which will trigger the log file to be purged to the minimum log file size
Enable Debug Logging (Normally Off)	Enables event logging on the mobile device. All MobiControl-related activity and events will be logged to a log file.The log file can provide vital information to IT support staff in diagnostics and resolving any issues that might have been reported for the mobile device with respect to MobiControl. The mobile device may operate more slowly with this option checked.

Android+ Deployment Server Priority

The **Deployment Server Priority List** dialog box allows you to specify the Deployment Server preferences for the devices. Priority one is the highest and five is the lowest. When a device is configured with more than one Deployment Server, it will try to connect to highest priority one first. If this server is not accessible, then it will try to connect to the next server available.



Deployment Server Priority List dialog box

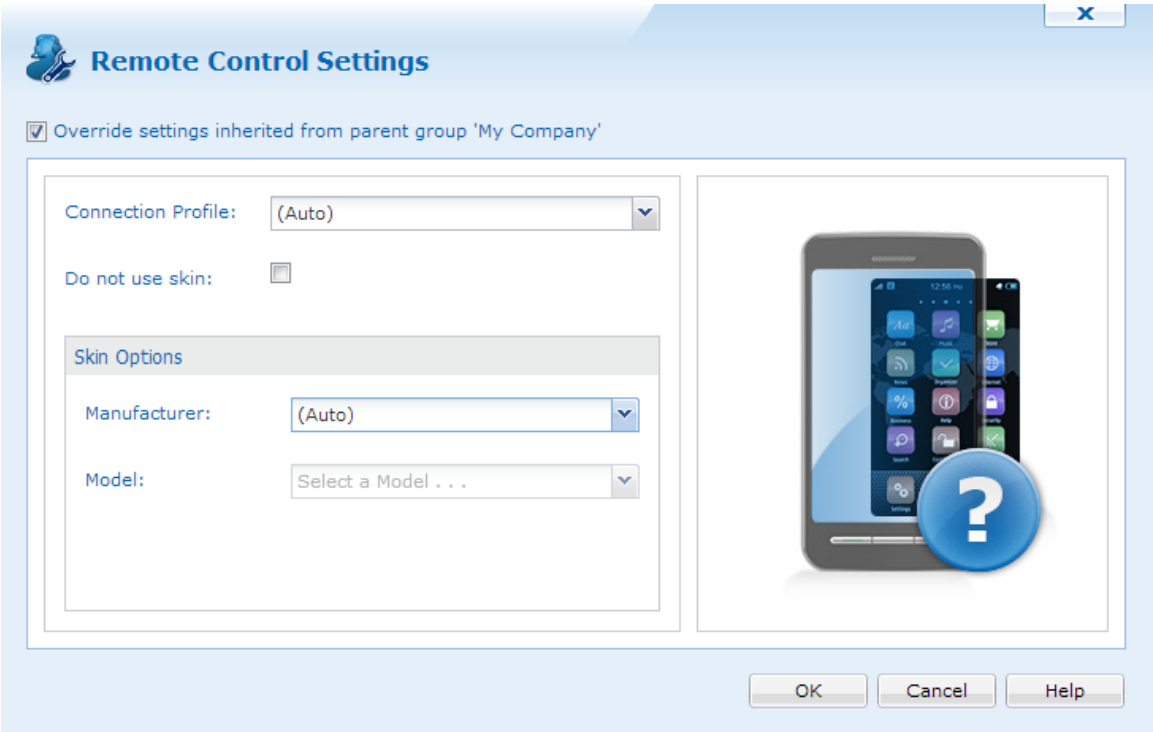
Multiple servers may be assigned the same priority level to establish a pool of Deployment Servers to balance the load of a large number of devices.

If you select "Not used," the selected devices will not connect to that Deployment Server.

Deployment Server priority is only applicable when you have installed multiple Deployment Servers using the same site name.

Android+ Remote Control Settings

In the **Remote Control Settings** dialog box, it's possible to select a device skins and connection profiles. Skins for these devices should appear automatically depending on the device model.



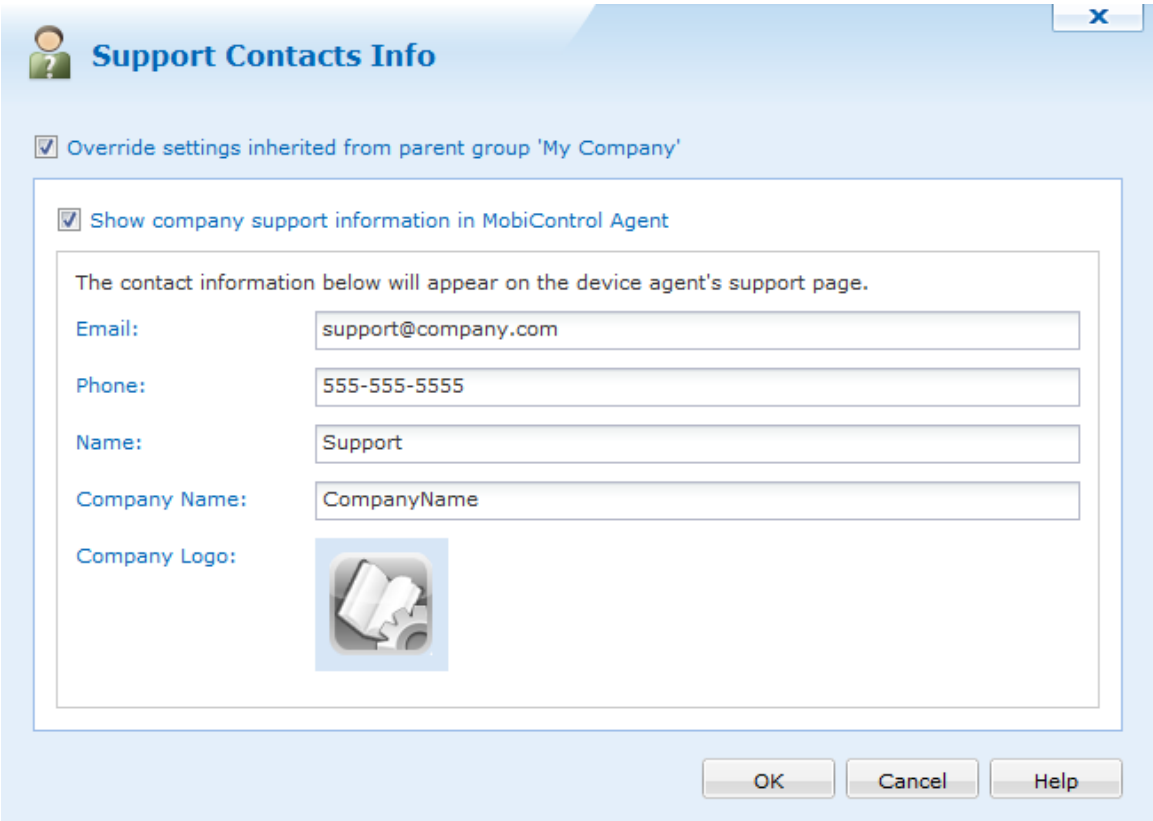
Remote Control Settings dialog box

The following table describes fields in the **Remote Control Settings** dialog box.

Field Name	Description
Connection Profile	This field allows the user to configure the type of connection that will be used for remote control sessions. The available connection types are Auto, ActiveSync, TCP/IP (SERVER) (recommended), TCP/IP(DIRECT), and <Prompt on Connect>.
Do not Use Skin	Checking this off will remove the skin from the device when remote controlling it.
Manufacturer, Model, and Skin Preview	A skin is an image of the body of your mobile device, which mimics the physical device on your desktop screen. Displaying your device in a skin gives you access to most of the physical buttons of the device. It can be useful in training or presentations. Skins should automatically be applied to devices depending on the device model. If another skin is wanted to be used, select the manufacturer and model of your device to have its skin be displayed in a remote control session. Skins for most Windows Mobile, Pocket PC and CE .NET based mobile devices are available. We are always adding new skins to our online collection, but if your device is not listed, please contact us to let us know which device you are using.

Android Support Contacts Info

The Support Contacts Info panel allows us to set contact information when a user opens up the MobiControl agent on their device. Information that we are able to configure are Email, Phone, Name, Company name and a company logo.



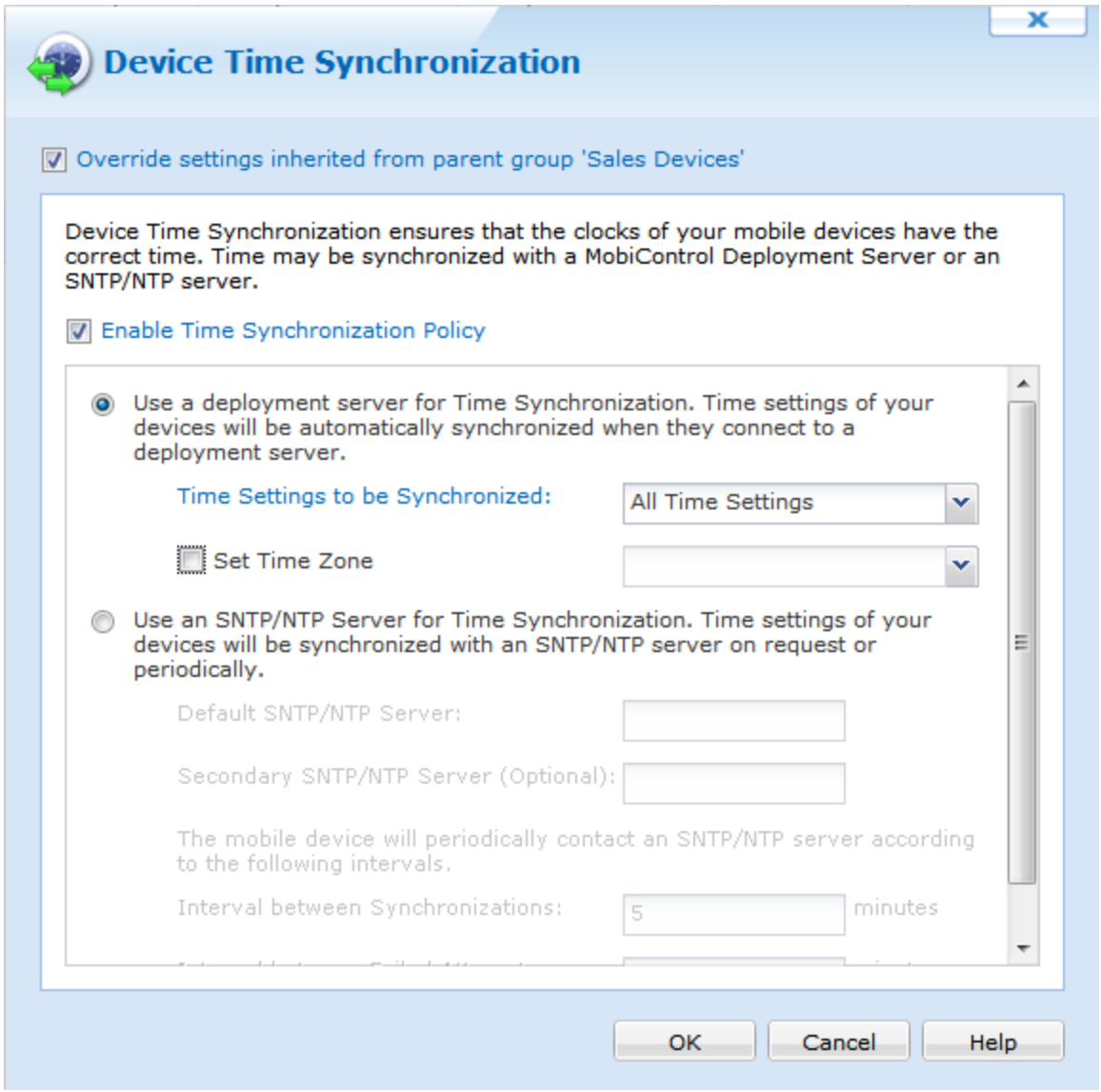
Support Contacts Info dialog box

When each of the fields are set and OK is pressed, this information will then be sent down to the devices where this was configured on. When a user opens up their MobiControl agent and goes to the support info tab, they will be able to see the appropriate information.

Android+ Time Synchronization

This feature allows you to enable time synchronization for a mobile device, allowing the device to update its date and time settings by periodically synchronizing them with an SNTP/NTP time server or the MobiControl Deployment Server.

To configure the time synchronization settings for a device or device group, select the device or group in the device tree and click **Device,** click **Configure Device(s),** and click **Time Synchronization.**



Device Time Synchronization dialog box

Time Synchronization Settings

There are three different modes available for time synchronization:

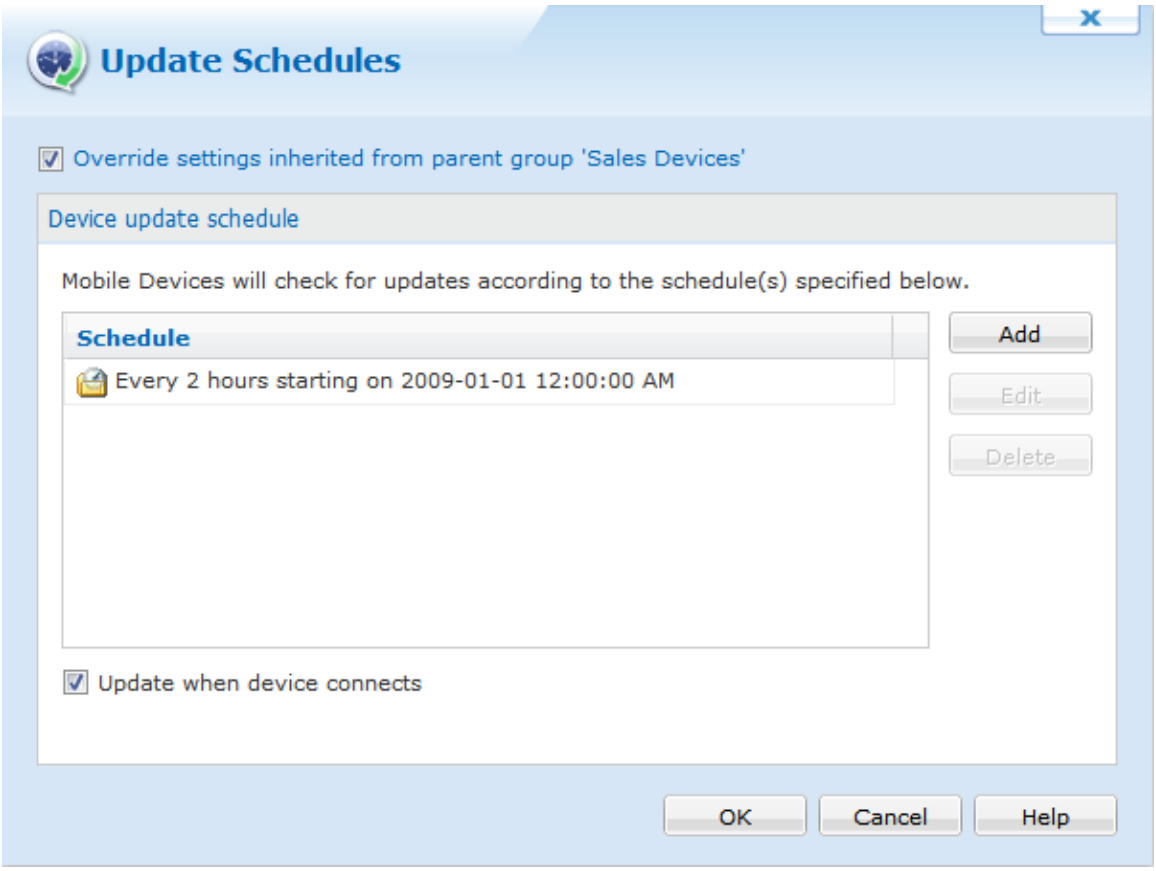
Option	Description
No Time Synchronization	The device time is not synchronized with any server.
Use a Deployment Server for Time Synchronization	The device will synchronize its time with a MobiControl Deployment Server when it connects to it. The time settings available for synchronization include Time Only, and All Time settings: • The **Time Only** option will result in the date and time being synchronized (but not the time zone) • The **All Time Settings** option will sync all of the time settings including DST, time zone, date, and time. • The **Set Time Zone** option to set the time zone for mobile devices which are in a different time zone than the Deployment Server. You can use this on device level or group level.
Use an SNTP/NTP server for Time Synchronization	The device will synchronize its time with the SNTP/NTP server(s) specified in the **Default SNTP/NTP Server** and **Secondary SNTP/NTP Server** fields. When this mode is selected, the option to synchronize automatically becomes available. With automatic synchronization enabled, the device will synchronize its time according to the interval specified in the **Interval between Synchronizations** field. If an automatic synchronization fails, the device will retry after the time interval specified in **Interval between Failed Attempts** has elapsed. **NOTE:** SNTP/NTP Server does not synchronize DST settings. It's similar to time only.

Android+ Device Update Schedule

The device update schedule specifies when the device(s) should query the Deployment Server(s) for updates. Updates may include the addition, update, or removal of packages and modifications to device settings.

If the Deployment Server determines there are pending updates for the device, it immediately sends them to the device. The device also sends the Deployment Server a summary of its installed packages and settings. If the Deployment Server identifies an inconsistency, such as a previously-installed package that is missing on the device, the Deployment Server will re-install the package.

The initial device update schedule is specified by the add devices rule used to add the device(s) to the system. You may edit the schedule for an individual device or a group of devices that have been added to the system by selecting the target device or group in the device tree view in the main console window and selecting **Update Schedules** from the **Configure Device(s)** sub-menu.



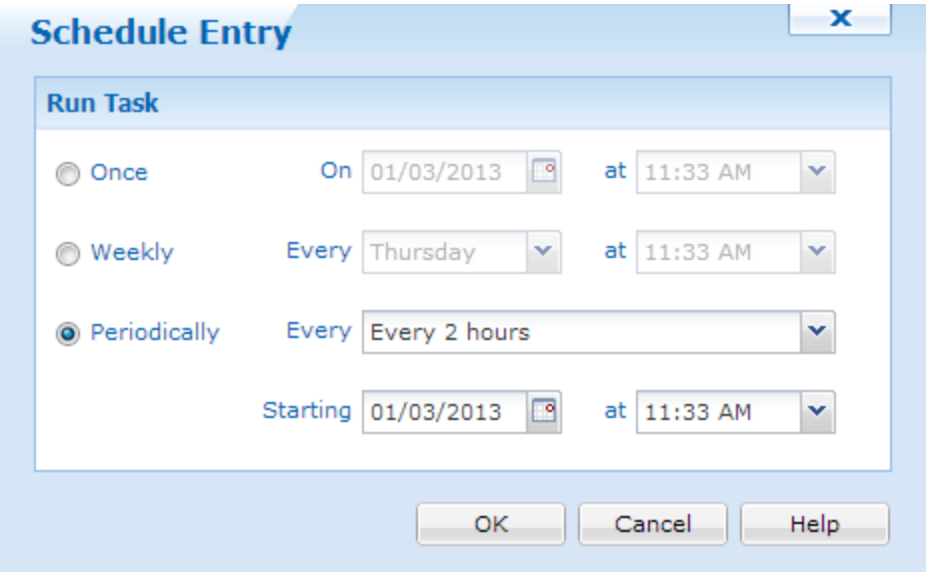
Device Update Schedules dialog box

The following table describes the **Device Update Schedules** dialog box:

Field Name	Description
Add	Select **Add** to specify additional update intervals. The **Schedule Entry** dialog box will be displayed. **EXAMPLE:** To sync a device twice a week, Monday at 06:00 and Friday at 19:00, create two weekly schedule entries.
Edit	Select **Edit** to modify an existing schedule entry. The **Schedule Entry** dialog box will be displayed.
Delete	Select **Delete** to permanently remove an update schedule entry from the dialog box.
Update when device connects	Select this check box to have the device(s) check for updates whenever they connect to a Deployment Server, that is, at every transition from offline to online. If this check box is not selected, the device(s) will only check for updates according to the schedule defined above.

Schedule Entry

The **Schedule Entry** dialog box allows you to specify schedule entries as one-time or periodic events.



Schedule Entry dialog box

Field Name	Description
Once	The device will check for updates once at the specified date and time.
Weekly	The device will check for updates once a week, on a specific day at a specific time.
Periodically	The device will check for updates periodically, at the specified interval from the set start date and time.

Android+ Sending Messages and Scripts

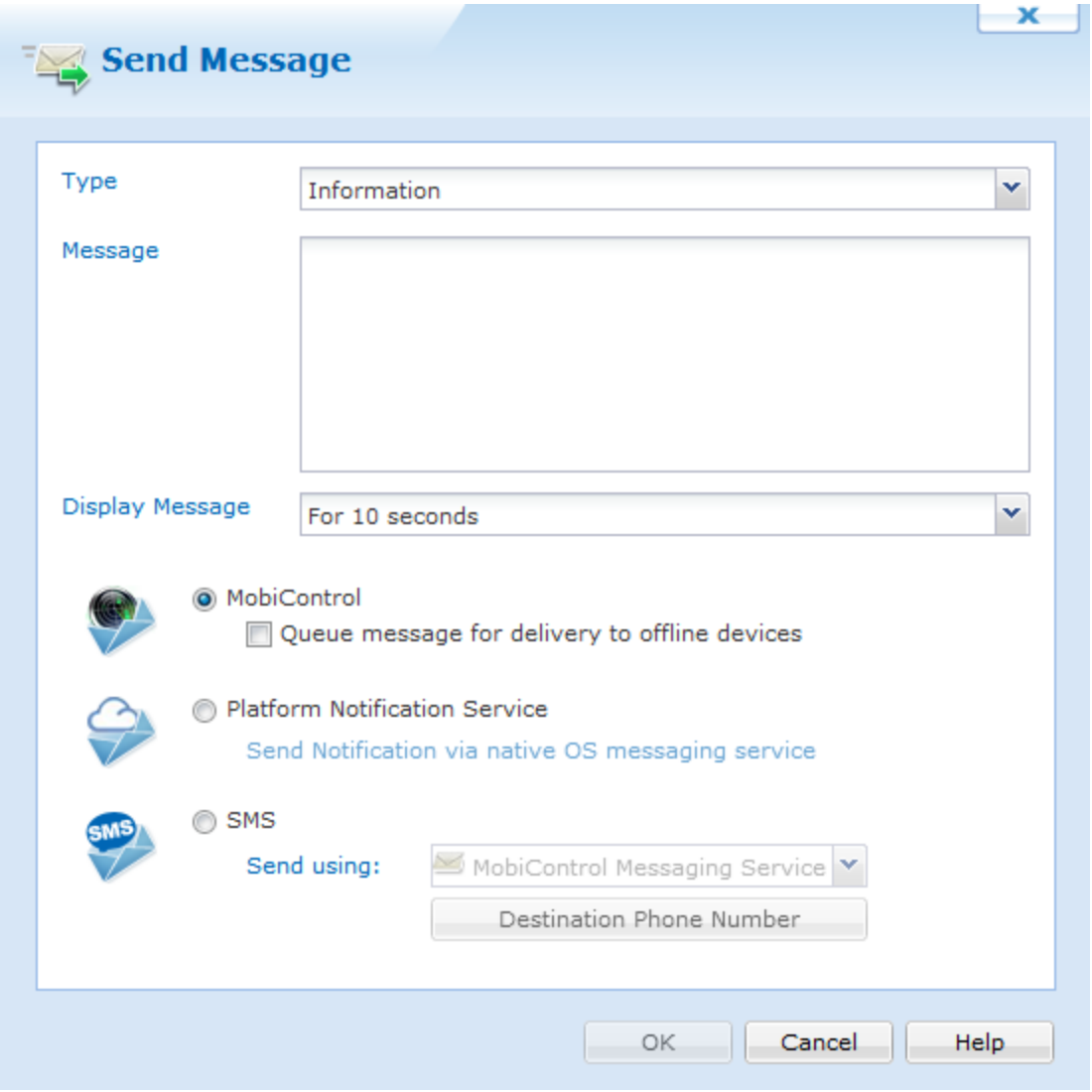
Select this option to send a message or script to one or more mobile devices. These can be sent using MobiControl or SMS (Short Message Service) from any online device or device connected via ActiveSync device. This feature can be used to keep users informed or updated remotely.

In the MobiControl Manager, right-click on a device, select **Send** and click **Message** or **Script** to start sending messages to the mobile devices. You can also choose to soft rest or turn off or suspend the device.

If your mobile device can receive SMS messages, MobiControl offers a way to send messages to the device through text messages.

IMPORTANT:

Only messages can be sent through SMS for Android devices. Sending SMS scripts to devices is only supported by Windows Mobile. To view how to send scripts to Windows Mobile devices by SMS, click here.



Send Message dialog box displaying the different message types

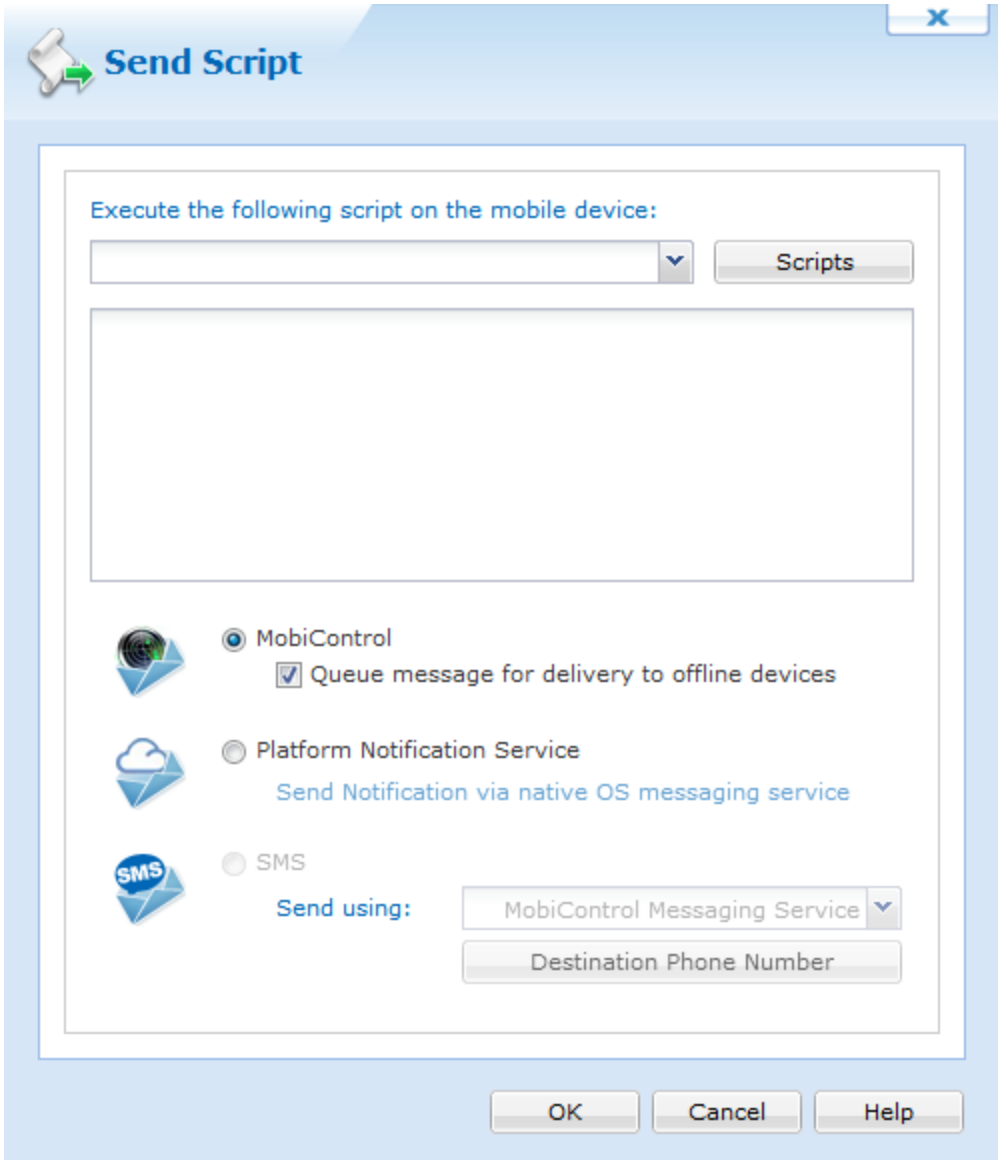
The table below describes each individual field of the **Send Message** dialog box:

Field Name	Description
Message Type	From the drop-down box, select the type of message you wish to send (information, exclamation, question, or error).
Message	A brief note to the recipient
Display the message on the device(s)	Select a time intervals for which the message can be displayed on the device.
MobiControl	Sends the messages via MobiControl. There is no character limit with this option.
Queue message	Sends the message to devices that are offline and will receive the message when they come online. The message will be stamped with the date and time it was sent.

Field Name	Description
for delivery to offline devices	
SMS (Short Message Service)	Send the message via SMS text message.
Send Using	Send a message using MobiControl's messaging service.
Destination Phone Number (s)	This is where the message will be delivered. This area is populated with the phone number(s) of the device you selected. If no phone number is present, you can double click the phone number area and manually enter a number.

Sending Scripts to the Device

If you want to run a custom script on a mobile device, you can do so with MobiControl. In the **Script** box, you can enter the script commands and instructions that you want to run on the device. When the instructions are received by the mobile device, it will then execute the script commands. These instructions can be sent using MobiControl or the device's platform notification service.



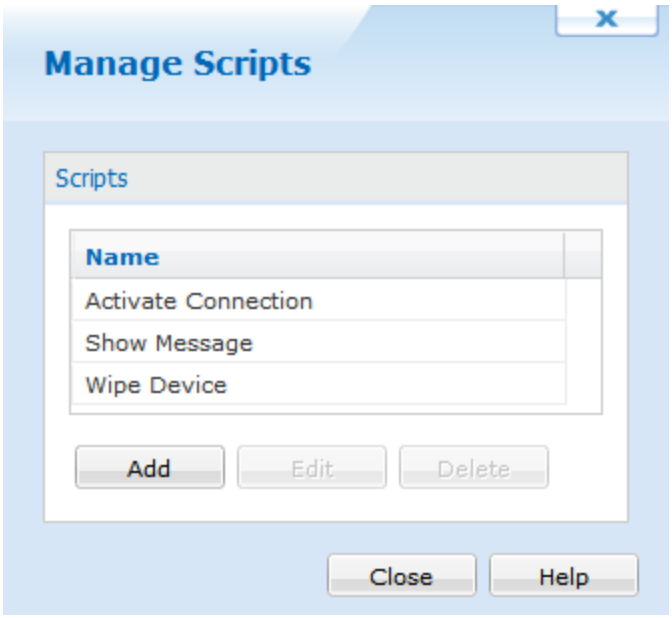
Send Script dialog box

The table below describes each individual field of the **Send Script** dialog box:

Field Name	Description
Scripts Drop Down	Select a pre-built script from the drop-down menu. Clicking the **Scripts** button opens the **Manage Scripts** dialog box where you can manage scripts. Please see the "Android+ Script Manager" topic below for more information.
Script	Preview or edit the select script
MobiControl	Sends the messages via MobiControl. There is no character limit with this option.
Queue message for delivery to offline devices	Sends the message to devices that are offline and will receive the message when they come online. The message will be stamped with the date and time it was sent.
Platform Notification Service	Sends the script message via GCM.

Android+ Script Manager

You can use the **Manage Scripts** dialog box to centrally manage all of the scripts that you are using within MobiControl. The Script Manager comes pre-built with four of the most commonly used scripts. Each one is fully customizable. The Activate Connection script connects the device to MobiControl and activates the data connection if it isn't present. The Log Event script is used to log an event with your Deployment Server. The Show Message script is used to display a message on the device, and the Wipe Device script is used to wipe the device. The scripts here are stored within the MobiControl database, and can be accessed with any MobiControl Manager console. One way to open the **Manage Scripts** dialog box is to right-click on a device or group, select **Send,** and click **Script.**

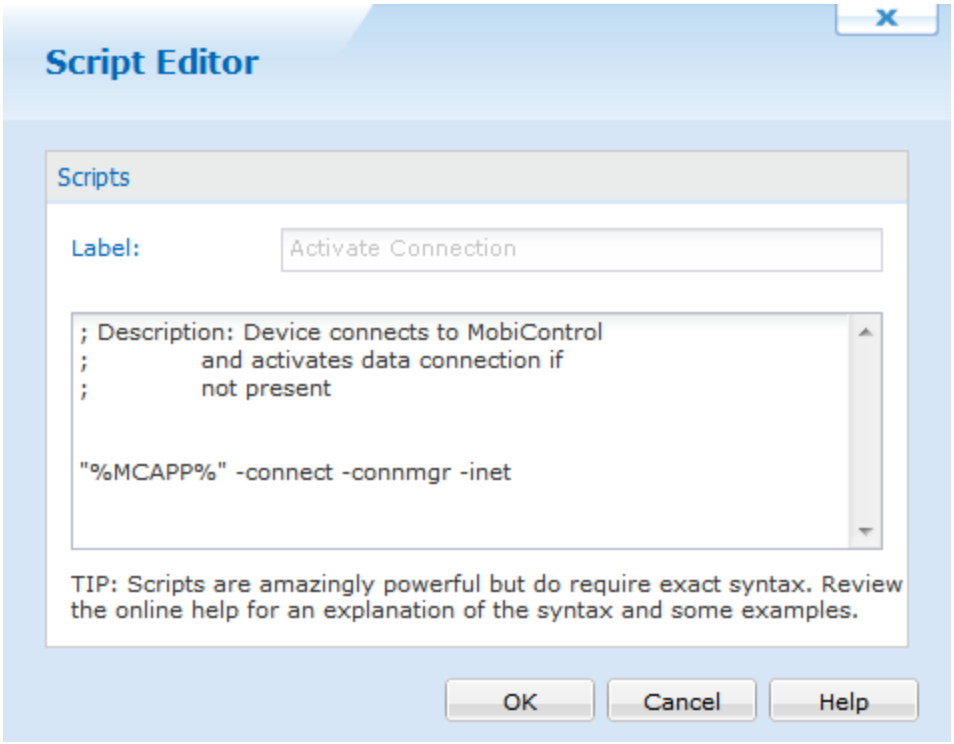


Manage Scripts dialog box

The following table describes the features of the **Manage Scripts** dialog box:

Field Name	Description
New	Creates a new script
Edit	Edits the selected script
Delete	Deletes the selected script
Import	Allows you to import a `.cmd` file containing MobiControl script commands. Please see the "Script Command Set" topic on page 72 for a full list of script commands.

Clicking the **New** button will bring up the **Script Editor** dialog box. In this window you can enter any script command that you would like to run on the device. Please see the "Script Command Set" topic on page 72 for a full list of script commands.



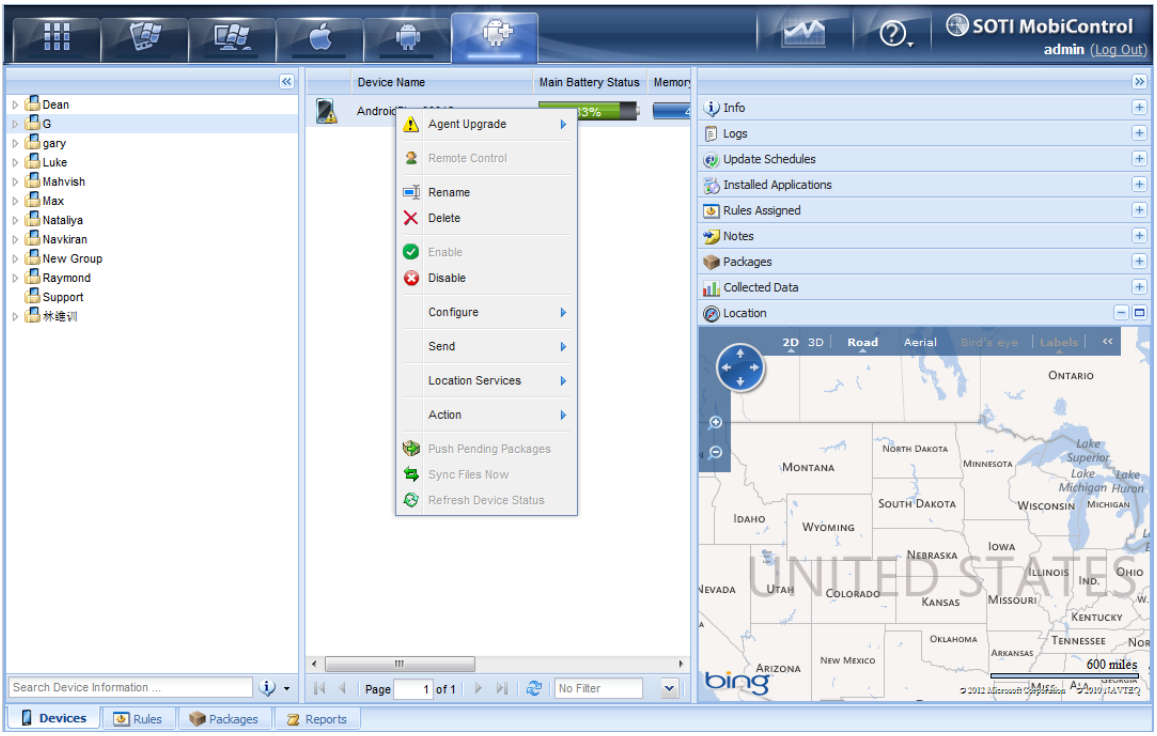
Script Editor dialog box

Android+ Location Services

MobiControl's Location Services provides the ability to locate and track mobile devices that are equipped with a GPS receiver that is internal or external to the unit. In order to locate a device, the GPS must be enabled and correctly configured on your device. The GPS determines the current location based on its

position relative to orbiting satellites. In order for this to happen, the device requires a clear view of the sky. Determining location may not be possible if the device is inside buildings or has an obstructed view of the sky.

You can activate Location Services for a device in MobiControl by right- clicking on a device and selecting the **Location Services** option from the menu. The first time you select an option from the Location Services menu for a device, it will automatically use the next available license. If there are no more licenses available, you will be notified to contact SOTI for information on acquiring additional licenses for Location Services.



Android+ Location Services

Please See the "Contact Us" page to contact us for more details on acquiring additional licensing.

NOTES:

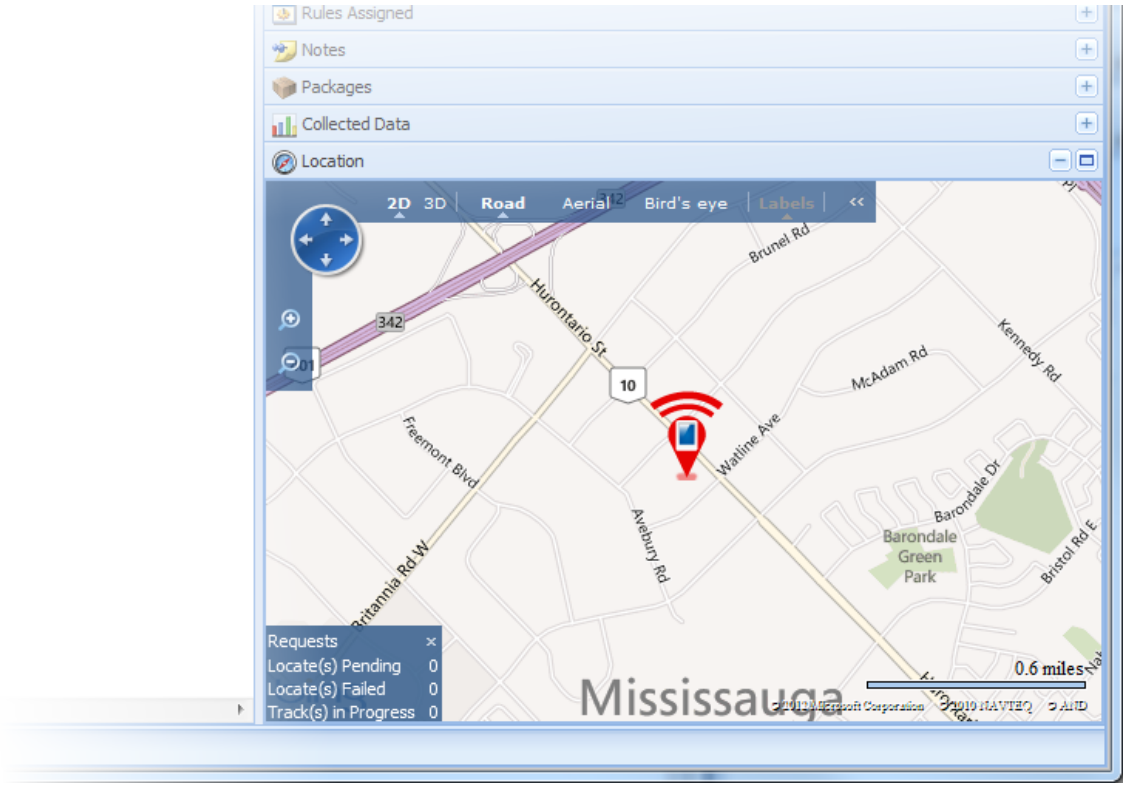
- When using Location Services in MobiControl to track devices, Internet Explorer 7 or higher is required.
- The Current Format for Regional and Language Options on your PC MUST be compatible with Bing Maps. Click here for a list of supported Bing Map control settings.

Android+ Locate Feature

To use the Locate feature in MobiControl's Location Services, right-click on the device you wish to locate, select **Location Services,** and click **Locate.**

The locate feature will use the GPS unit associated with your mobile device to determine the current latitude and longitude of the device. These coordinates are returned to MobiControl and displayed in the Location panel using Microsoft's Virtual Earth. The coordinates plotted in the Location panel represent the exact position of the device at the time of the request. To follow the position of the device in real time, use the **Track** option under the **Location Services** menu.

You can locate the position of multiple devices at once: select the parent folder or hold the CTRL key and select all the devices you wish to locate, right-click, select **Location Services,** and click on **Locate.** In order to use the Locate feature, the device(s) must be online and communicating with the MobiControl Deployment Server. The status of the current (and completed) Locate and Track commands is displayed in the lower left hand corner of the screen.



Location Services locate user interface

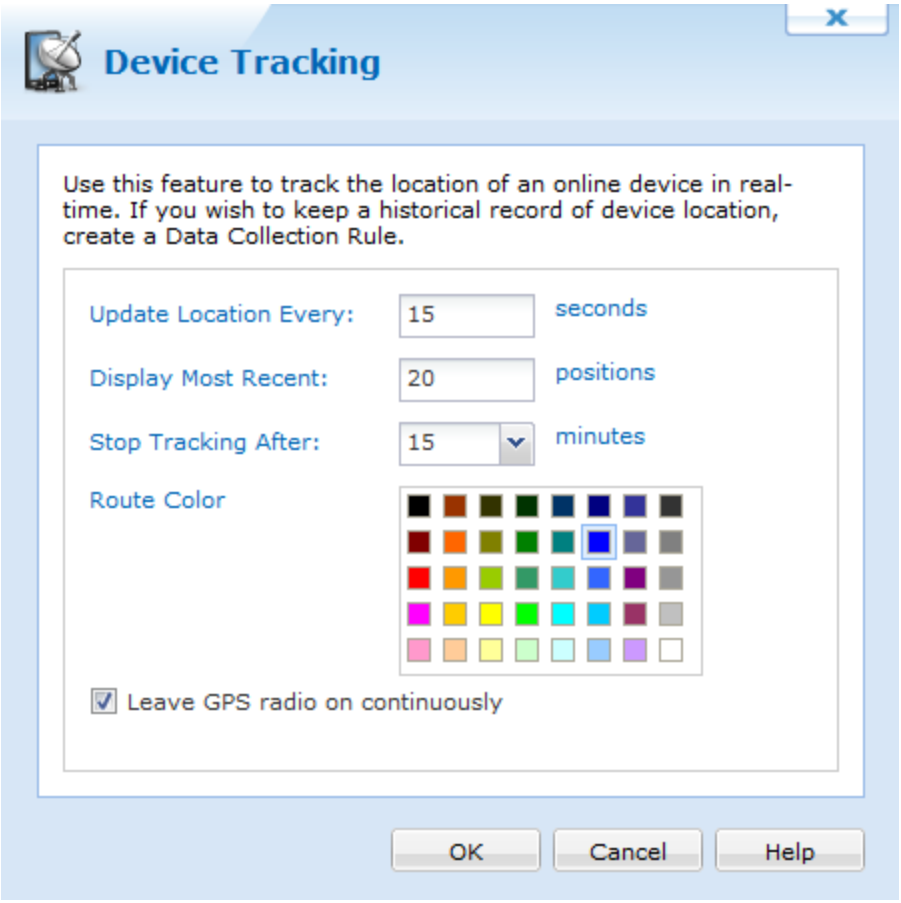
Th

NOTE:

If the MobiControl Manager is behind a proxy server and you are unable to use Location Services, please run the following command through the **Start** menu then **Run**:
`netsh winhttp set proxy -server="http=<ProxyServerIP>: <Port>; https=<SSLProxyServerIP>: <Port>"` (on Windows Vista, **with no spaces between the quotation marks**.)
This command will update the WinHTTP service with the settings from Internet Explorer.

Android+ Tracking

To use the Track feature in MobiControl's Location Services, right-click on the device you wish to track, select **Location Services,** and click **Track.**



Device Tracking dialog box

The track feature will use the GPS unit associated with your mobile device to determine the current latitude and longitude of the device at a given schedule and send the co-ordinates back to the MobiControl Deployment Server. These co-ordinates are then displayed in the Location panel using Microsoft's Virtual Earth. The co-ordinates plotted in the Location panel represent the exact position of the device at the time of the request along with where the device has been since the request was initiated. To view where the device has been in the past, you need to use the show history option within MobiControl's Location Services.

In order to use the track feature, the device must be online and communicating with the MobiControlDeployment Server.

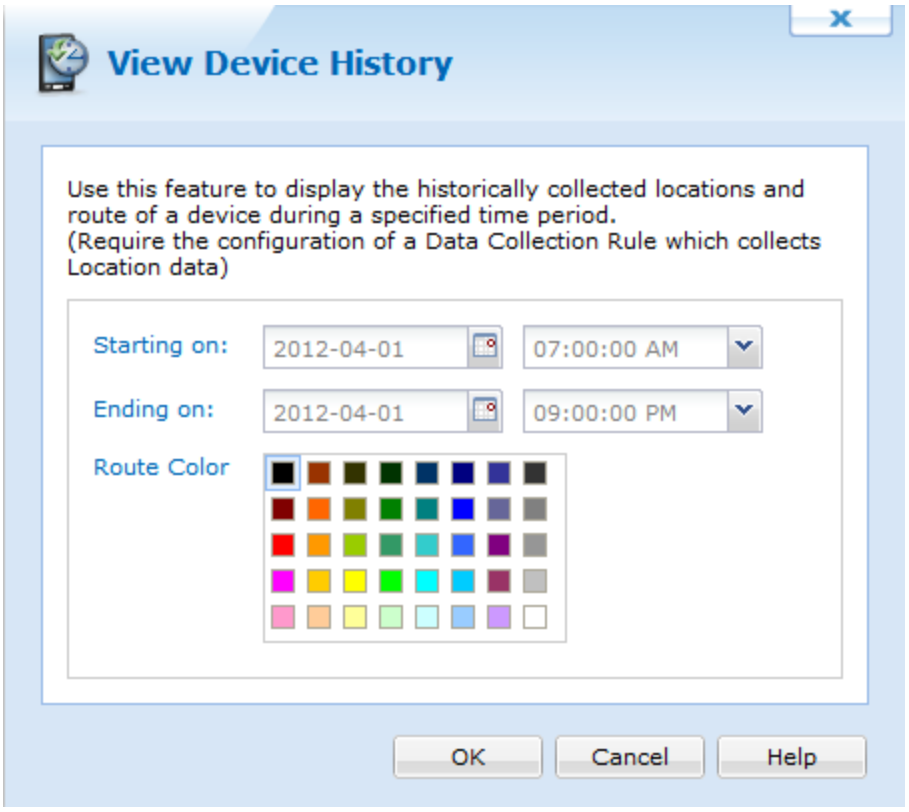
The following table describes each field in the dialog:

Feature	Description
Update Location Every	Set a time interval in seconds (5–86400) for how frequently you would like to have the device location reported.
Display Most Recent	Choose a value to represent the number of recent positions (maximum 100) that you would like to see plotted on the map of the device(s) that you will be tracking.
Stop Tracking After	Set the time interval in minutes (5– 60) for when you would like to end tracking the device.
Route Color	Identifies the device route you will be tracking
Leave GPS radio on continuously	For faster response time from the GPS radio on the device, you should enable this check box. The device's GPS radio will constantly be on.

Android+ Location History

The show history feature will use the GPS unit associated with your mobile device, allowing you to view where the device has been over a given period of time. To use this feature, you need to set up a data collection rule that collects the location information from the device on a given schedule. The data will be sent back to the deployment server, or, if there is no active data connection on the device, it will be collected and stored in a temporary file and then sent back to the server the next time the device connects. The show history feature does not require the device to be online and communicating with the MobiControl Deployment Server. You can plot information from the history that has been transmitted back to the server during the last active connection.

To use the show history feature, right-click on the device you wish to view, select **Location Services,** and click **Show History.** You will then be prompted to enter the time period for which information is desired, and the route color. Once this is filled in, click **OK** and the path will be plotted.

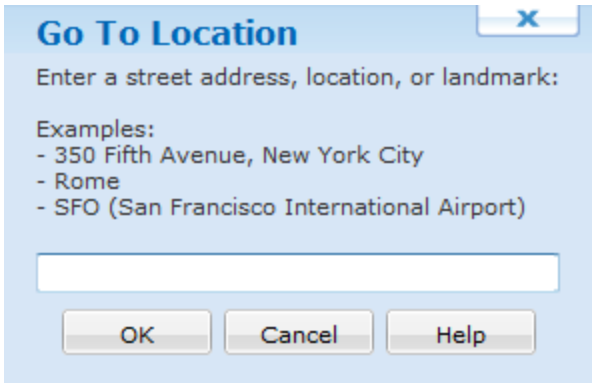


View Device History dialog box

Feature	Description
Starting On	Enter the date and time that you wish to start.
Ending On	Enter the date and time that you wish to stop.
Route Color	Select the color to be used on the map when connecting the co-ordinates.

Using Go To Location

Go To Location allows you to quickly centre and zoom the map to a specific location. Go To Location is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "Android+ Location Services" topic on page 1366 for more information.

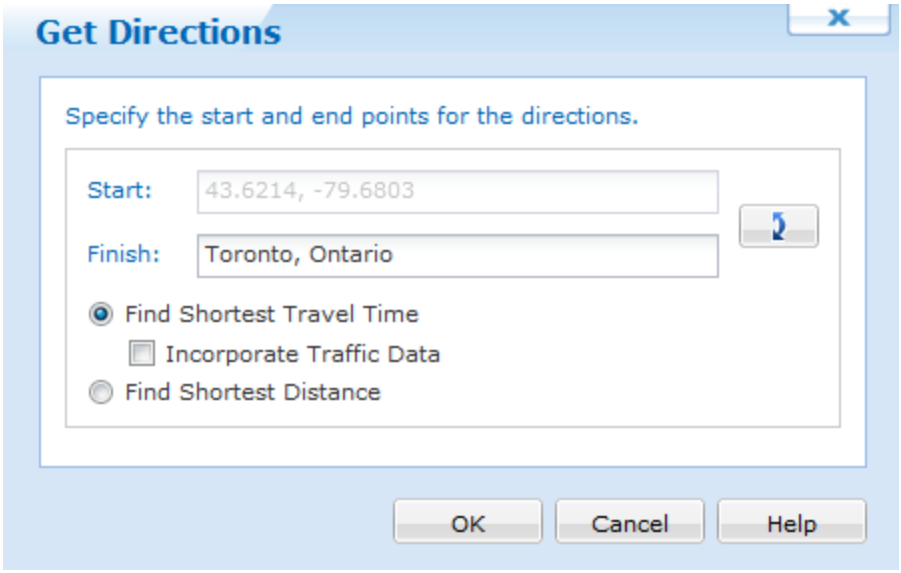


Go To Location dialog box

To use this feature, right click on the Location panel and select "Go To..." from the pop-up menu that appears to open the Go To Location window. You can then enter an address, location, landmark, or the name of an existing geofence. Once you have entered the location information, click the OK button and the map will reload centring on the information you provided. If you entered the name of an existing geofence, the map will change to the location of that geofence and display it on the screen in red.

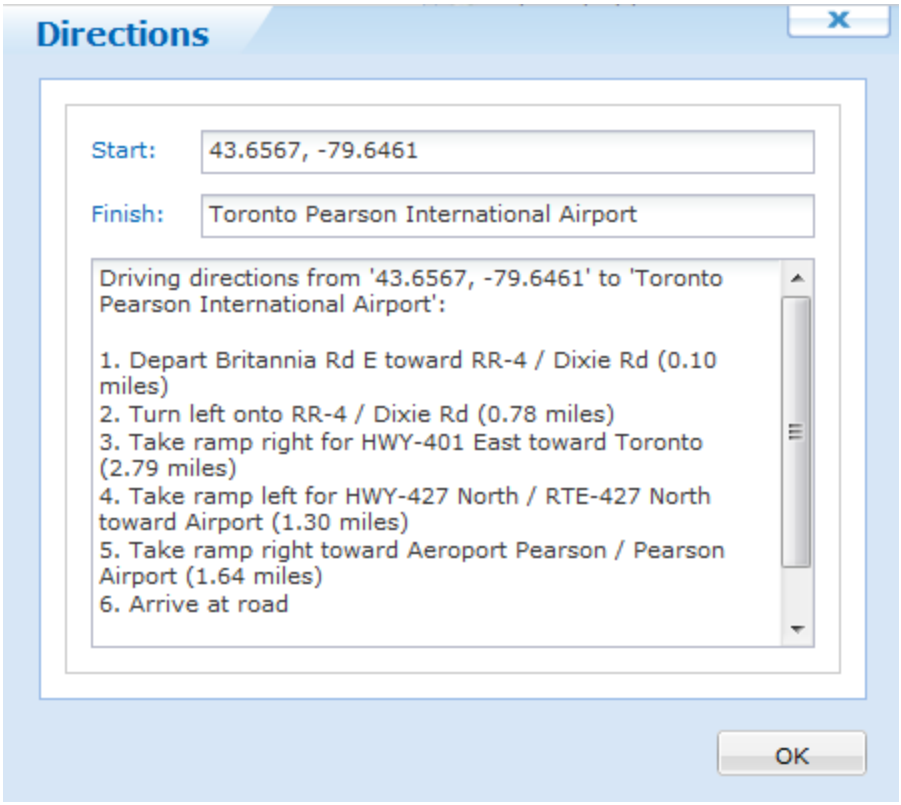
Android+ Get Directions

Powered by Microsoft's Bing Maps, MobiControl's Get Directions will return turn-by-turn directions between two locations on the map. These directions can be sent directly to the device, or they can be pasted into an email and sent to a larger group of people. Get Directions is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "Android+ Location Services" topic on page 1366 for more information.



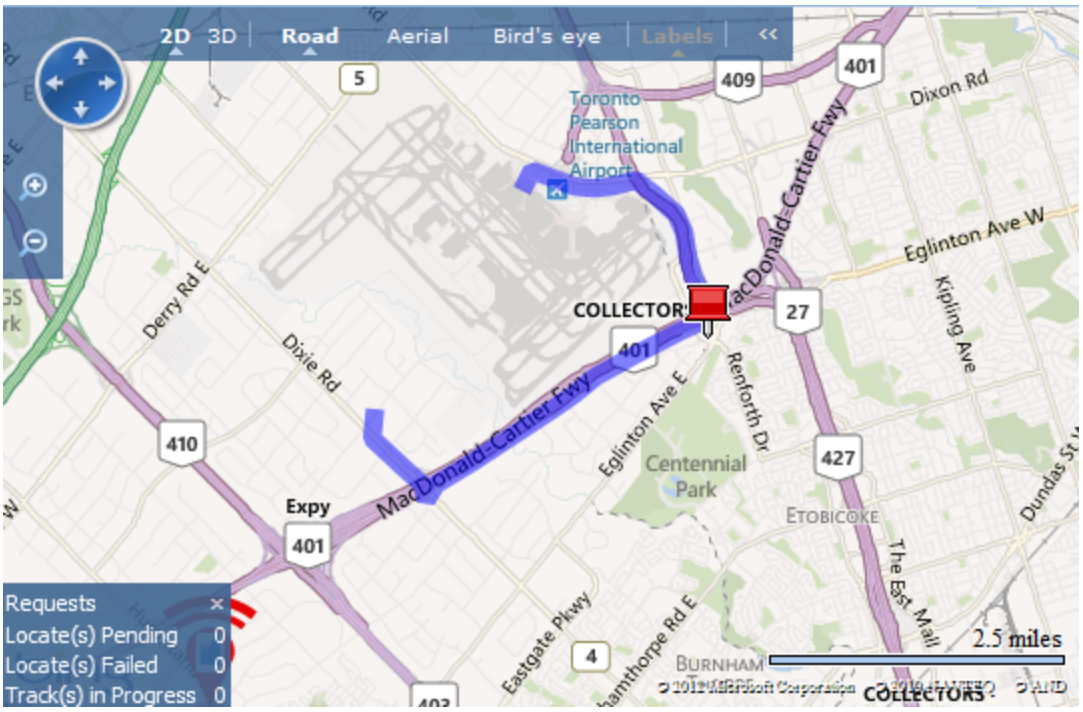
Get Directions dialog box

To use Get Directions, in the Location panel right click on any device or a point on the map and select "Get Directions" from the pop-up menu. The Get Directions dialog box will appear. Be default, the device or map location clicked on will be used as the starting point. To change this, click the double arrow button located to the left of the Start and Finish fields. You can enter GPS co-ordinates, landmarks, or an address. Directions can be optimised by selecting shortest travel time or shortest distance from the options list and press the OK button.



Driving Directions window

MobiControl will determine the turn-by-turn driving directions between the two locations you specified. The resulting directions will be displayed in the Driving Directions window. If you started by right clicking on a device, the "Send to Device" button will be enabled and you can send the instructions directly to the device. You can copy the directions from this window and paste them into an email or document or your choice.

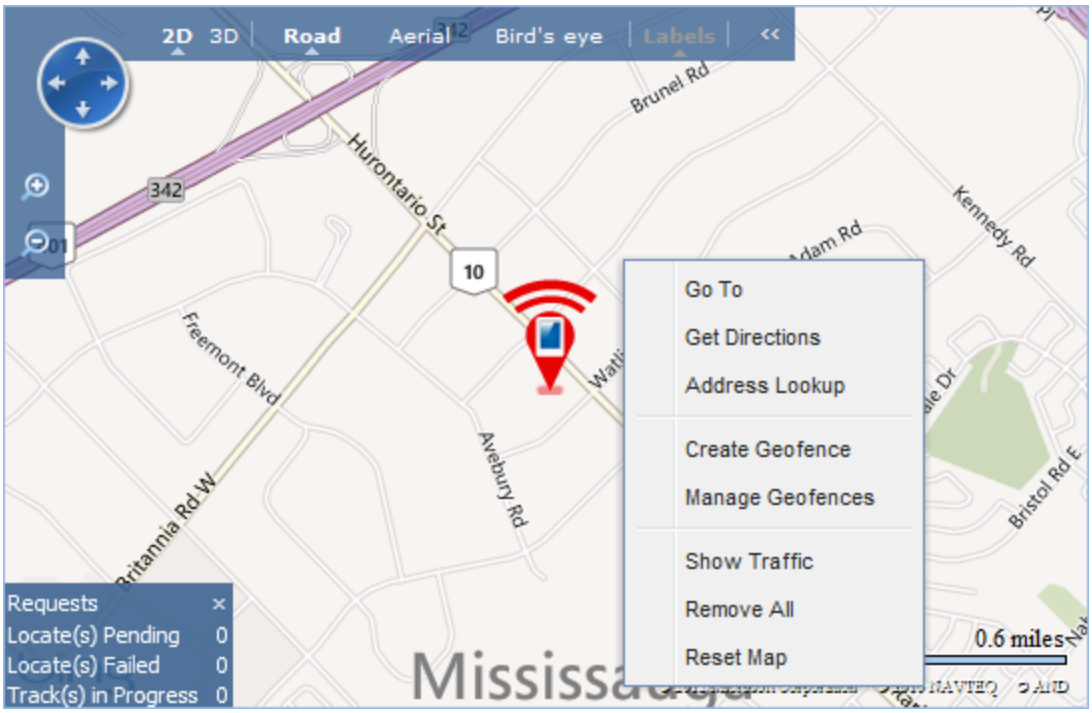


Driving directions displayed on the Map

The Location panel will reload the map to show the driving route highlighted. If the map is in Bird's Eye view, the highlight will not be displayed. Both Aerial and Road view will display the highlighted route.

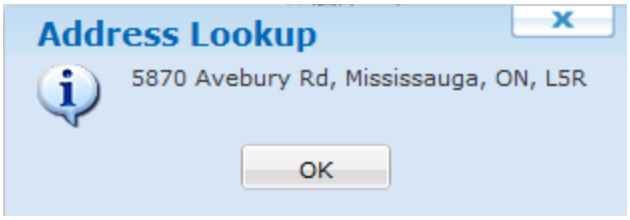
Android+ Address Lookup

The Address Lookup feature allows you to determine the address of a specific point on the map displayed on the Location panel. Address Lookup is based upon MobiControl's Location Services, as such, there may be a fee associated with its use. Please read the "Android+ Location Services" topic on page 1366 for more information.



Location panel right click menu with Address Lookup option

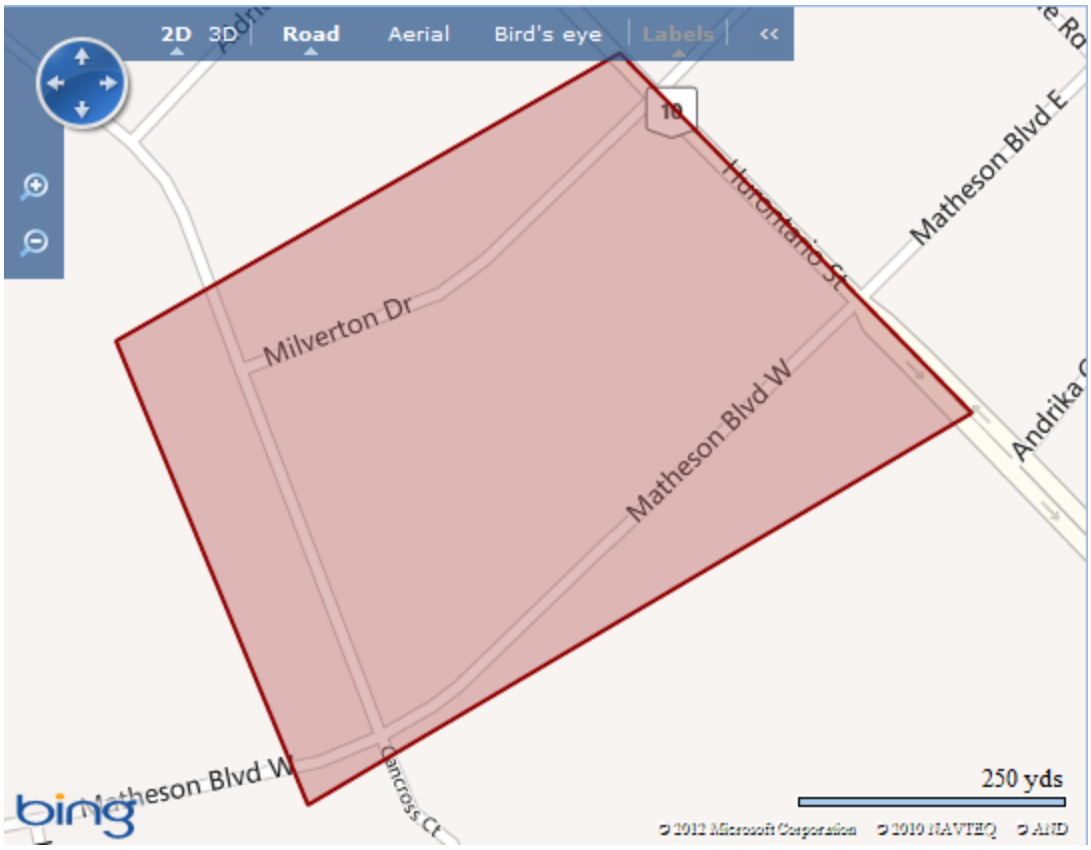
To use the Address Lookup feature, right click anywhere on the map in the Location panel and select the Address Lookup option from the menu that appears. The address of that location will be displayed in a new information window.



Address Lookup window

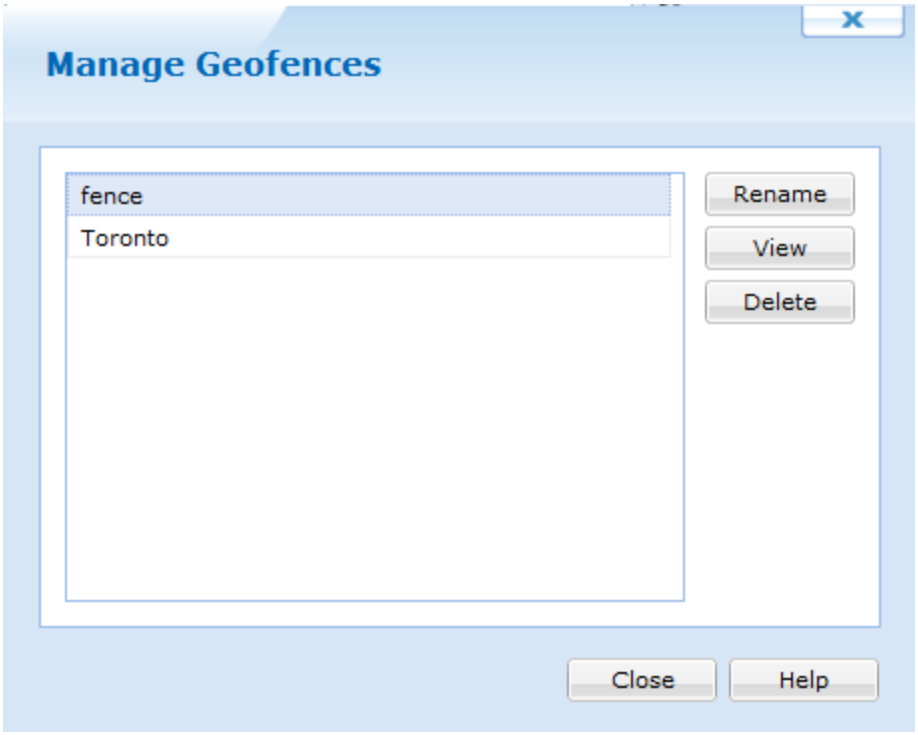
Using Manage Geofences

The Manage Geofences feature provides an area in which to rename, delete or view current created Geofences. You also have the option to create a new geofence from the drop down menu.



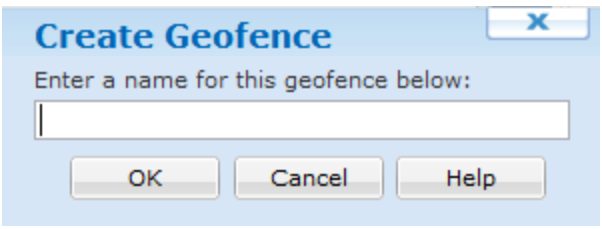
Location panel right click map and select Manage Geofence option

Selecting Manage Geofence brings up the following window.



Field Name	Description
Rename	Allows you to rename a Geofence
View	Allows you to view an already created Geofence on the map
Delete	Allows you to delete a Geofence **NOTE:** In order to Delete the Geofence, no Geofence Event can be associated with it

The **Create Geofence** option allows you to begin drawing on the map. The area drawn on the map will be defined as the Geofence. The defined area must be a complete geometric shape, which means the Start Drawing point will be the same as the End Drawing point. When you have completed a proper geometric shape you be asked to name your geofenced area.



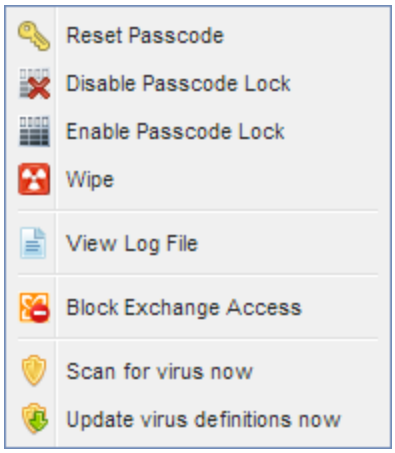
Android+ Actions

MobiControlallows you to reset passcodes, disable/enable passcode locks, wipe devices and block/unblock Exchange access on a group or an individual device level. These options can be viewed when you right click a device group/device and go to **Action**.

Device Level Actions

Selecting actions on a device level allows you to specifically send actions to that particular device. From here you can reset, disable or enable the passcode, restart and wipe the device, view log file and block or enable Exchange Access. To successfully use the Block/unblock Exchange Access action, you must have the Exchange ActiveSync filter installed on your Exchange Server. For more information on how to install this, please Skin/Formats/CrossReferencePrintFormat(See "Secure Email Access Install The Secure Email Access Filter allows you to achieve greater control with devices receiving email from your Exchange Service. When the filter is installed, you can block access to Exchange on certain devices as well as other controls. To successfully install the Exchange ActiveSync Filter, the MobiControl Root CA must be installed on the server that is publishing the Exchange ActiveSync Service. Below shows how to install the filter on your Exchange Server. Prerequisite StepsInstall MobiControl's Secure Email Access filter (Optional) 3rd party Exchange ActiveSync Filter Configuration Prerequisite StepsThe prerequisite steps show how to install the MobiControl Root CA on the Exchange Server. Go to the MobiControl Administration Utility and go to Certificates. The MobiControlAdministration Utility (MCAU)Click the Export button at beside the MobiControl Root Certificate label. Export the MobiControlRoot CertificateSave the exported certificate in a directory that is easy to remember. Next we need to go to the server with the Exchange ActiveSync Service.Open the Microsoft Management Console (MMC) by opening up the run command and typing mmc. Open the Microsoft Management Console. In MMC, click File then Add/Remove Snap In...Adding Snap-insSelect the Certificates snap-in and click Add >. Adding the Certificates Snap-inA new window will appear asking to select an account. Select the Computer account and click Next. Select the Computer Account. On the next screen select Local Computer and click Finish. Select ComputerAfter clicking Finish, click OK in the Add or remove Snap-ins window. Expand the Certificates (Local Computer) tree on the left side and go to Trusted Root Certification Authorities, then Certificates. Right click the Certificates folder and go to All Tasks then Import.Importing a new CA Follow the steps in the Certificate Import Wizard leaving all settings default. After the wizard has finished you will see the MobiControl Root CA in your Trusted Root Certification Authorities. The MobiControl Root CAInstall MobiControl's Secure Email Access filterMobiControl's Secure Email Access Filter must be installed on the server that is publishing the Exchange ActiveSync service. Typically this is the same computer that is hosting OWA (Outlook Web Access). From the server where the Secure Email Access filter will be installed, open Internet Explorer and browse to the MobiControl Web ConsoleLog in to the Web Console as an Administrator based account that has the "Configure Deployment Servers" permissionSelect the All Devices tab at the top of the MobiControl Web Console and then select the Servers tab located along the bottom of the Web ConsoleRight click on the Secure Email Access filter listed under the Deployment Server, and select Install Exchange ActiveSync FilterSave and then run the ExchangeActiveSyncFilter.exe program. This will place the needed files onto the server. Note: Depending on your Internet Explorer settings, you may be prompted to allow file downloads from the web pageOpen IIS manager and select the web site that is publishing Exchange ActiveSync Select ISAPI filters and select Add from the list of actionsEnter MobiControl Secure Email Access as the filter name For the Executable, If the Exchange ActiveSync site is running in a 32-bit application pool, select \Program Files\SOTI\XAS\mcxas.dll or, if the Exchange ActiveSync site is running in a 64-bit application pool, select \Program files\SOTI\XAS\mcxas64.dllSelect OK to save the filterIn the resulting list of filters, ensure that the MobiControl Secure Email Access filter is listed above the Microsoft Exchange ActiveSync filter. If this is not the case, select View Order List from the available actions, highlight MobiControl Secure Email Access and select Move Up to place it at the top Note: MobiControl's Secure Email Access required communication between the server that is publishing Exchange ActiveSync where the filter is installed, to the MobiControl Web Console. This communication happens over SSL on

port 443.3rd party Exchange ActiveSync Filter ConfigurationBefore you begin, the following components must be installed/enabled.1. IIS 7 with ASP.NET role service enabled.2. URL Rewrite Module installed (version 2.0 is required)3. Application Request Routing version 2.5 (Link)The URL Rewrite Module and Application Request Routing version 2.5 are both installed at the same time. After installation, please follow these steps:Open the IIS managerSelect the server in the tree view on the left hand side and then click on the Application Request Routing feature.Application Request RoutingOn the right menu, click Server Proxy Settings in the Proxy SectionServer Proxy SettingsCheck the Enable Proxy check box. Leave the default values for all the other settings on this page. Click Apply on the right side to commit the change.Enable ProxyNext step is to add the HTTP_ACCEPT_ENCODING server variable and Inbound and Outbound rules. To do this, please go to the left hand panel and select the Default Web Site and then select URL Rewrite. URL rewriteIn the URL Rewrite page, select View Server Variables on the right hand side. View Server VariablesClick the Add... link on the right side of the page to add the HTTP_ACCEPT_ENCODING variable. Click OK then Back to Rules. Adding a server variableClick the Add Rule(s)... link on the right side to add Inbound and Outbound rules. Add rule(s)...When creating the Inbound and Outbound rules, select Blank Rule under the respected heading and click OK.Adding a Blank Inbound or Outbound ruleOn the page shown below, the following fields need to have values entered (Please ensure that you enter your appropriate owa address):NameReverseProxyInboundRule1Pattern^(.*)Rewrite URLhttps://owa.myDomain.com/{R:1} Inbound Rule creation pageAfter the values have been entered, the server variable needs to be added. To do this, expand the Server Variables panel. Click Add and choose HTTP_ACCEPT_ENCODING from the drop down menu. Under value, enter 0, then click OK. Set Server VariableAfter entering all required values, click Apply.Apply Inbound RuleCreate a new blank rule to create an Outbound Rule. Please see below for what values to set on this page: Outbound rule pageUnder precondition, you will need to create a new condition. To do this, select <Create New Precondition...>. When the pop up window appears, click Add... to add a pattern:Add PreconditionAfter entering all required values, Click OK then click Apply.Apply Outbound RuleAfter the rules have been created, click the IIS server, and restart. To confirm that everything has been configured properly, go to C:\inetpub\wwwroot and open the web.config file in notepad. Your file should look similar to this: <?xml version="1.0" encoding="UTF-8"?> <configuration> <system.webServer> <rewrite> <rules> <rule name="ReverseProxyInboundRule1"> <match url="^(.*)" /> <serverVariables> <set name="HTTP_ACCEPT_ENCODING" value="0" /> </serverVariables> <action type="Rewrite" url="https://owa.soti.net/{R:1}" /> </rule> </rules> <outboundRules> <rule name="ReverseProxyOutboundRule1" preCondition="ResponseIsHtml1"> <match filterByTags="A, Form, Img" pattern="^http(s)?://owa.soti.net/(.*)" /> <action type="Rewrite" value="http{R:1}://owa.soti.net/{R:2}" /> </rule> <preConditions> <remove name="ResponseIsHtml1" /> <preCondition name="ResponseIsHtml1"> <add input="{RESPONSE_CONTENT_TYPE}" pattern="^text/html" /> </preCondition> </preConditions> </outboundRules> </rewrite> </system.webServer> </configuration>" on page 1)



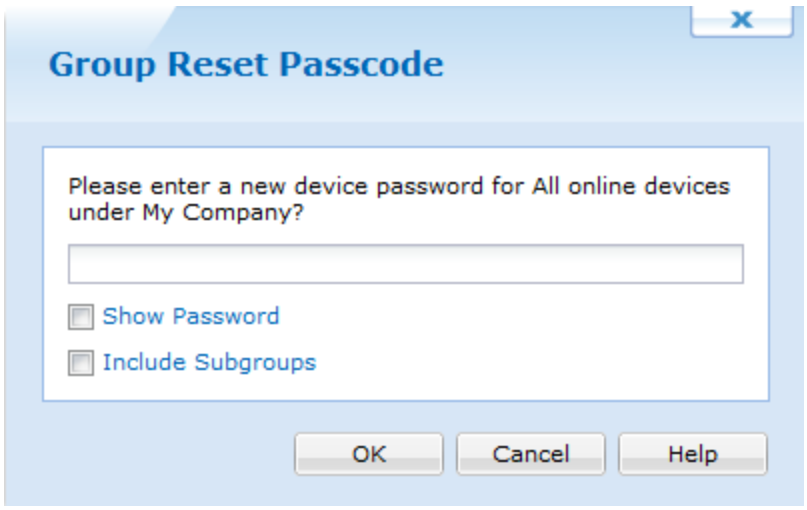
Android+ Device Action Selections

Group Level Actions

With group level actions, you are able to reset the passcode, disable/enable the passcode lock, wipe devices, and block/unblock Exchange access to every device under the group.

Reset Passcode

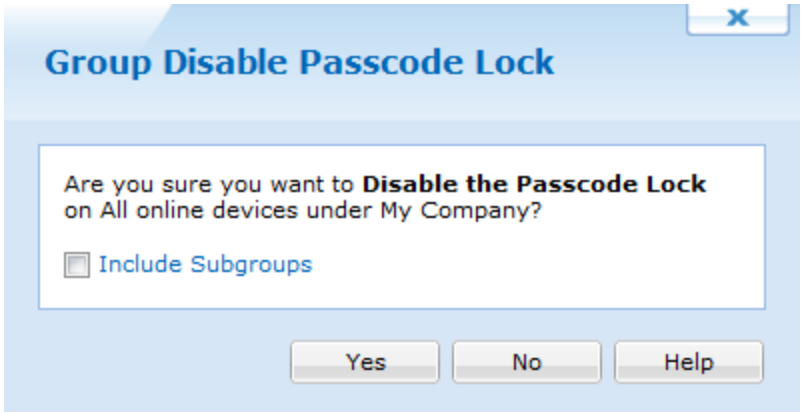
Reset Passcode allows you to reset the passcode for every device in the group. This can be useful when you move multiple devices into a specific group for resetting passcodes.



Group Reset Passcode

Disable/Enable Passcode Lock

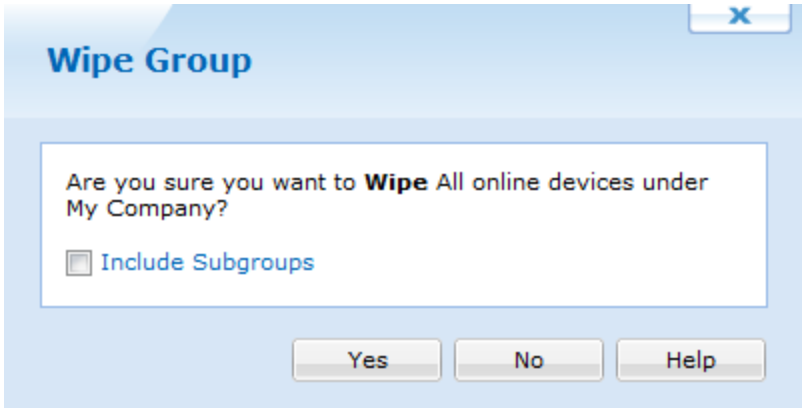
Using the Disable Passcode Lock turns off the pin code on the lock screen in iOS devices. This can be useful when you move multiple devices into a specific group for resetting passcodes. Selecting Enable Passcode Lock enabled the pin code on the lock screen.



Disabling Passcode Lock

Wipe Device

Using the Wipe Device action allows you to delete all information and apps from the devices in the selected group. This can be used when you have devices that pass between multiple users and you do not want users to see previous users accounts or information.



Wipe Group

Block/Unblock Exchange Access

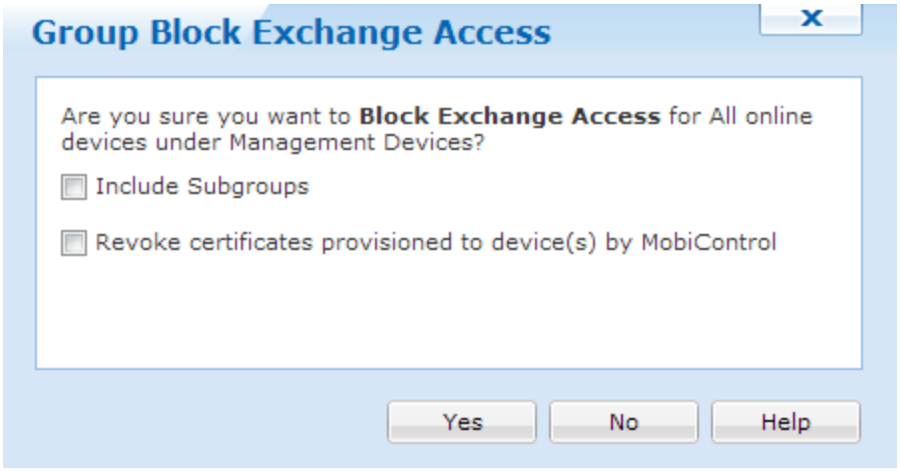
Using these options allow you to block and unblock Exchange access to every device in the group. To successfully use this action, you must have the Exchange ActiveSync filter installed on your Exchange Server. For more information on how to install this, please Skin/Formats/CrossReferencePrintFormat (See "Secure Email Access Install The Secure Email Access Filter allows you to achieve greater control with devices receiving email from your Exchange Service. When the filter is installed, you can block access to Exchange on certain devices as well as other controls. To successfully install the Exchange ActiveSync Filter, the MobiControl Root CA must be installed on the server that is publishing the Exchange ActiveSync Service. Below shows how to install the filter on your Exchange Server. Prerequisite StepsInstall MobiControl's Secure Email Access filter(Optional) 3rd party Exchange ActiveSync Filter Configuration Prerequisite StepsThe prerequisite steps show how to install the MobiControl Root CA on the Exchange Server. Go to the MobiControl Administration Utility and go to Certificates. The MobiControlAdministration Utility (MCAU)Click the Export button at beside the MobiControl Root Certificate label. Export the MobiControlRoot CertificateSave the exported certificate in a directory that is easy to remember. Next we need to go to the server with the Exchange ActiveSync Service.Open the Microsoft Management Console (MMC) by opening up the run command and typing mmc. Open the Microsoft Management Console. In MMC, click File then Add/Remove Snap In...Adding Snap-insSelect

the Certificates snap-in and click Add >. Adding the Certificates Snap-inA new window will appear asking to select an account. Select the Computer account and click Next. Select the Computer Account. On the next screen select Local Computer and click Finish. Select ComputerAfter clicking Finish, click OK in the Add or remove Snap-ins window. Expand the Certificates (Local Computer) tree on the left side and go to Trusted Root Certification Authorities, then Certificates. Right click the Certificates folder and go to All Tasks then Import.Importing a new CA Follow the steps in the Certificate Import Wizard leaving all settings default. After the wizard has finished you will see the MobiControl Root CA in your Trusted Root Certification Authorities. The MobiControl Root CAInstall MobiControl's Secure Email Access filterMobiControl's Secure Email Access Filter must be installed on the server that is publishing the Exchange ActiveSync service. Typically this is the same computer that is hosting OWA (Outlook Web Access). From the server where the Secure Email Access filter will be installed, open Internet Explorer and browse to the MobiControl Web ConsoleLog in to the Web Console as an Administrator based account that has the "Configure Deployment Servers" permissionSelect the All Devices tab at the top of the MobiControl Web Console and then select the Servers tab located along the bottom of the Web ConsoleRight click on the Secure Email Access filter listed under the Deployment Server, and select Install Exchange ActiveSync FilterSave and then run the ExchangeActiveSyncFilter.exe program. This will place the needed files onto the server. Note: Depending on your Internet Explorer settings, you may be prompted to allow file downloads from the web pageOpen IIS manager and select the web site that is publishing Exchange ActiveSync Select ISAPI filters and select Add from the list of actionsEnter MobiControl Secure Email Access as the filter name For the Executable, If the Exchange ActiveSync site is running in a 32-bit application pool, select \Program Files\SOTI\XAS\mcxas.dll or, if the Exchange ActiveSync site is running in a 64-bit application pool, select \Program files\SOTI\XAS\mcxas64.dllSelect OK to save the filterIn the resulting list of filters, ensure that the MobiControl Secure Email Access filter is listed above the Microsoft Exchange ActiveSync filter. If this is not the case, select View Order List from the available actions, highlight MobiControl Secure Email Access and select Move Up to place it at the top Note: MobiControl's Secure Email Access required communication between the server that is publishing Exchange ActiveSync where the filter is installed, to the MobiControl Web Console. This communication happens over SSL on port 443.3rd party Exchange ActiveSync Filter ConfigurationBefore you begin, the following components must be installed/enabled.1. IIS 7 with ASP.NET role service enabled.2. URL Rewrite Module installed (version 2.0 is required)3. Application Request Routing version 2.5 (Link)The URL Rewrite Module and Application Request Routing version 2.5 are both installed at the same time. After installation, please follow these steps:Open the IIS managerSelect the server in the tree view on the left hand side and then click on the Application Request Routing feature.Application Request RoutingOn the right menu, click Server Proxy Settings in the Proxy SectionServer Proxy SettingsCheck the Enable Proxy check box. Leave the default values for all the other settings on this page. Click Apply on the right side to commit the change.Enable ProxyNext step is to add the HTTP_ACCEPT_ENCODING server variable and Inbound and Outbound rules. To do this, please go to the left hand panel and select the Default Web Site and then select URL Rewrite. URL rewriteIn the URL Rewrite page, select View Server Variables on the right hand side. View Server VariablesClick the Add... link on the right side of the page to add the HTTP_ACCEPT_ENCODING variable. Click OK then Back to Rules. Adding a server variableClick the Add Rule(s)... link on the right side to add Inbound and Outbound rules. Add rule(s)...When creating the Inbound and Outbound rules, select Blank Rule under the respected heading and click OK.Adding a Blank Inbound or Outbound ruleOn the page shown below, the following fields need to have values entered (Please ensure that you enter your appropriate owa address):NameReverseProxyInboundRule1Pattern^(.*)Rewrite URLhttps://owa.myDomain.com/{R:1} Inbound Rule creation pageAfter the values have been entered, the server variable needs to be added. To do this, expand the Server Variables panel. Click Add and choose HTTP_ACCEPT_ENCODING from the drop down menu. Under value, enter 0, then click OK. Set Server VariableAfter entering all required values, click Apply.Apply Inbound RuleCreate a new blank rule to create an Outbound Rule. Please see below for what values to set on this page: Outbound rule pageUnder precondition, you will need to create a new condition. To do this, select <Create New Precondition...>. When the pop up window appears, click Add... to add a pattern:Add PreconditionAfter entering all required values, Click OK then click Apply.Apply Outbound RuleAfter the rules have been created, click the IIS server, and restart. To confirm that everything has been configured properly, go to C:\inetpub\wwwroot and open the web.config file in notepad. Your file should look similar to this: <?xml

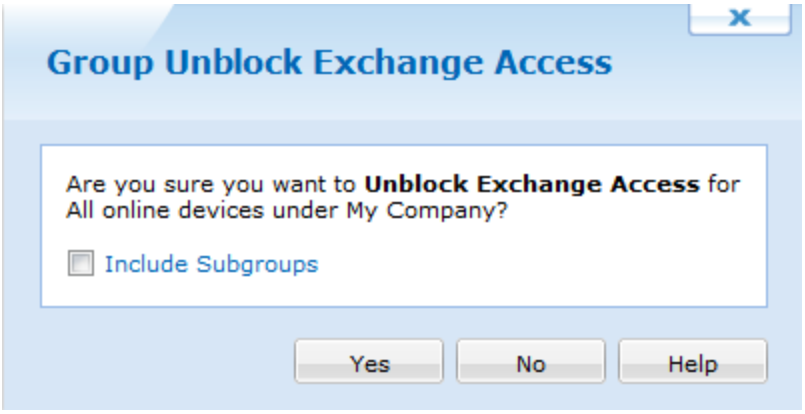
version="1.0" encoding="UTF-8"?> <configuration> <system.webServer> <rewrite> <rules> <rule name="ReverseProxyInboundRule1"> <match url="^(.*)" /> <serverVariables> <set name="HTTP_ ACCEPT_ENCODING" value="0" /> </serverVariables> <action type="Rewrite" url="https://owa.soti.net/ {R:1}" /> </rule> </rules> <outboundRules> <rule name="ReverseProxyOutboundRule1" preCondition="ResponseIsHtml1"> <match filterByTags="A, Form, Img" pattern="^http (s)?://owa.soti.net/(.*)" /> <action type="Rewrite" value="http{R:1}://owa.soti.net/{R:2}" /> </rule> <preConditions> <remove name="ResponseIsHtml1" /> <preCondition name="ResponseIsHtml1"> <add input="{RESPONSE_CONTENT_TYPE}" pattern="^text/html" /> </preCondition> </preConditions> </outboundRules> </rewrite> </system.webServer> </configuration>" on page 1) If the filter is not installed, a confirm message will appear.

If any certificates were provisioned by MobiControl to devices, we can revoke them when we block Exchange access.

No Filter installed



Blocking Exchange Access



Unblocking Exchange Access

Scan for virus now

When this is selected, MobiControl will scan the device for any virus's, rather than waiting for a schedule to scan.

Update virus definitions now

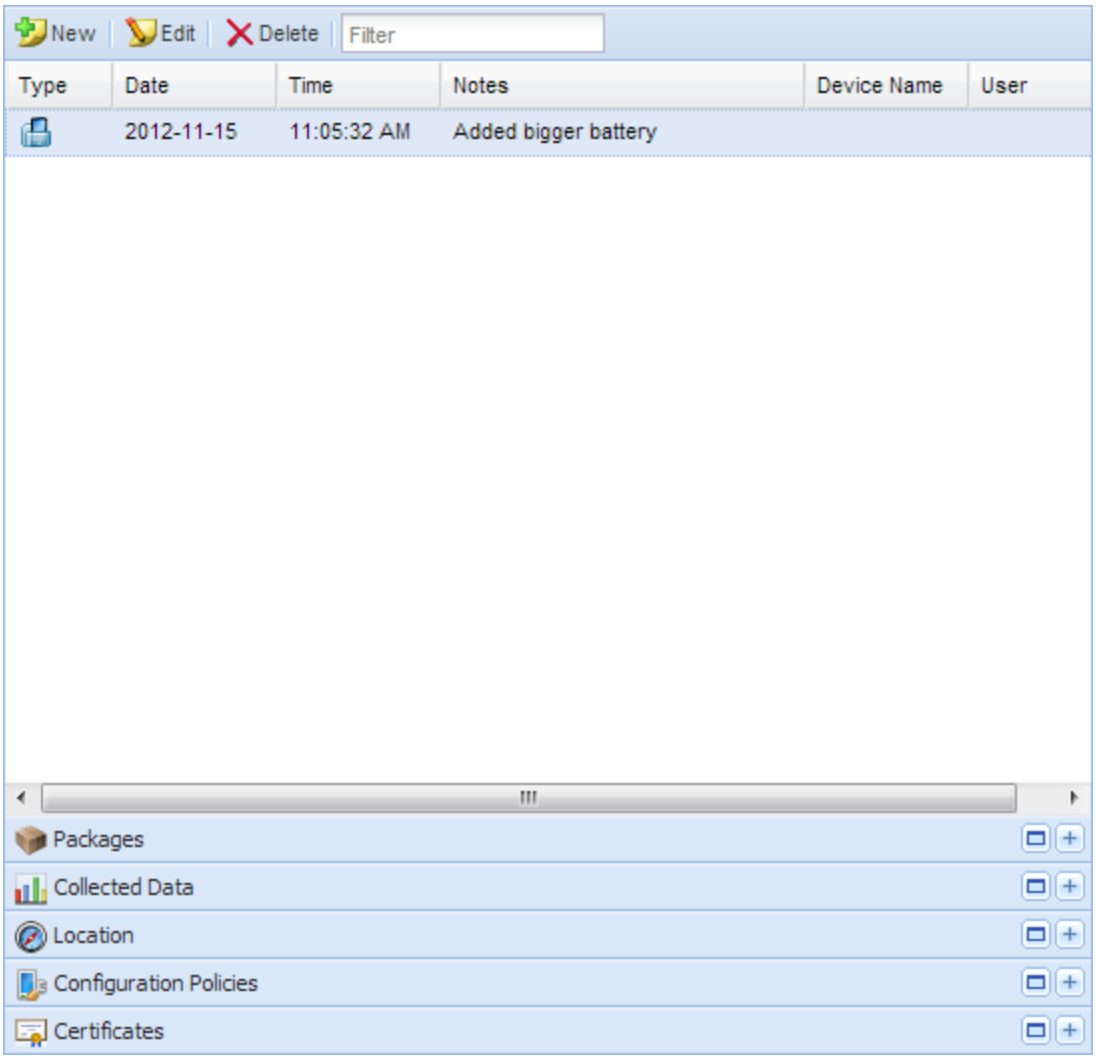
When selected, this will update the virus definition on devices.

Device Notes

The Device Notes feature allows you to create a note for a device and archive it for future reference and tracking purposes. Each note is editable and includes the date and time when the note was added or edited. The note includes the name of the user creating the note and can be assigned different colors for color-coded categorization.

This feature is useful for creating a "trouble ticket" for help desk tracking in an end-user support or CRM (Customer Relationship Management) environment. It also allows users with access to the MobiControl Web Console to document a device-specific issue and share their comments and memos related to that device with other users of the MobiControl Web console.

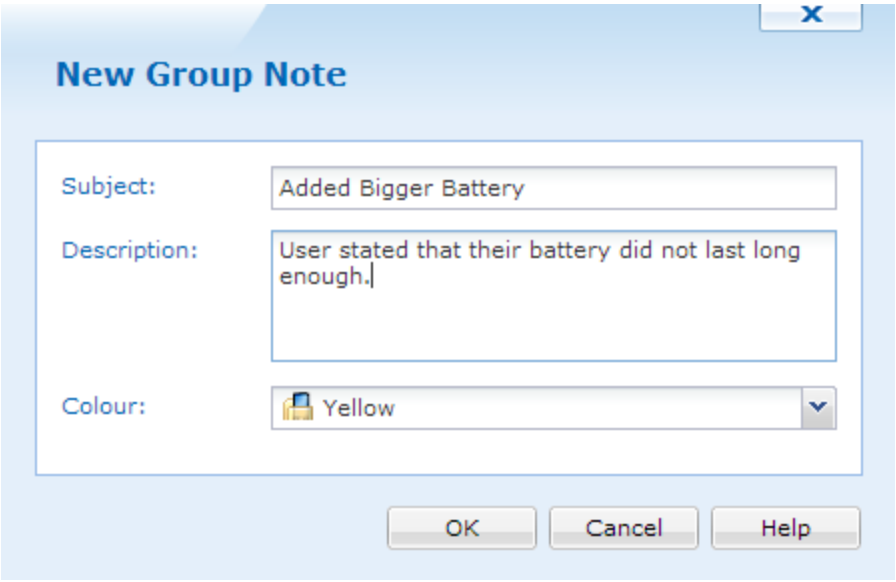
To view and edit notes for a device, select the Devices view (tab) in any of the All Devices, Windows Mobile, Windows Desktop, iOS, Android or Android Plus tab. Select a device and the notes for that device appear in the Notes panel.



Device Notes

Adding or Editing a Note

From within the Notes panel, click **New** to add a new note for the currently selected device or click **Edit** to make changes to an existing note.



Add Note dialog box

The following table describes the fields of the **Add Note** dialog box:

Field Name	Description
Subject	Text entered in the subject field appears in the Notes panel as the title of the note.
Icon	You can choose different colors for the icon to adopt a color-coding to indicate different priority levels or to distinguish between different departments or users creating the note. Notes can be sorted by icon color for a categorized view.
Description	The description field is available for viewing when the note is opened. This field can contain troubleshooting notes, administrative memos or any other device-specific information.

Device Group Notes

MobiControl now offers a way to place notes on a device group level. For example, if you are planning a roll out of devices across the country in phases based on location, you can add device group notes to state which phase each group is in. Therefore, when someone else logs into the MobiControl Web Console, they can see what part of the roll out each group should be in.

To create a device group level note, click a group on the left side of the MobiControl Web Console. After a group has been selected, expand the Notes panel on the right side, and click New.

Android+ Rules Tab

Android Plus Rules Tab

MobiControl uses rules to simplify the tasks of device management and configuration. See Below for a description of each rule.

Add Devices

1. Create an add devices rule.

   An add devices rule allows you to configure the settings that MobiControl uses to set up and communicate with your devices. These settings include: the device group to which devices are added, how often the device is to check for updates, and the parameters to be used for remote control sessions. Please see the "Adding Android+ Devices" topic on page 1389 for detailed information about creating an add devices rule.

2. Create a Device Agent.

   The Device Agent is the MobiControl software that resides on mobile devices and communicates with MobiControl Deployment Servers. Device Agents execute instructions received from MobiControl Deployment Servers, report status information, and send real-time information to Deployment Servers. Device Agents also restore the device state after a hard reset, service remote control sessions, install or uninstall packages, and synchronize the device clock. Please see the "Android+ Agent Install Methods" topic on page 1282 for detailed information about creating a Device Agent.

3. Install the Device Agent onto the devices.

   Once created, there are several options for installing the agent on to your devices. For example, installation can be accomplished via cradled ActiveSync, via a website download, via an SD card, or using an existing software distribution mechanism. Please see the "Adding Android+ Devices" topic on page 1389 for detailed information about installing the Device Agent.

Package Deployment

1. Create a package.

   A package is a set of software and data files that have been packed into a single compressed file. MobiControl provides a tool called MobiControl Package Studio that allows you to quickly and easily create packages. For complex packages, Package Studio allows users to add scripts that get automatically executed at various points in the installation or un-installation of the package. Please see the "Creating Packages" topic on page 414 for detailed information about creating packages using MobiControl.

2. Create a deployment rule.

   To deploy a package using MobiControl, you need to create a deployment rule. When you create a deployment rule, you need to specify the package(s) to be deployed, the devices to which the package(s) will be deployed, and the installation time. Please see the "Android+ Package Deployment" topic on page 1397 for detailed information about creating a deployment rule.

3. Check the rule execution status.

   Once you have created a deployment rule, you may want to confirm that all devices have been provisioned with the specified packages. The execution status of the deployment rule is graphically represented in the execution chart in the Rules view (tab). MobiControl also provides a report called the 'Deployment Rule Execution Summary Report'. Please see the "Android+ Reports" topic on page 1453 for detailed information about MobiControl Reports.

Application Catalog

1. Create an Application Catalog Rule

   An Application Catalogue Rule allows Administrators to distribute proprietary, in-house applications to employees or members of the organization. Please see the "Android+ Application Catalog" topic on page 1403 for detailed information about creating an Alert Rule.

2. Check the Application Catalog Rule Report.

   Once the Application Catalog Rule has been created, you may want to run a report to see what alerts have been generated. You can do this by looking at the Application Catalog Rule Report in the Reports view (tab). Please see the "Android+ Reports" topic on page 1453 for more detail about reports.

File Sync

1. Create a file sync rule.

   A file sync rule allows you to schedule file(s) to be synchronized between a set of devices and the Deployment Server. When creating a file sync rule, you will need to specify the file(s) you want synced (both their original location and their destination), the interval in between the syncs and which direction the sync should go in (either device to server, or server to device) and which devices should be involved in the sync. Please see the "Android+ Creating File Sync Rules" topic on page 1408 for detailed information about creating a file sync rule.

2. Check the rule execution status.

   Once the file sync rule has been created, you may want to confirm that the scheduled syncs occurred. You can do this by looking at the rule execution status or by checking the rule execution report in the Reports view (tab). Please see the "Android+ Reports" topic on page 1453 for more detail about reports.

Device Relocation

1. Create a device relocation rule.

   A device relocation rule allows you to automatically move your mobile devices among different device groups in the MobiControl device tree, based on the IP address or other custom criteria. This is useful for managing mobile devices in a deployment where the device tree represents different physical locations (e.g. retail stores, warehouses, regional offices, etc). Please see the "Android+ Device Relocation Rule" topic on page 1421 for detailed information about creating a device relocation rule.

Data Collection

1. Create a data collection rule.

   A data collection rule allows you to set up rules to collect data from your mobile devices automatically. Please see the "Android+ Data Collection Rules" topic on page 1425 for detailed information about creating a data collection rule.

2. Check the data collection rule execution status.

   Once the data collection rule has been created, you may want to confirm its execution. You can do this by looking at the rule execution status or by checking the rule execution report in the Reports view (tab). Please see the "Android+ Reports" topic on page 1453 for more detail about reports.

Alert

1. Create an Alert Rule

   An Alert Rule allows Administrators and Users to be notified when events of interest arise on the system. Please see the "Android+ Alert Rules" topic on page 1434 for detailed information about creating an Alert Rule.

2. Check the Alert Rule execution status.

   Once the Alert Rule has been created, you may want to run a report to see what alerts have been generated. You can do this by looking at the Alert Rule Summary report in the Reports view (tab). Please see the "Android+ Reports" topic on page 1453 for more detail about reports.

Telecom Expense

1. Create an Telecom Expense Rule

   A Telecom Expense Rule allows Administrators and Users to be notified on current usage of company data and voice minutes. Please see the "Android+ Telecom Expense Management" topic on page 1443 for more information.

2. Check the Telecom Expense Rule execution status.

   Once the Alert Rule has been created, you may want to run a report to see what alerts have been generated. You can do this by looking at the Telecom Expense Rule Summary report in the Reports view (tab). Please see the "Generate Reports" topic on page 623 for more details about reports.

Adding Android+ Devices

To Add Google Android Devices you need to create an 'Add Devices Rule' and then download the installation files to the mobile device. Alternately, you may Publish your **Add Devices Rule** to the Enrollment Service and provide the Enrollment ID to the mobile user.

Add devices rules allow MobiControl to name devices, place devices in the appropriate device group, and to generate a customized Enrollment ID that, when enrolled by the user, allows MobiControl to manage the devices.

To create an add devices rule, select the Google Android Tab within MobiControl Web Console, then select the **Rules** Tab. Right-Click the **Add Devices Rules** folder and select **Create Add Devices Rules**.

Android+ Tab

The seven steps below describe how the Create Add Devices Rule Wizard can be used to create an add devices rule:

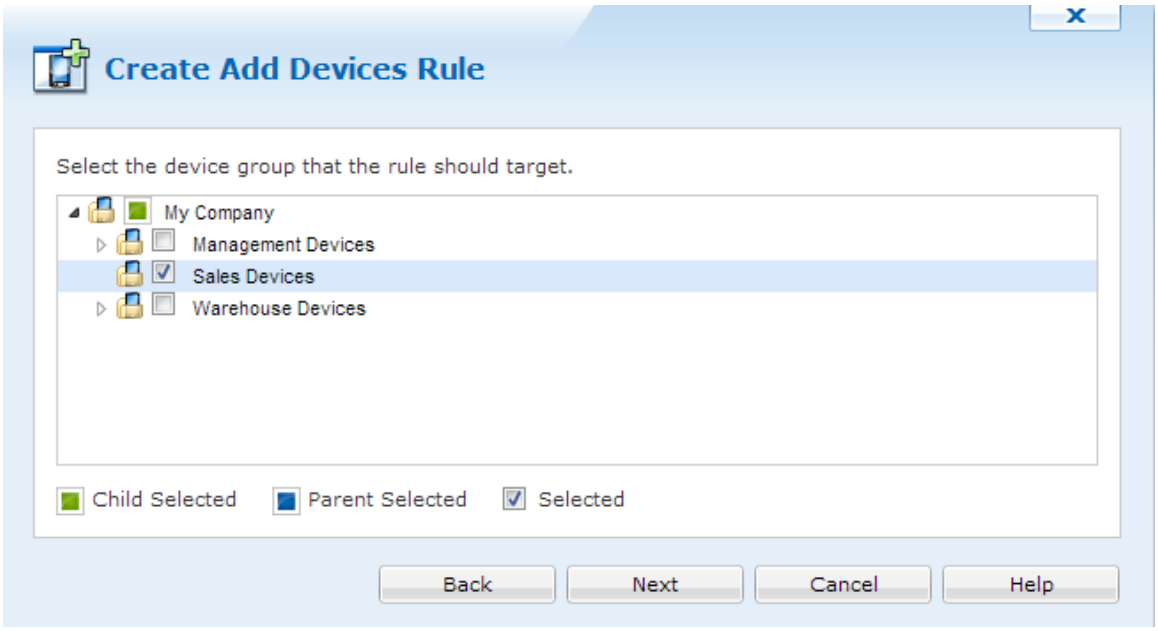
1. Start the wizard.

   Select the **Rules** Tab, from the **Google Android** Tab, then Right-Click the **Add Devices Rules** folder and select **Create Add Devices Rules**. The first page of the Create Add Devices Rule Wizard will be displayed.

   Enter a descriptive name for the add devices rule you are creating and click **Next.**

First page of the Create Add Devices Rule Wizard

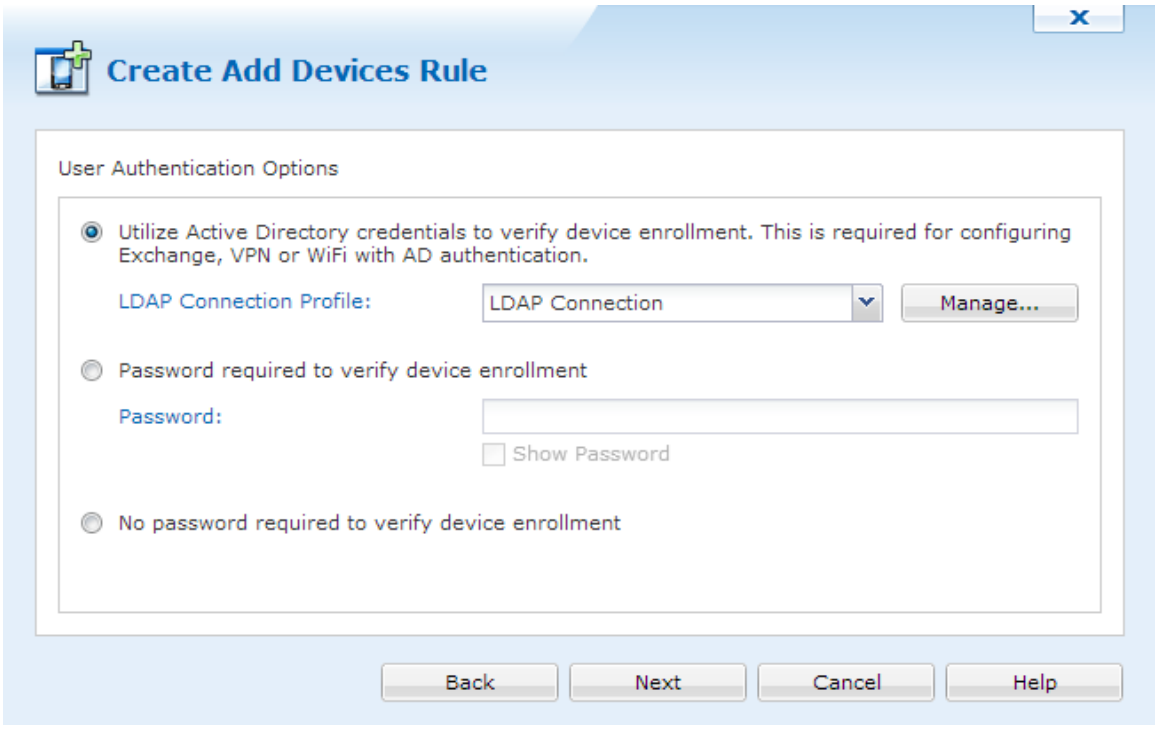
2. Configure the device group.



Device Group Selection page

First, select to which device group the devices configured by this rule will be added. The dialog box below displays the current device tree. Select the group where devices need to be inserted and then click **Next.** After selecting a device group click on the **Next** button.

3. Configure authentication options.



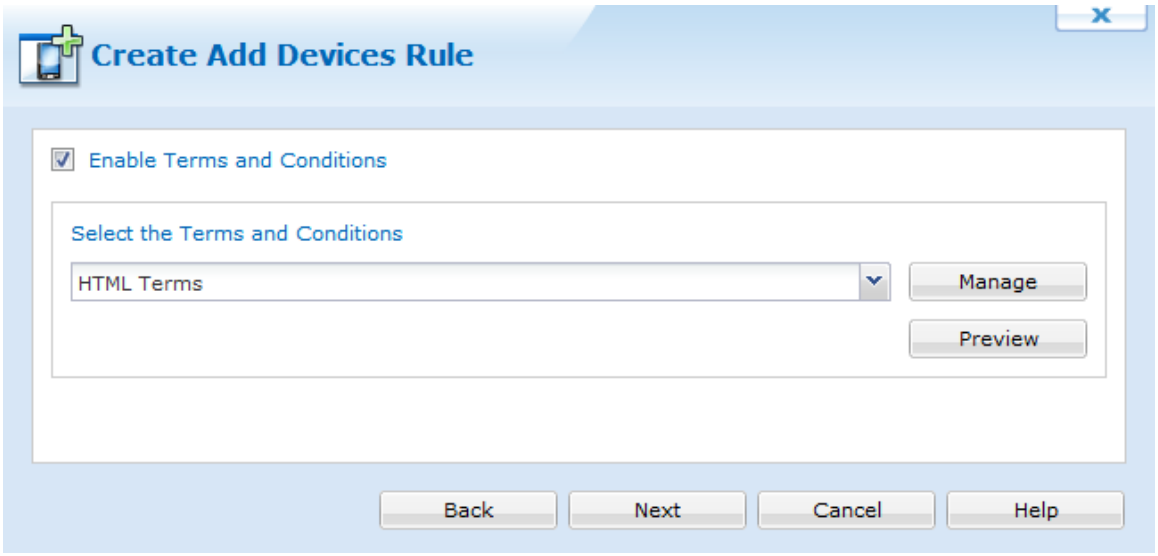
User Enrollment Authentication

Select a user authentication method for enrolling devices. A password may be set to ensure unwanted devices are unable to enroll in your network.

If Utilize Active Directory credentials is selected, choose the connection type from the drop down menu. If there is no connections, click Manage to create a new connection. Please see the "LDAP Connections Manager" topic on page 616 for more information regarding LDAP connections.

4. Terms and Conditions

The terms and conditions page allows us to send terms and conditions to devices. Users must accept these terms before they are able to enroll their device to MobiControl. If they do not accept the terms and conditions, the device will not connect. If Terms and Conditions is required, click "Enable Terms and Conditions".



Terms and conditions

To add new Terms and Conditions to the Add Devices rule, click Manage. Once clicked, we can see the Terms and Condition Manager. Please see the "Terms and Conditions" topic on page 619 for more information.

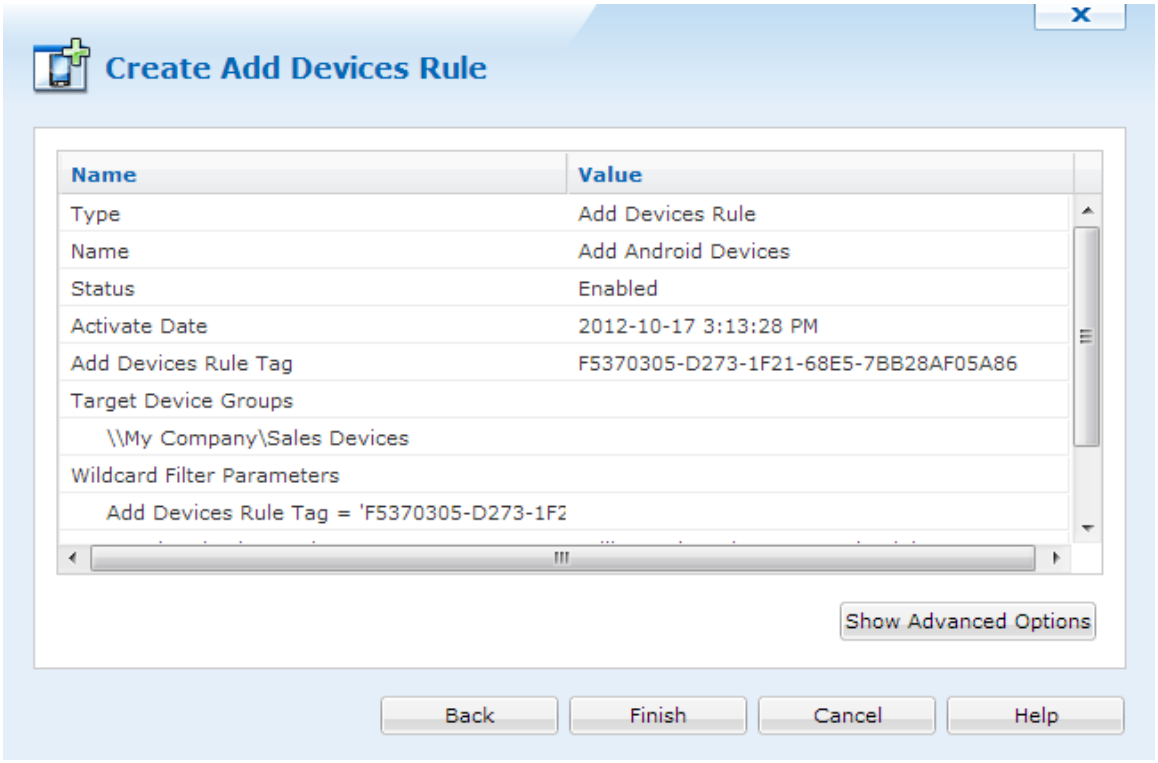
After selecting the Terms and Conditions, click **Next** to continue the creation of the rule.

5. Review summarized information.

The **Rule Summary Information** page summarizes the settings configured on the previous pages of the wizard.

If you are satisfied with the configured settings, click on the **Finish** button to create the device rule, otherwise use the **Back** button to go to previous screens and make adjustments.

Selecting the "Publish To Enrollment Service" option allows all of your Add devices rule options to be saved in the cloud and accessed by devices via an Enrollment ID. The Enrollment ID contains the information used for the Device Agent to get back to your company's Deployment Server. The Enrollment ID is entered in the Device Agent. The Device Agent is available from Google Play by searching for MobiControl

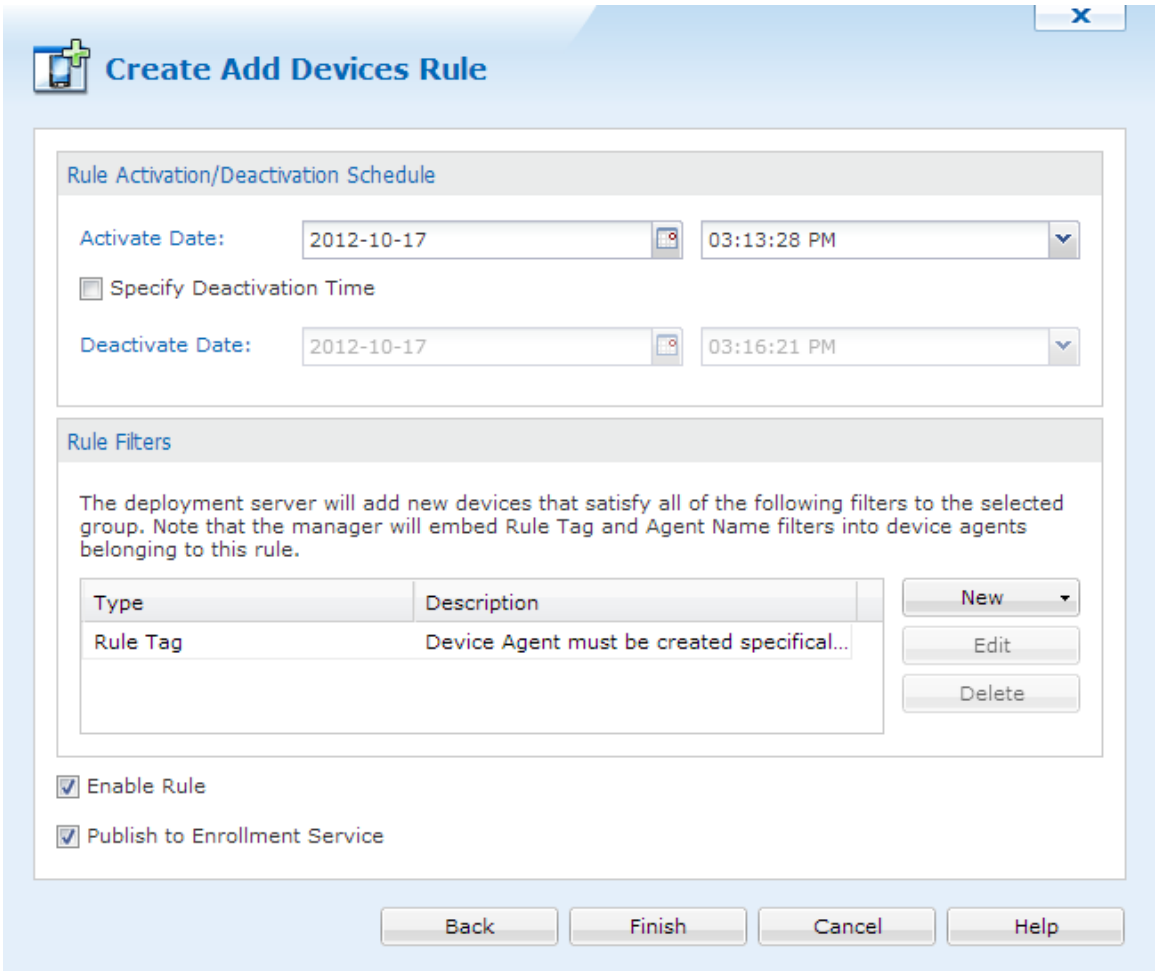


Rule Summary Page

6. Advanced Settings.

The **Advanced Settings** button allows you to specify which devices are to be configured by this rule. By default, MobiControl will use this rule to configure only those devices that are running a Device Agent created specifically for this device rule. By using advanced settings filters, you can broaden or further restrict which devices get configured by this rule when they connect to MobiControl.

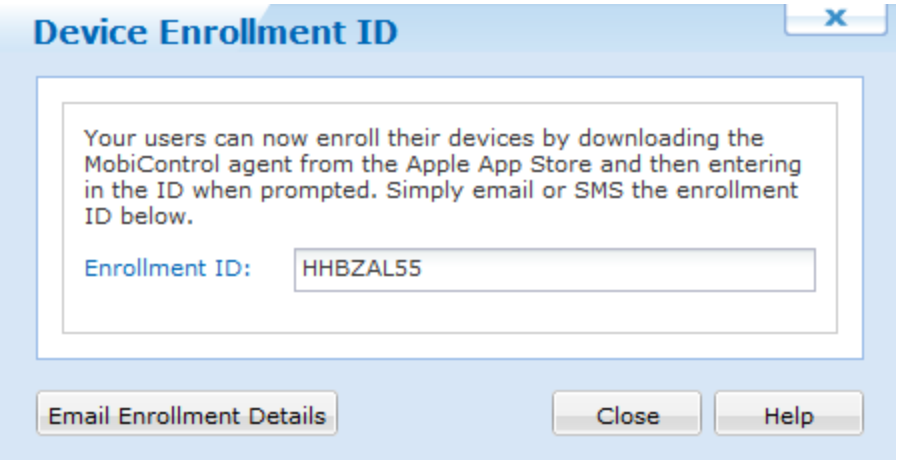
Once you have made the changes, click **Next.**



Advanced Settings Page

7. Enrollment ID

If you download the MobiControl Device Agent from Google Play, then you should enter the ID that is shown in the Device Enrollment ID window. This allows the Device Agent to configure what server your device should connect to.

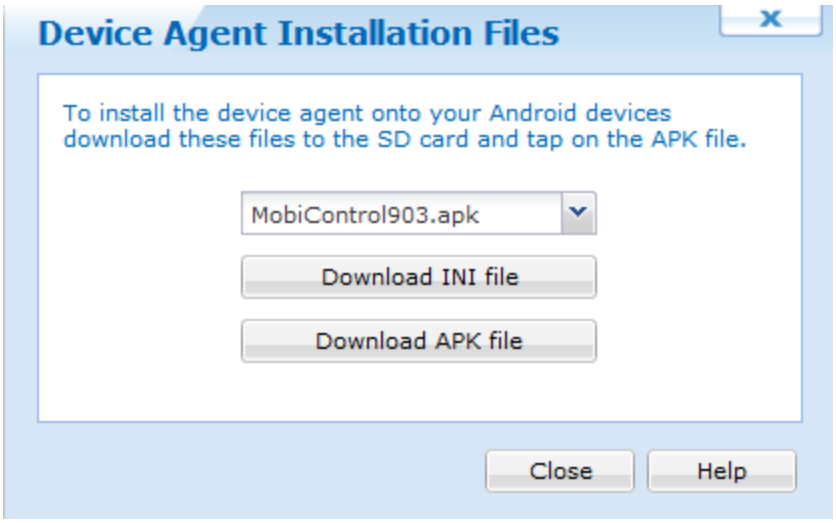


Device Enrollment ID

7. Download the MobiControl Android files

   You can download and place the Google Android Installation Files onto the Root of the SD Card and install the APK from there. You are able to download the Generic MobiControl agent or the Android+ Agent by selecting the APK file from the drop down shown below.

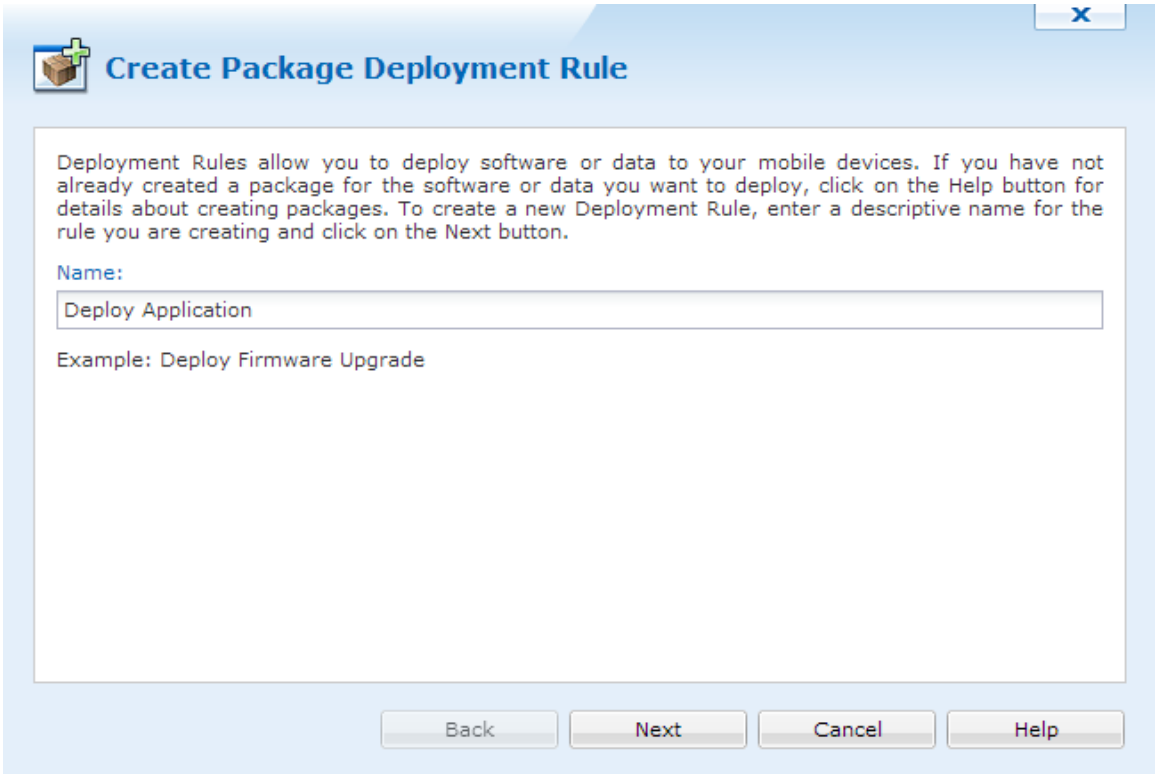
   If the INI file and the APK file are both downloaded and placed on the SD card, no enrolment ID needs to be entered after installing the MobiControlDevice Agent. For more information about the device agent please see the "Android+ Agent Install Methods" topic on page 1282



Device Agent Installation Files page

Deployment rules allow administrators to automatically provision mobile devices with packages that contain software or data. The following series of steps describes how to use the Create Deployment Rule Wizard to create a deployment rule.

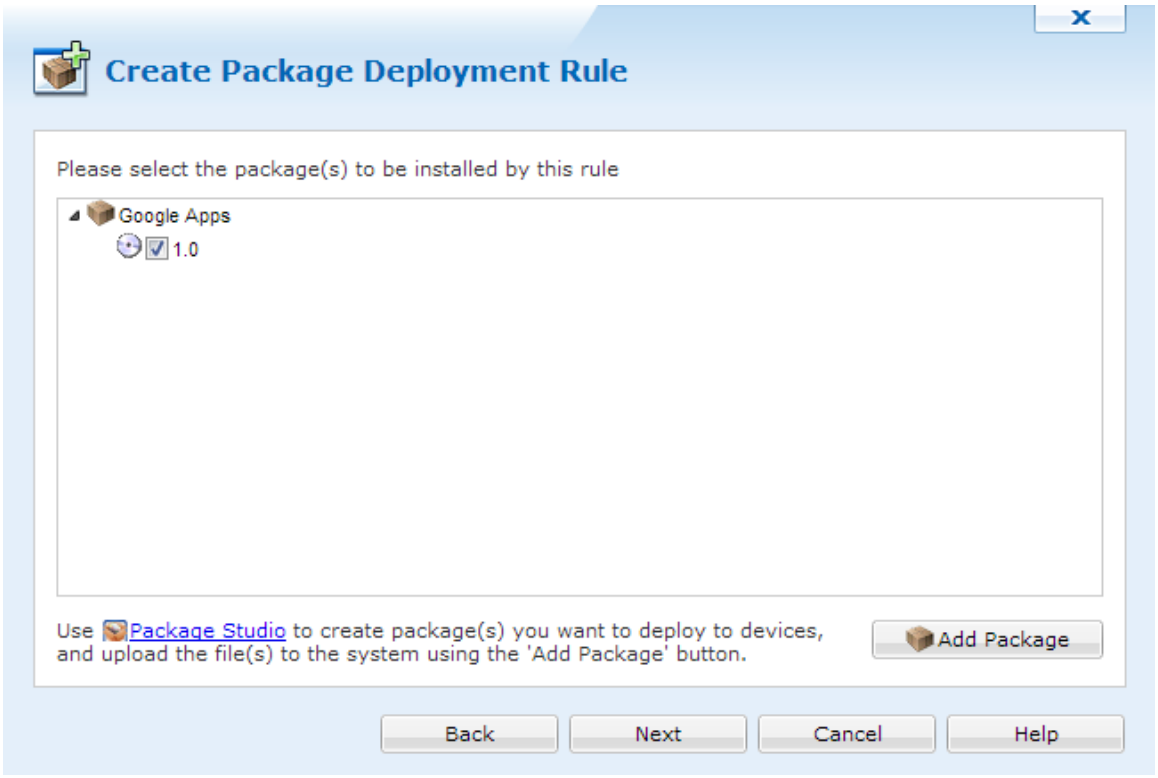
1. Start the wizard.



First page of the Create Deployment Rule Wizard

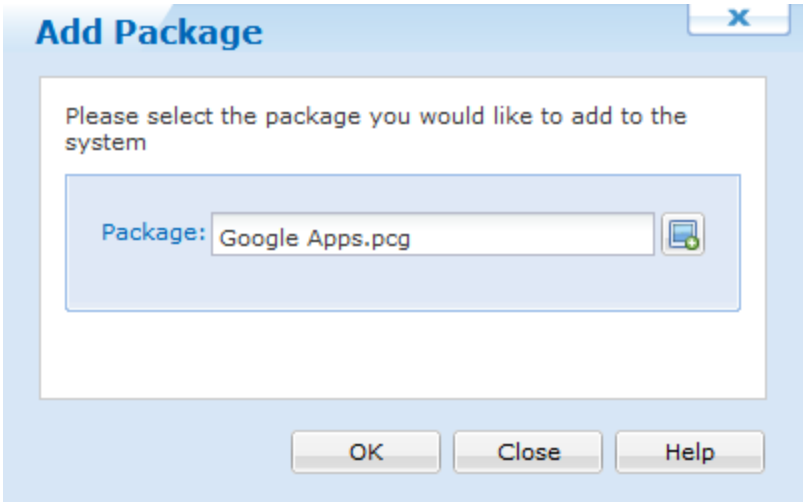
From MobiControl Manager select the **Rules view (tab)**, then click the **Rule** menu, click **Create Rule**, and click **Deployment Rule**. The first page of the Create Deployment Rule Wizard will be displayed. Enter a descriptive name for the deployment rule you are creating and click **Next**.

2. Select the package(s) to be deployed.



Select Package page

The dialog box displays a list of the packages that have been previously loaded into the MobiControl database. Select the relevant packages that need to be installed by this rule.



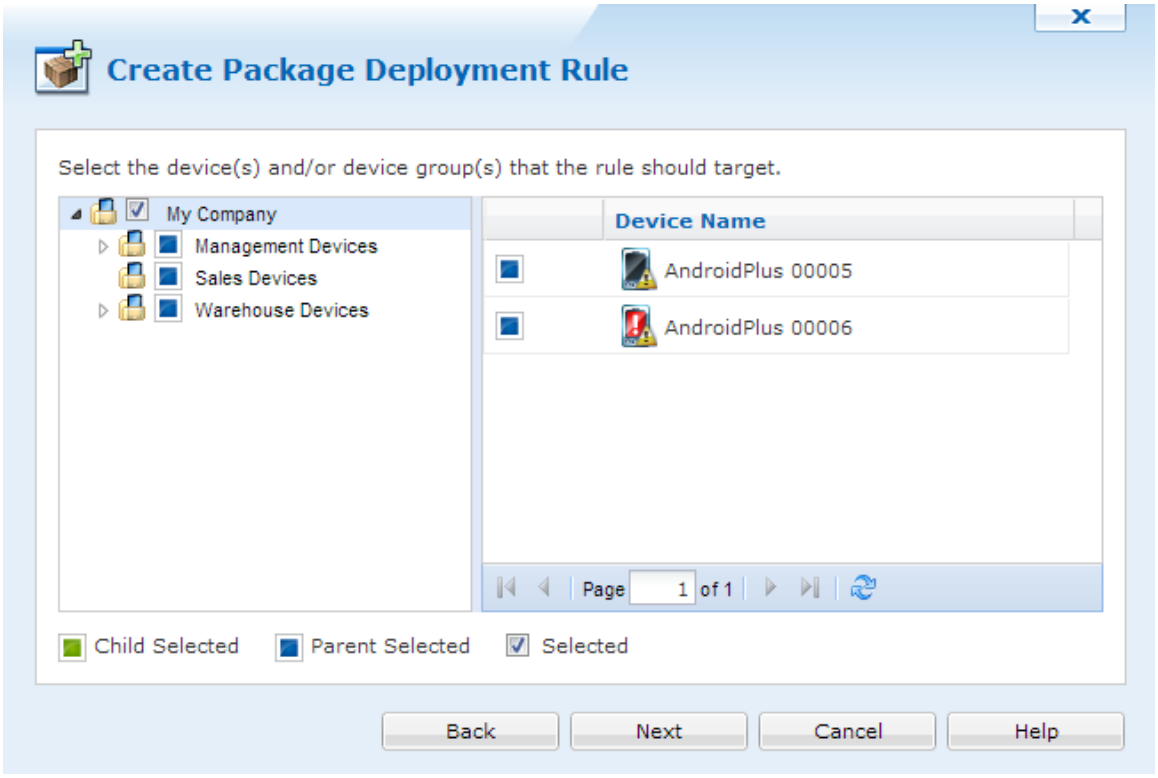
Add Package dialog

If the package to be installed has been created but not loaded into MobiControl, click the **Add Package** button and select the package file from the file system.

If the package has not yet been created, exit the wizard and use MobiControl Package Studio to create a package. (Please see the "MobiControl Package Studio" topic on page 413.)

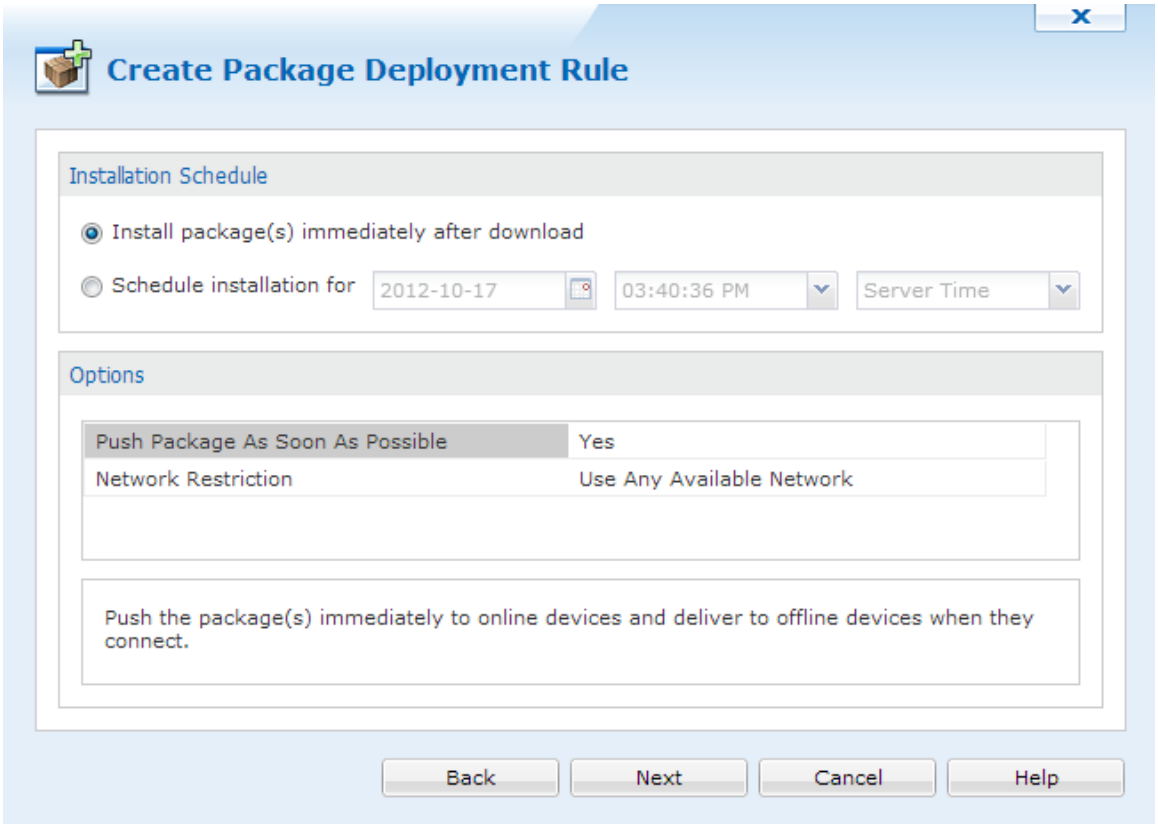
3. Select where the package(s) will be deployed.

   Select the device(s) or group(s) to which the package(s) will be deployed and click the **Next** button.



Device Group Selection page

4. Configure deployment rule optional settings.



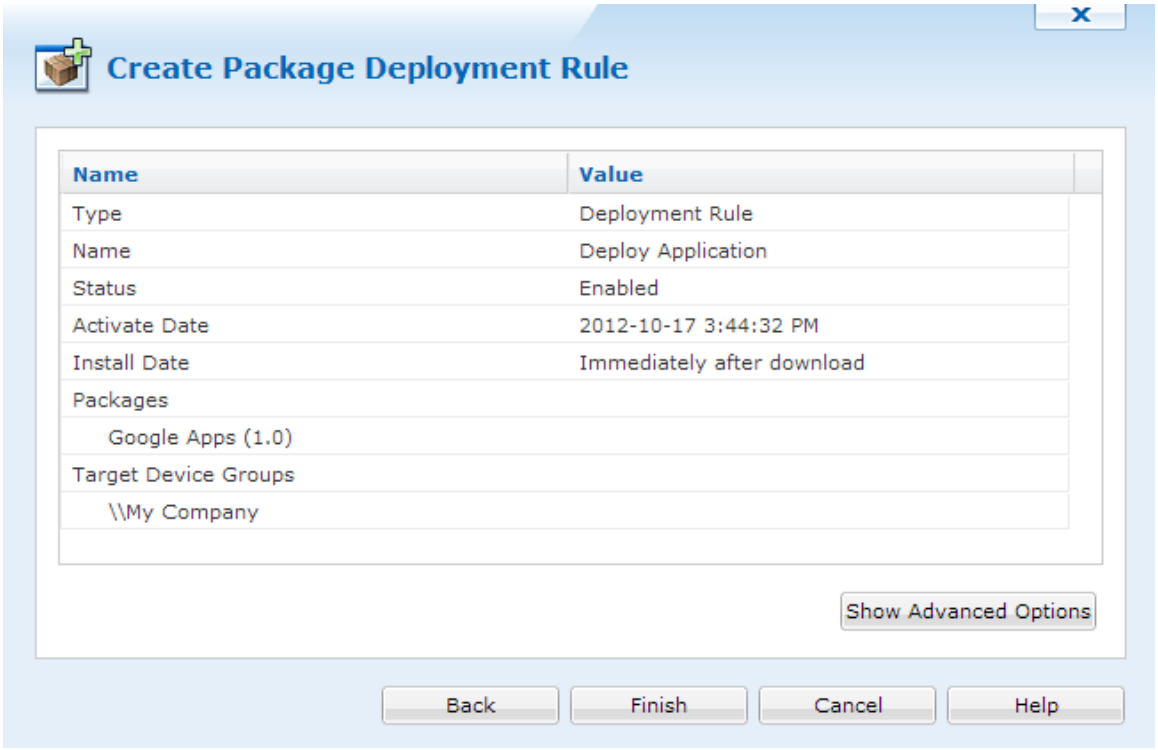
Device Settings Configuration page

The deployment rule can be customized to using the settings mentioned.

Field Name	Description
Install package(s) immediately after download	Selecting this will ensure that the packages are installed as soon as the devices receive them
Schedule installation for	If selected, this will ensure that packages are installed on the date specified after being downloaded by the devices
Push Packages As Soon As Possible	By default, packages will be deployed to the devices according to the device synchronization schedule. The device synchronization schedule is specified by the add devices rule used to add the device to MobiControl. If this option is selected, package(s) will be deployed to the target devices immediately. If the devices are currently offline, the package(s) will be deployed as soon as the device connects to MobiControl
Network Restriction	Restrict whether package deployment should take place over cellular data networks

5. Review the summarized information.

   A **summary** of the deployment rule is displayed. Review the settings you have chosen and click **Finish** to complete the wizard.



Summary page

NOTE:

After five unsuccessful attempts to deploy the package, deployment to that device is temporarily deferred. In order to start deployment of that package again, you must right-click the package from the Package panel and select **Force Re-install**.

Application Catalog Android+

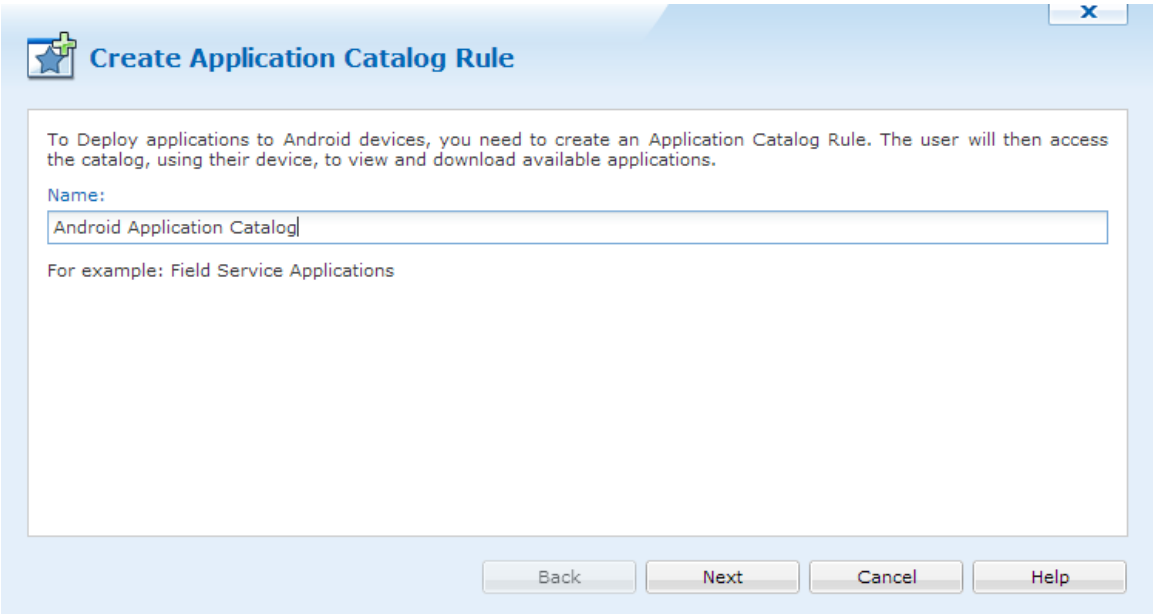
The Application Catalog allows us to let users know what approved apps they are able to download on their device. We can configure Play Store applications to appear, set it to be mandatory so that users must download it, or set it as optional. We can also upload enterprise built applications without posting them into the Play Store.

If an application is set to mandatory, the user will constantly be prompted to download it.

To create an Application Catalog, we must first create it's rule. To do this, go to the Android rule tab. Right click Application Catalog then click **Create Application Catalog Rule**.

Naming the Rule

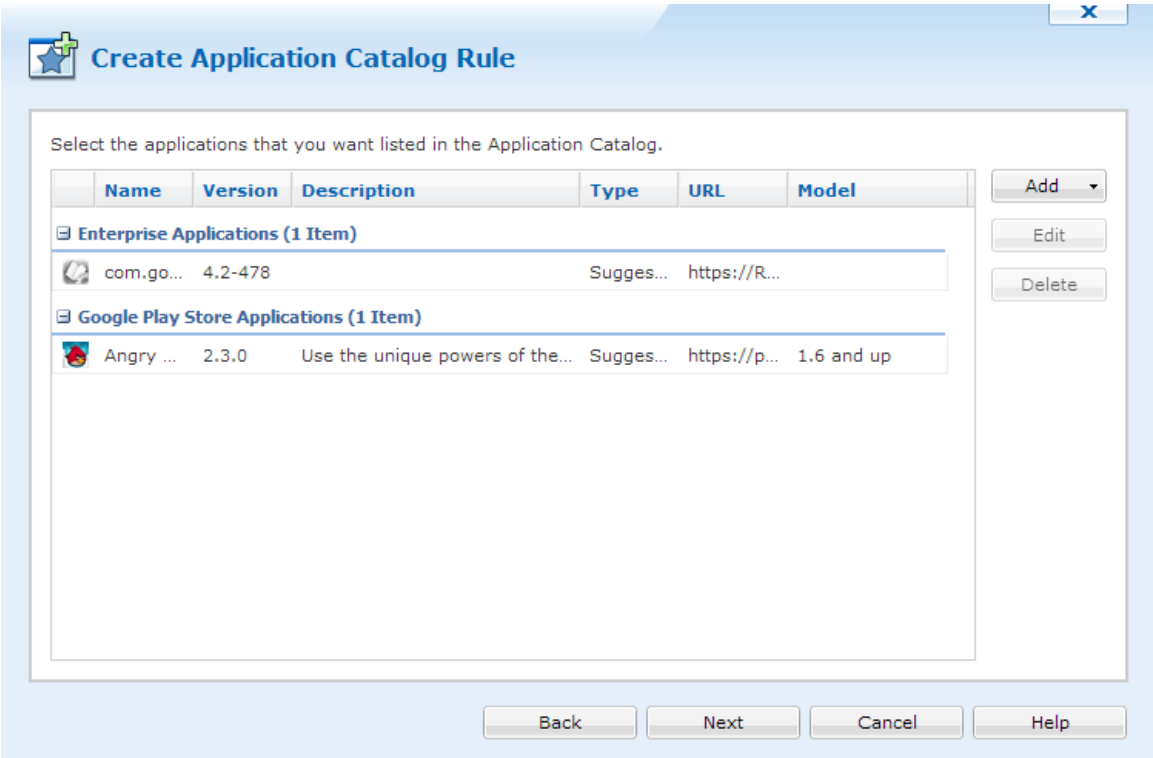
When the Application Catalog wizard appears, enter a name then click Next



Name the Application Catalog

Application Selection

The next panel will allow us to add App Store or Enterprise Apps.



Adding Applications

Click Add and select either Enterprise Applications or App Store Applications.

Clicking each header below will reveal more information about each topic:

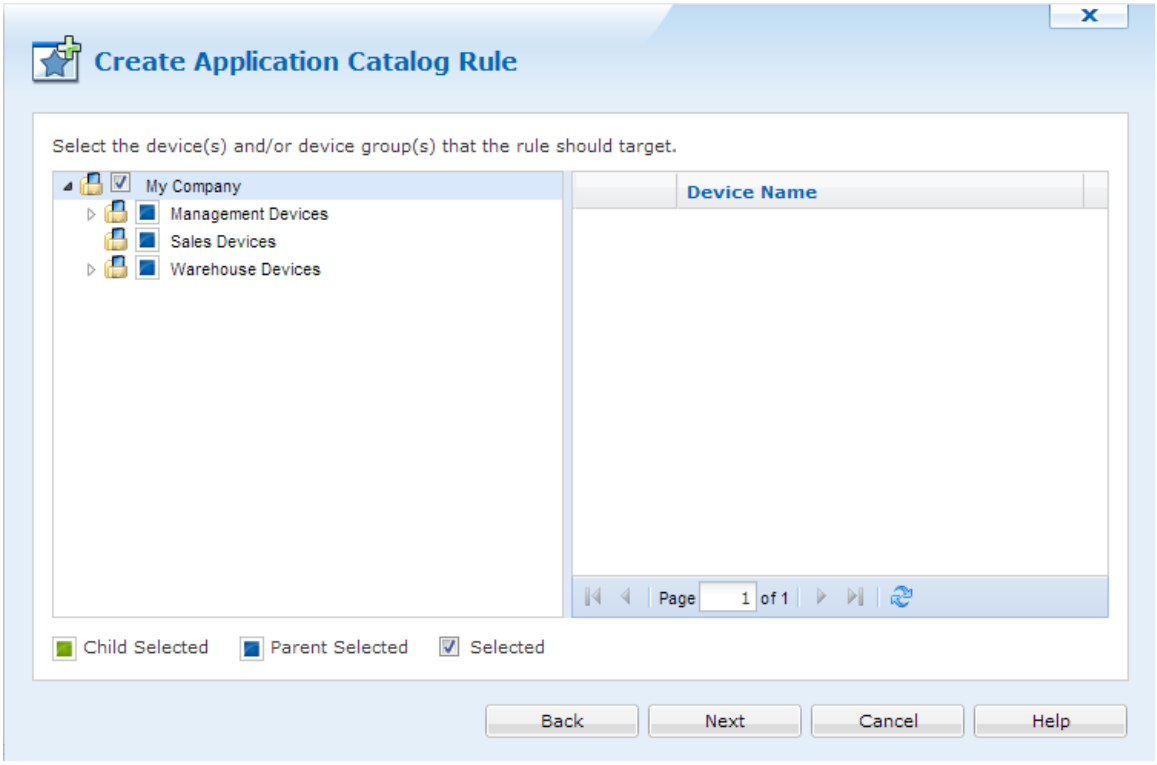
Enterprise Applications

Play Store Applications

After all desired apps are added, click Next.

Select Devices and Groups

The next panel will let us choose which groups and/or devices will receive this Application Catalog.

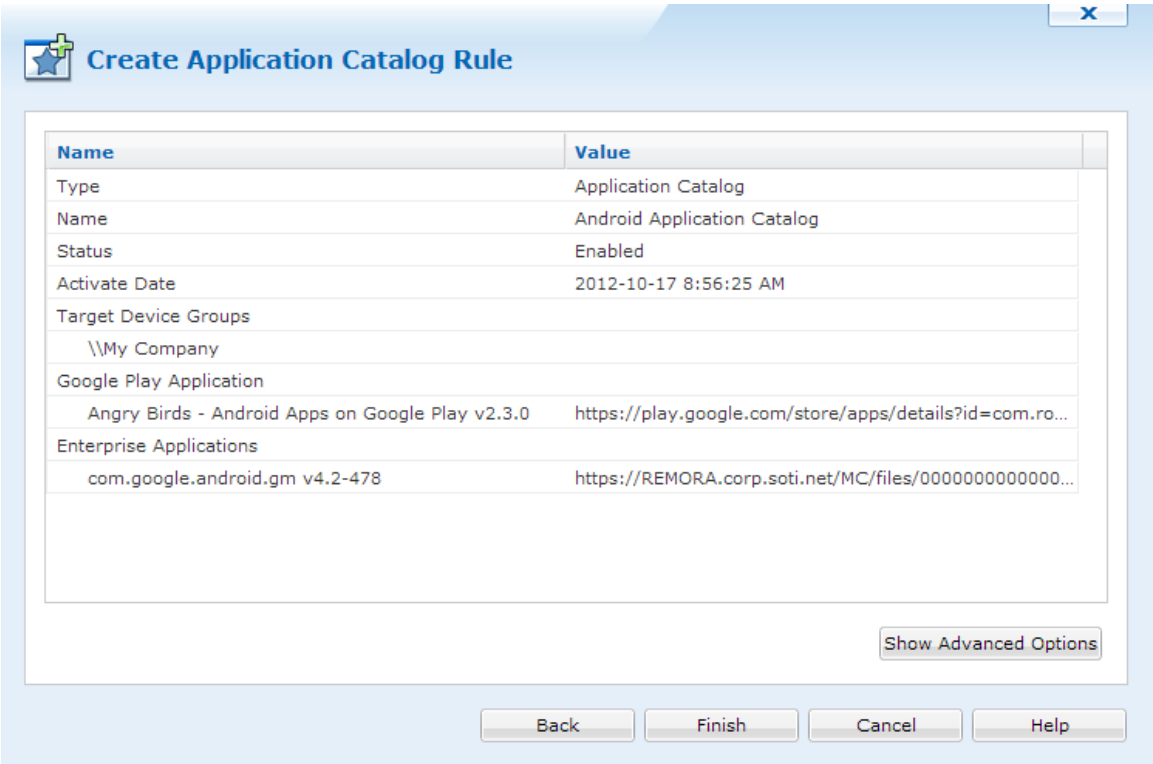


Target Groups or Devices

When devices are selected, click Next.

Summary

The last panel will show us a summary of the Application Catalog.



Application Catalog Summary

Clicking **Show Advanced Options** will allow us to configure more settings for the Application Catalog. Some of these settings include changing the Application Catalog banner.

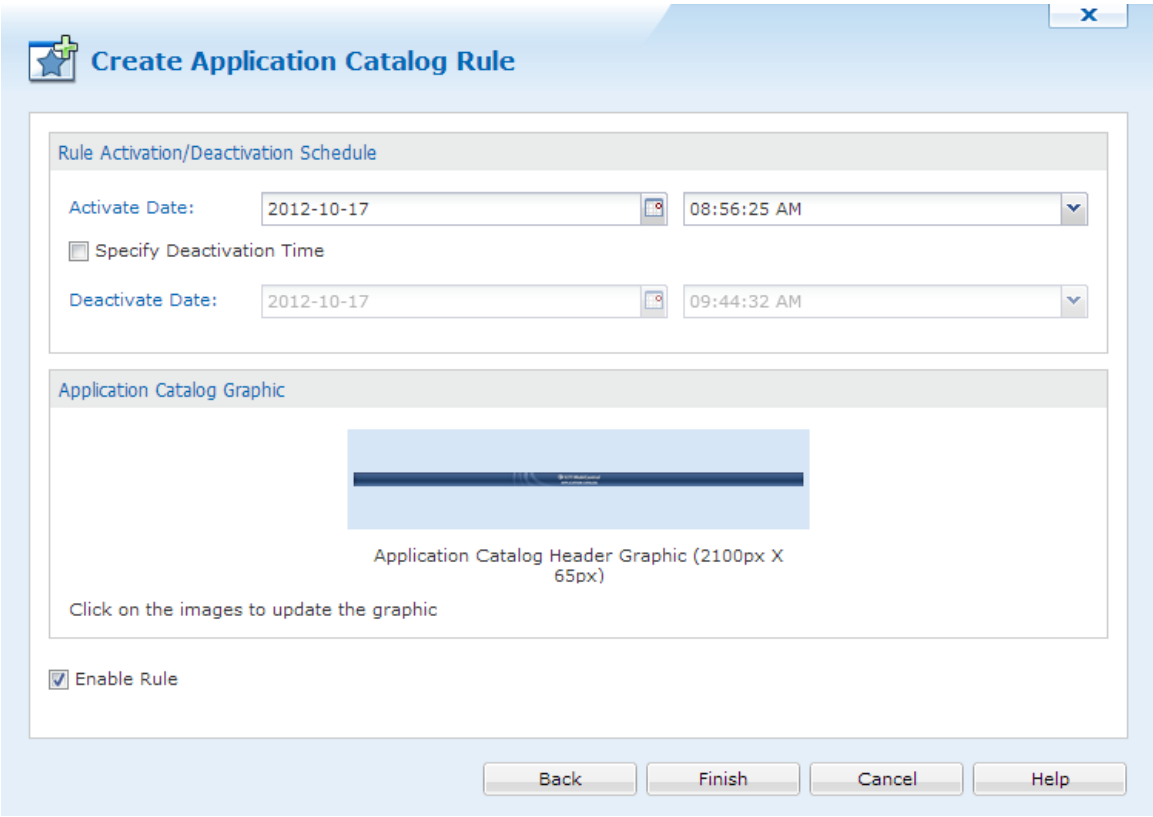
Advanced Options

Here we are able to set when this rule will be activated and deactivated, and change the Application Catalog graphics.

The Application Catalog icon is what would appear on the home screen, while the Application Catalog Header is what appears in the actual catalog. Clicking each image will allow us to upload new images.

NOTE:

The Application Catalog Header can be 2100px X 65px.



Application Catalog Advanced Options

After everything is configured, click Finish to save and close the wizard.

Android+ Creating File Sync Rules

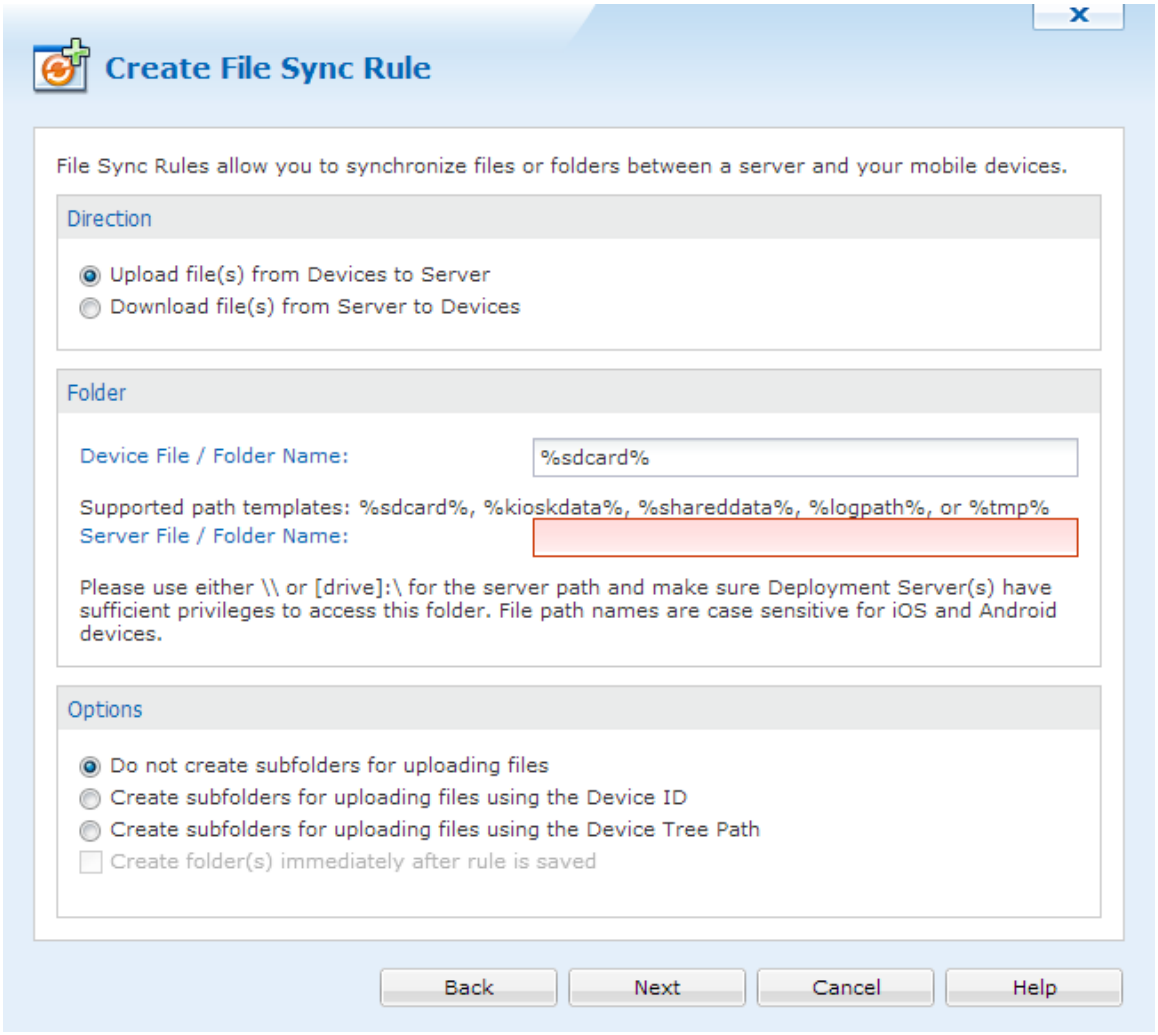
File sync rules allow you to synchronize files and folders between your devices and a server. File collection, also referred to as file uploading, is a very convenient method for gathering information from devices, for example a transaction log file. File dissemination, also referred to as file downloading, is a quick and easy way to send one or more files to a set of devices such as an updated product listing or configuration file.

1. Start the wizard.

   Select the Rules view (tab), then click **Rule,** point to **Create Rule,** and click **File Sync Rule.** Enter a meaningful name for the rule.

First page of the Create File Sync Rule Wizard

2. Configure file synchronization source and destination.



Configure file sync source and destination

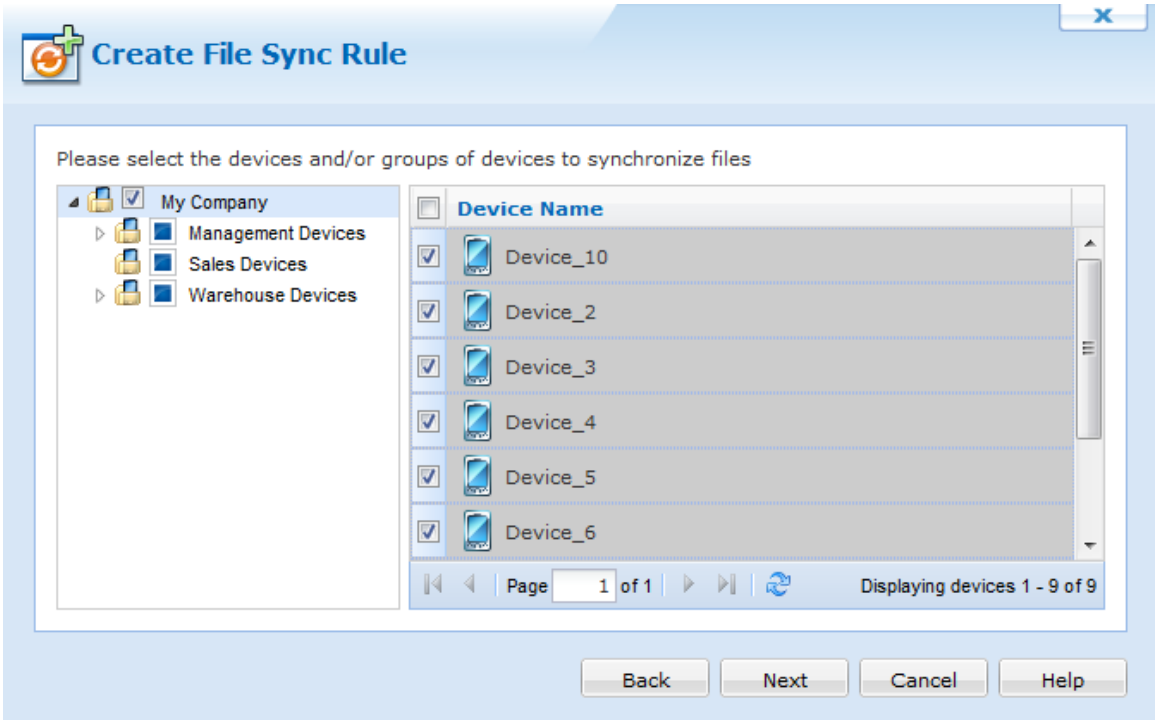
The following table describes the fields of this page of the wizard:

Field Name	Description
Direction	• **Upload** (File collection) The rule will be used to upload files from the devices to a server. • **Download** (File dissemination) The rule will be used to download files from the server to devices.
Device File/Folder	Specifies the complete file system path to the files or folders being synchronized on the device. "%sdcard%" is a global variable that is used to specify the devices external storage.

Field Name	Description
Server File/Folder	Specifies the complete file system path to the files or folders being synchronized on the server It is strongly recommended that a UNC (Universal Naming Convention) path be used. A local path (i.e. `C:\MyFiles`) can be used if only one Deployment Server is being used and the local path is on the computer running the Deployment Server. **NOTE:** It is important that the Deployment Servers have sufficient permission to read and write to the source or destination UNC path. Best practice is to run the Deployment Server under its own Active Directory user profile.
Server-side Folder Options	For **upload rules,** files collected from the devices can be written to: • A single shared folder, meaning files could potentially be overwritten if they have the same name. • A per-device subfolder, named using the device ID (i.e {00135304-41D7-019E-5800-0050BF3F5173}) • A per-device subfolder, named using the device tree path (i.e. `.\Management Devices\Device 0001`) For **download rules,** files disseminated from the server can be read from: • A single shared folder, meaning all devices get the same file (s). • A per-device subfolder, named using the device ID (i.e. {00135304-41D7-019E-5800-0050BF3F5173}) • A per-device subfolder, named using the device tree path (i.e. `.\Management Devices\Device 0001`)
Create folder(s) immediately after rule is saved	When the **Create folder(s) immediately after rule is saved** option is enabled, the server-side folders will be created immediately after the file sync rule is saved. This allows adding files to the folders on the servers that are synchronized with the devices when the file sync event occurs.

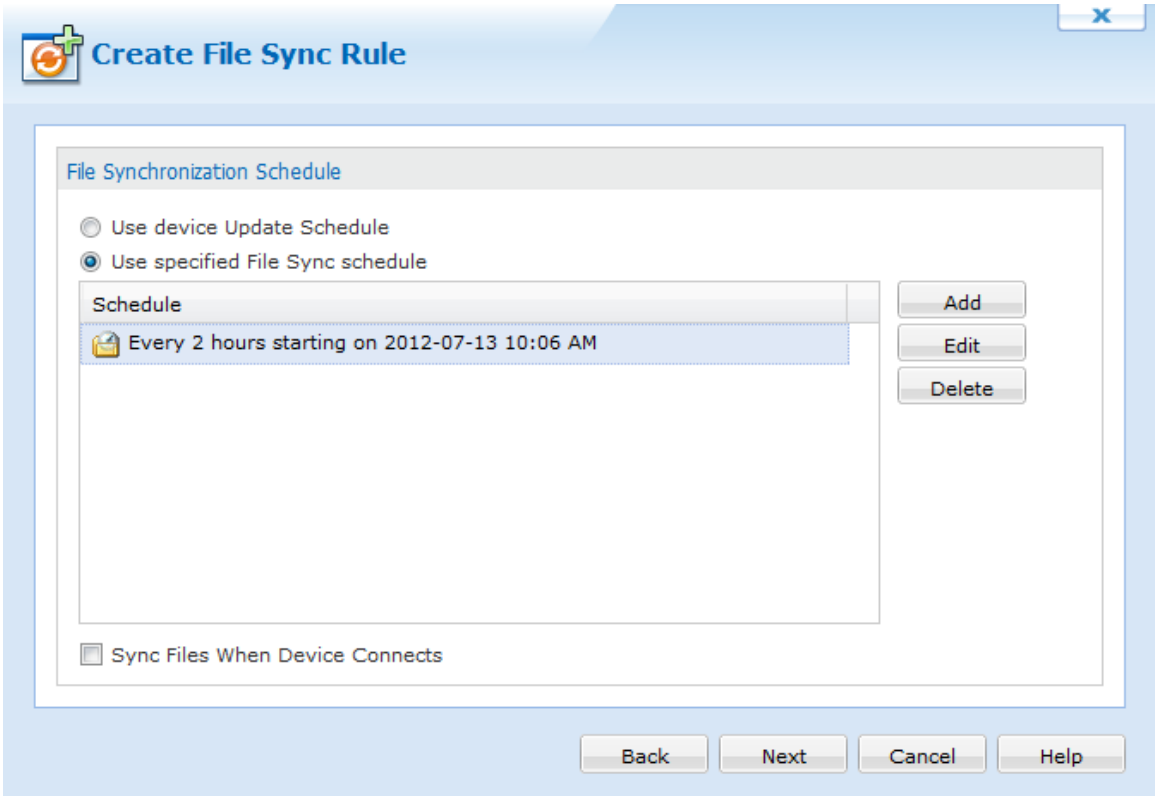
3. Select devices.

   Select the device(s) and group(s) for which the file sync rule will apply.



Device Group selection page

4. Specify the synchronization

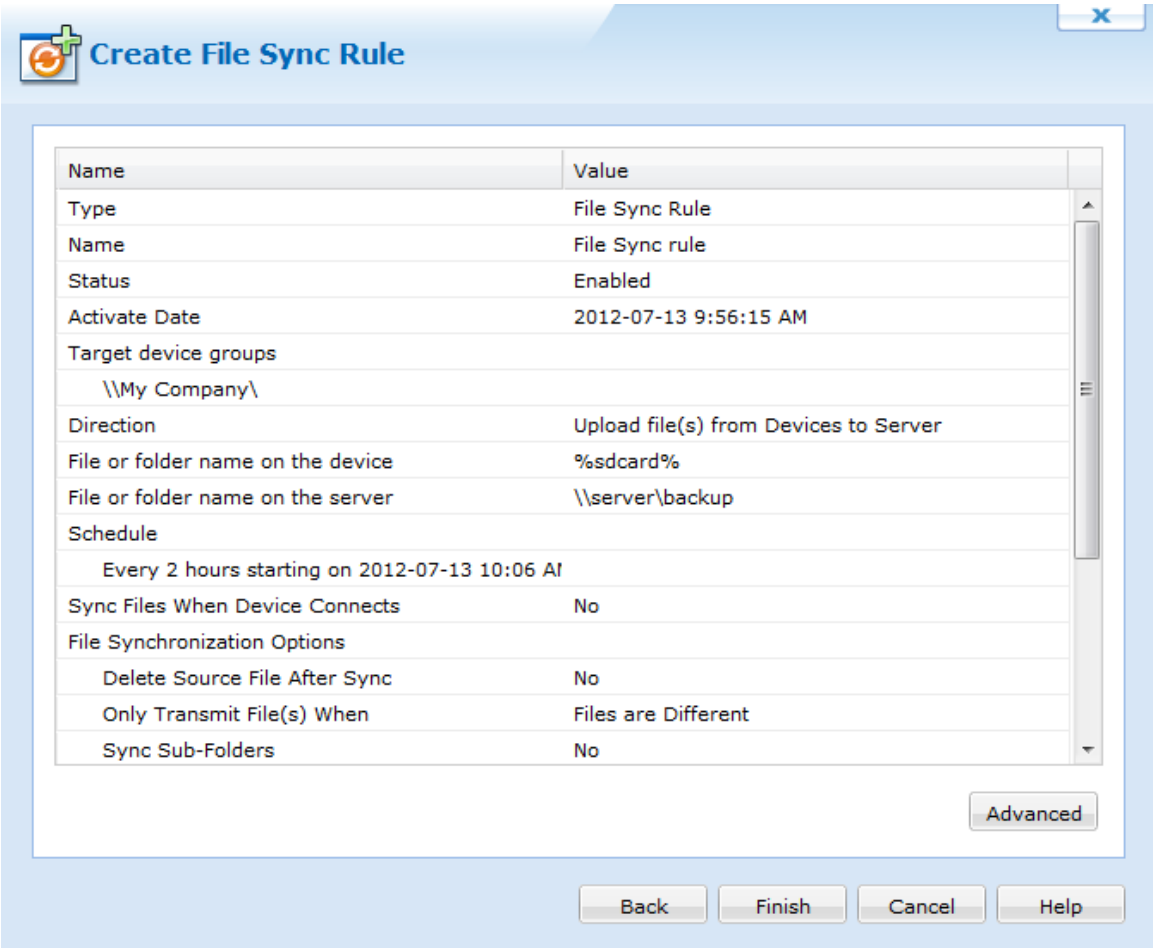


Rule activation schedule

Field Name	Description
Use Device Update Schedule	By default, the device update schedule (specified by the file sync rule used to add the devices to the system) triggers file synchronization
Use Specified File Sync Schedule	If you specify a file synchronization schedule in this dialog box, only that schedule will be used, and the device synchronization schedule will not trigger file synchronization. To Specify the custom schedule click the **Add** button. Please see the "File Synchronization Schedule" topic on page 1238 for more information about creating a custom file sync schedule.

5. Review summarized information

Review information on the **file sync rule summary page**. This page gives you an opportunity to review the settings of the file sync rule before committing them. If you wish to make any corrections, click the **Back** button. Clicking the Advanced button allows additional File sync rule configuration.

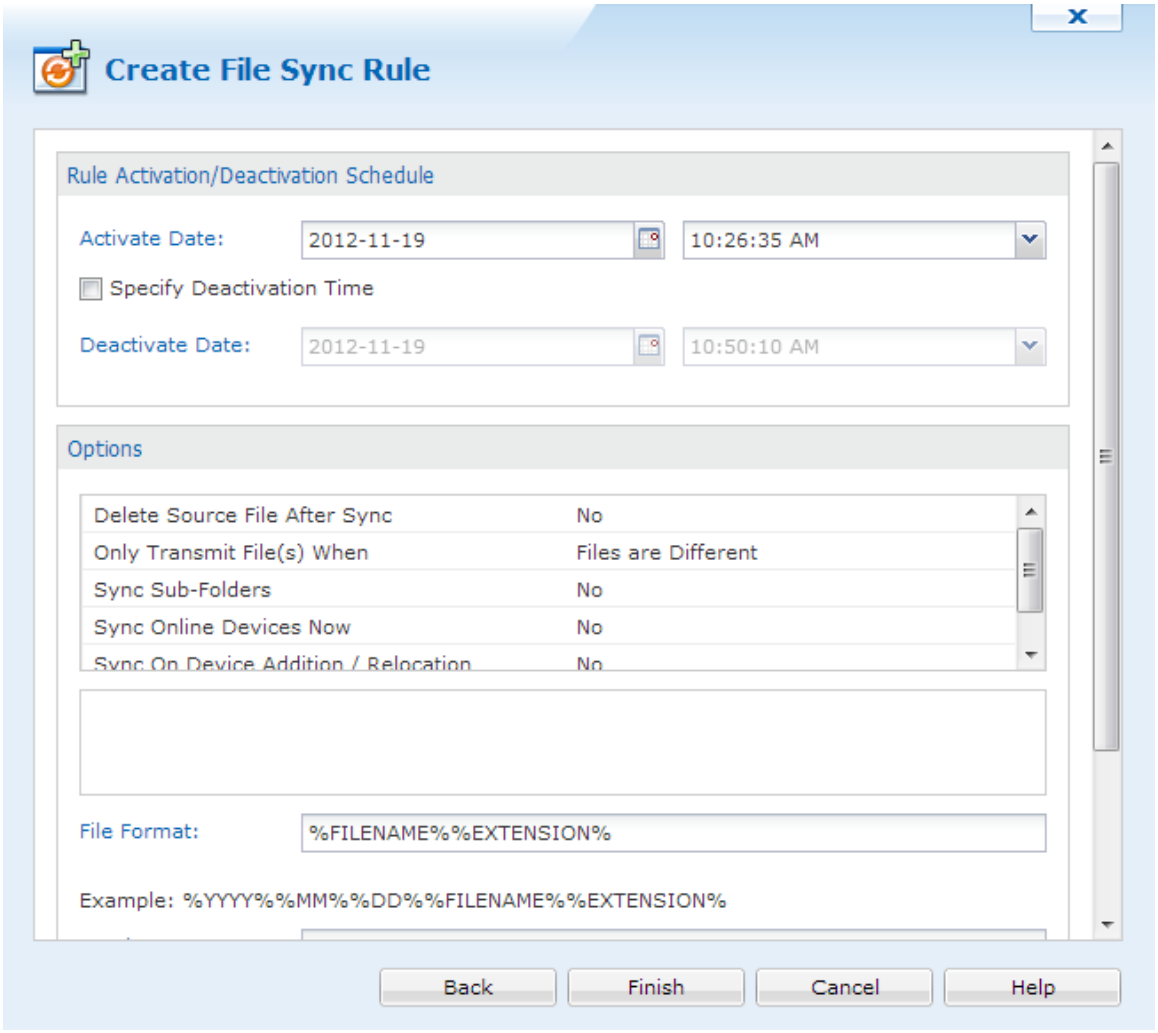


Summary page

6. Advanced options

The following table describes the file synchronization options on this page of the Create File Sync Rule Wizard. By default, the file sync rule will be activated immediately upon completion of the wizard. If you wish to delay the activation you can modify the activate date. A deactivate date can

optionally be entered to specify a date from which the rule will be disabled.



File synchronization options

Field Name	Description
Delete Source File After Sync	(This applies only to upload rules.) When selected, the source file(s) on the device are transmitted to the server and then deleted from the device.

Field Name	Description
Only Transmit File (s) when	• The **Always Transmit** option will cause file(s) to be uploaded or downloaded regardless of whether or not the source and target are different or the same. • The **Files are different** option will cause file(s) to be uploaded or downloaded only if the source file is different from the destination file. • The **Source file is newer** option will cause file(s) to be uploaded or downloaded only if the source file has a more recent date-time stamp. • The **Destination file does not exist** option will cause file(s) will cause file (s) to be uploaded or downloaded only if the destination file does not exist.
Sync Sub-Folders	Synchronize files in sub-folders in addition to the files located in the target folder
Sync Online Devices Now	File synchronization will be executed immediately following the completion of the wizard for online devices.
Sync On Device Addition or Relocation	Perform file synchronization when a device is added or relocated to a device tree group for which this rule has been configured This setting is useful to easily invoke file synchronization when a device is moved from one group to another in the device tree.
Network Restriction	Restrict whether file synchronization should take place over cellular data networks (i.e. GPRS)

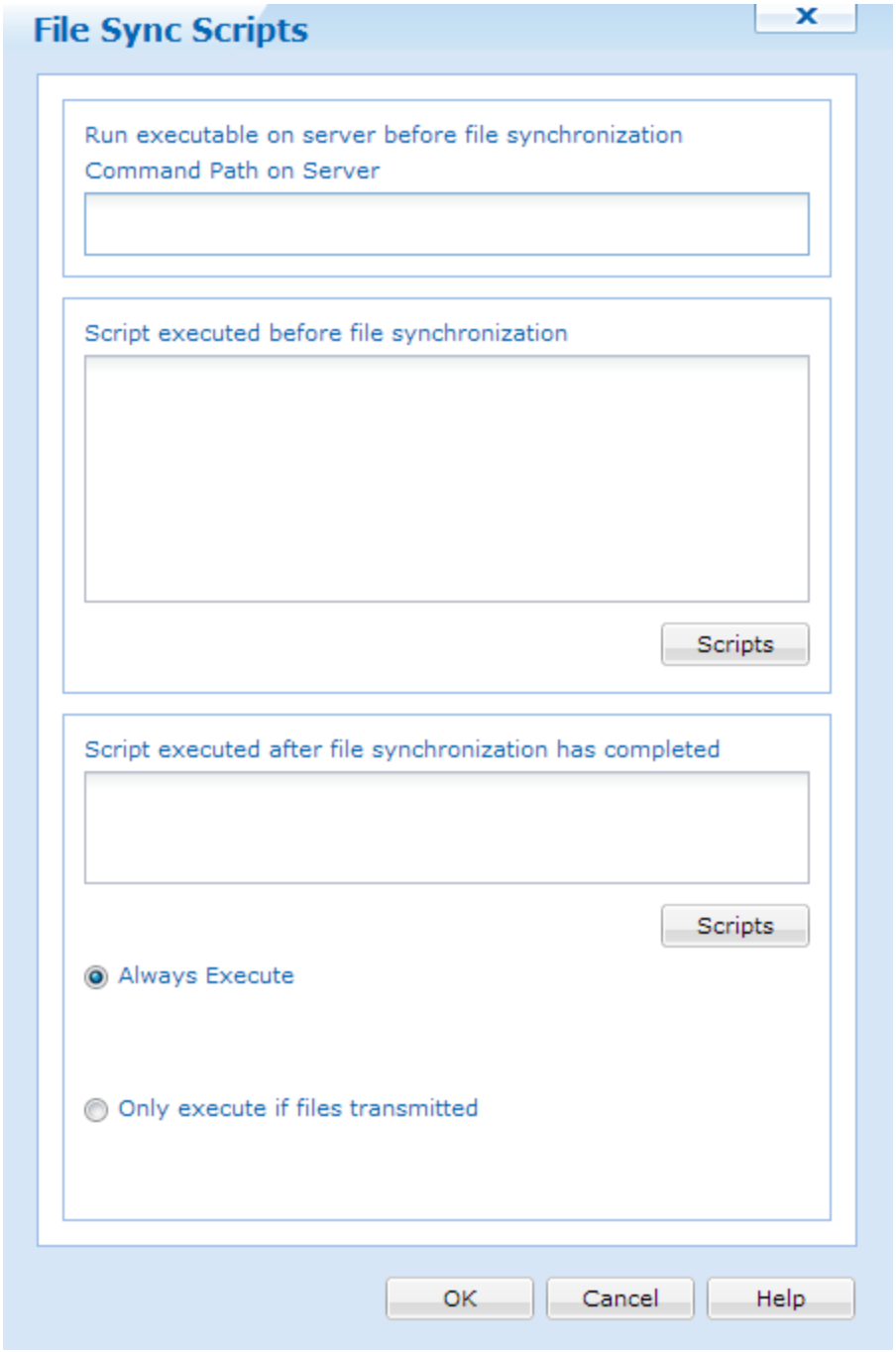
Click the **Scripts** button to configure file synchronization scripts.

File Synchronization Scripts

File synchronization scripts provide flexibility in automating actions on the server before the file sync or on the device pre or post file synchronization.

EXAMPLE: RUN EXECUTABLE ON SERVER

MobiControl contains plenty of server side utilities used to manage devices in the deployment server. One of these utilities is a device move. If this utility is ran before the file sync, we can ensure that all the devices are in the proper location before syncing the files down. For additional help with this utility and more, please contact us.



File synchronization advanced options

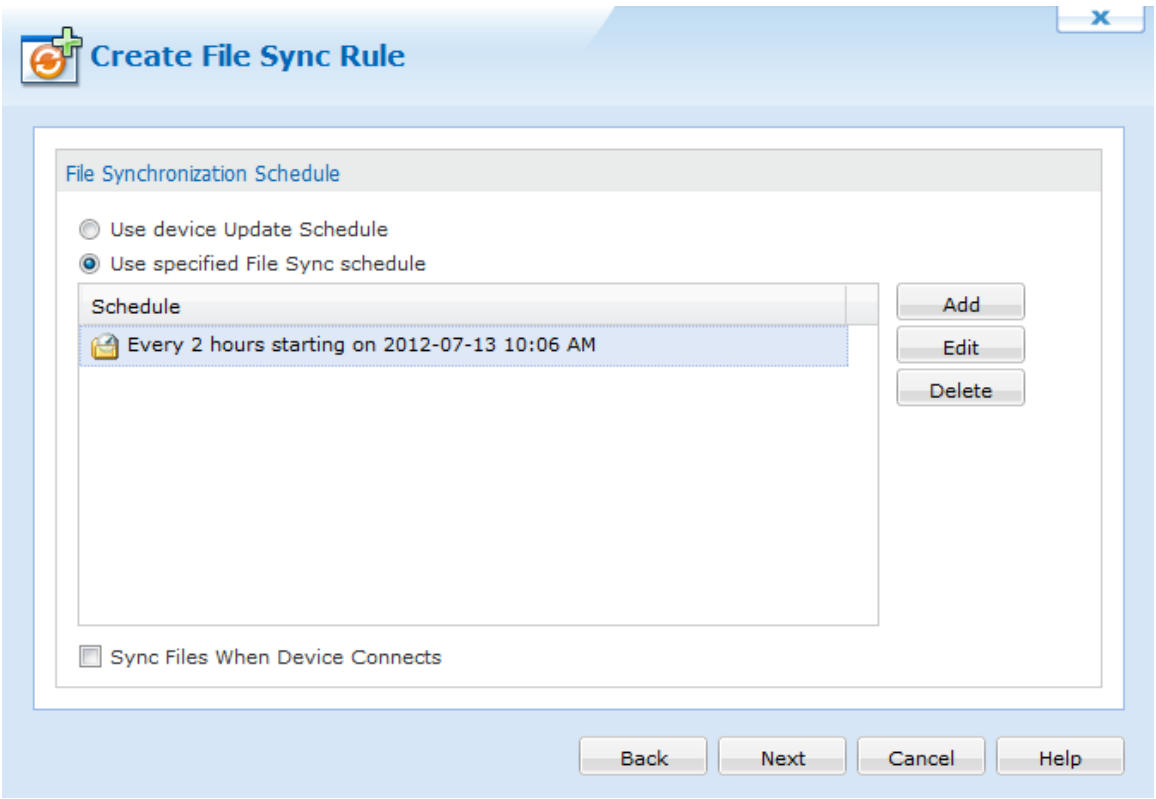
Field Name	Description
Always execute	Will execute the script every time there is a scheduled sync, even if the files are updated or not
Only execute if files transmitted	Will execute the script when files have been updated by the sync schedule
Scripts	Will allow you to import previously created scripts

Android+ File Synchronization Schedules

The file synchronization schedule specifies when the Deployment Server(s) should check device(s) for synchronization.

If the Deployment Server identifies an inconsistency, such as a mismatch in the file size or finds the new file, the Deployment Server will act according to the file sync rule.

By default, the device synchronization schedule, specified by the add devices rule used to add the devices to the system, is selected for file synchronization. You may add, edit or delete the custom schedule using the following dialog box.



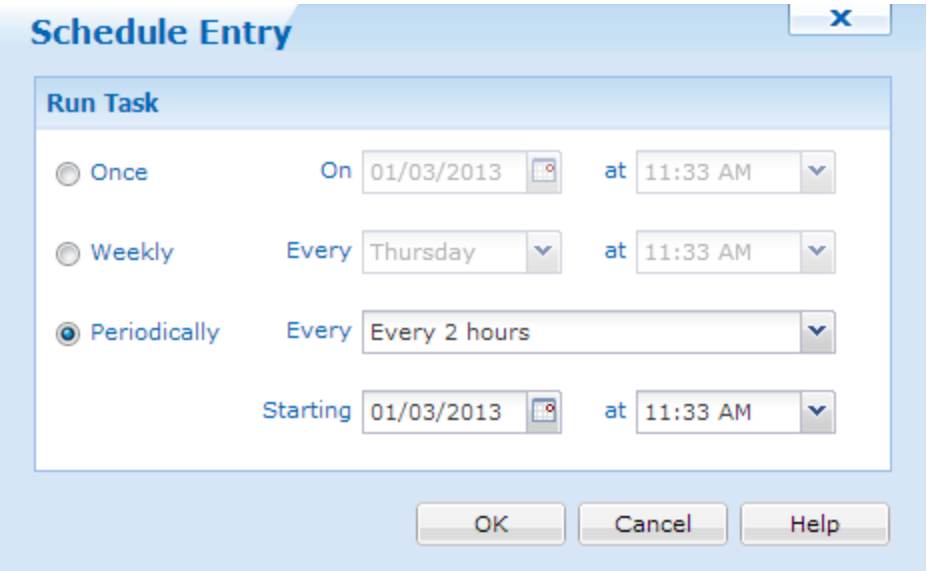
Create File Sync Rule Wizard dialog box

The following table describes the fields of the Create File Sync Rule Wizard dialog box.

Field Name	Description
Add	Specify your own file synchronization intervals. When you select **Add,** the **Schedule Entry** dialog box is displayed. **EXAMPLE:** To sync twice a week (Monday at 06:00 and Friday at 19:00), create two weekly schedule entries.
Edit	Select **Edit** to modify an existing schedule entry. The **Schedule Entry** dialog box is will be displayed.
Delete	Permanently remove a file sync schedule entry from the dialog box
Sync Files when device connects	Sync whenever devices under this rule connect to a Deployment Server (i.e. transition from offline to online)

Schedule Entry

The **Schedule Entry** dialog box allows you to specify schedule entries as one-time or periodic events.



Schedule Entry dialog box

Field Name	Description
Once	Device will check for file synchronization once at the specified date and time.
Weekly	Device will check for file synchronization once a week, on a specified day and time.
Periodically	Device will check for file synchronization periodically at the specified interval from the set, start date-time.

Android+ Device Relocation Rules

Dynamic device relocation allows you to set up rules to move your mobile devices automatically between different virtual groups or device groups in the MobiControl device tree based on the IP address or other custom criteria. This is useful when managing mobile devices in a deployment where the device tree is set up to represent different physical locations (e.g. retail stores, warehouses, regional offices, etc.).

In a deployment that has mobile devices connecting from and moving frequently between several different sites, properties or regions, the administrator needs visibility over the movement of mobile devices across different locations. Dynamic device relocation allows the MobiControl device tree to be updated automatically when a device moves to a different location (e.g. a mobile device that has moved from a warehouse or site in Chicago to a site in New York will automatically be relocated in the device tree on reconnection and will appear in the device group for devices in New York based on the new IP address information). Additionally, the devices can also be automatically reconfigured and any modifications to the mobile device settings, specific to the new location, will be sent to the device automatically.

The devices are relocated based on the IP address ranges specified for each location. You can also create a custom data identifier which can be the criterion that will be utilized to relocate the devices to the appropriate device group. (Please see the "Android+ Custom Data" topic on page 1346 for detailed information on custom data identifiers.)

1. Start the wizard.

   From MobiControl Manager, select the Rules view (tab), then click **Rule,** select **Create Rule,** and click **Create Device Relocation Rule.** The first page of the Create Device Relocation Rule Wizard will be displayed. Enter a meaningful name for the rule and click **Next** to continue.

Create Device Relocation Rule Wizard startup dialog box

2. Review the device relocation mappings.

This page lists **device relocation mappings** that determine how the devices would be relocated and in which groups they would appear if the specified criteria is met. When a device connects to the MobiControl Deployment Server, its IP address and custom data information will be checked against all device relocation rules configured, and it will be moved to the appropriate device group based on the information in the relocation mappings.

NOTE:

Devices that are already connected and online in MobiControl will be relocated when they disconnect and re-connect to the MobiControl Deployment Server.

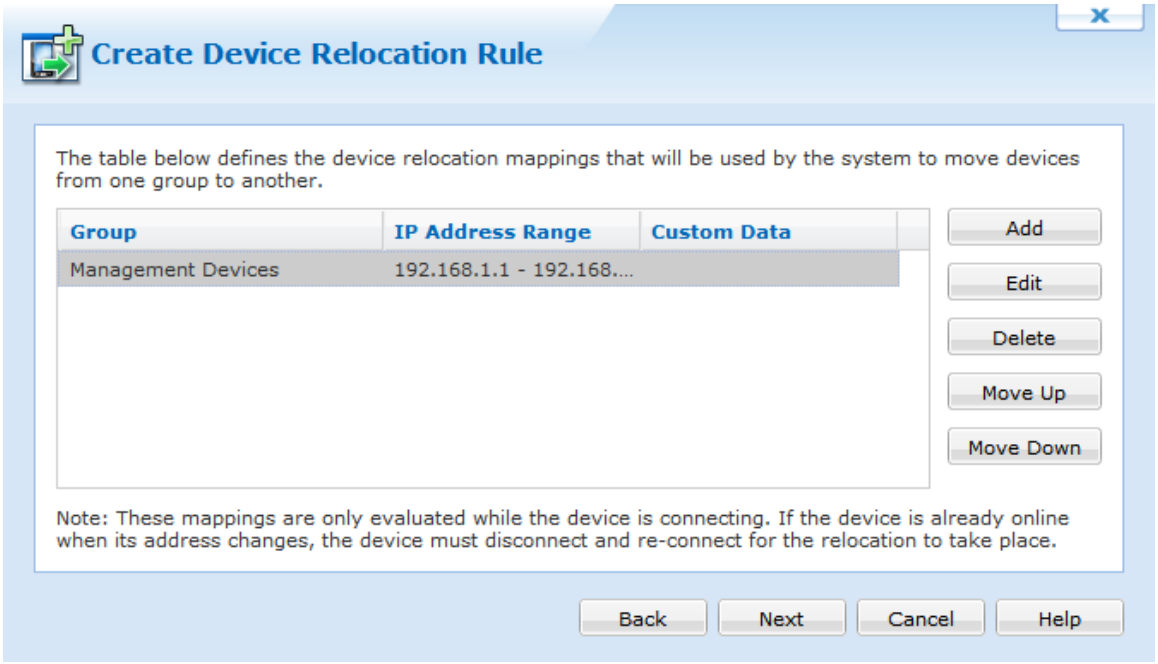
Edit Device Relocation Rule dialog box

The buttons on the **Edit Device Relocation Rule** dialog box are explained below:

Button Name	Description
Add	Click the **Add** button to add an entry for the relocation mapping.
Edit	Click the **Edit** button to change the settings for an existing relocation mapping entry.
Delete	Click the **Delete** button to delete a relocation mapping entry.
Move Up / Move Down	Click these buttons to change the order of the relocation mappings. The entry listed higher in the list have a higher priority and take precedence over entries listed lower in the list. For more details, read about relocation mappings priority below.

A relocation mapping can use just the IP address or the custom data entry to specify the relocation rule for mobile devices. If a relocation mapping has both the IP address and custom data entry specified as the criteria, the mobile devices would be relocated only if both these conditions are satisfied. If a device is affected by more than one relocation mapping, the one

higher in the list of mappings will have a higher priority and will be effective. You can use the **Move Up** and **Move Down** buttons to change the precedence of the relocation mappings if multiple mappings apply to a device.

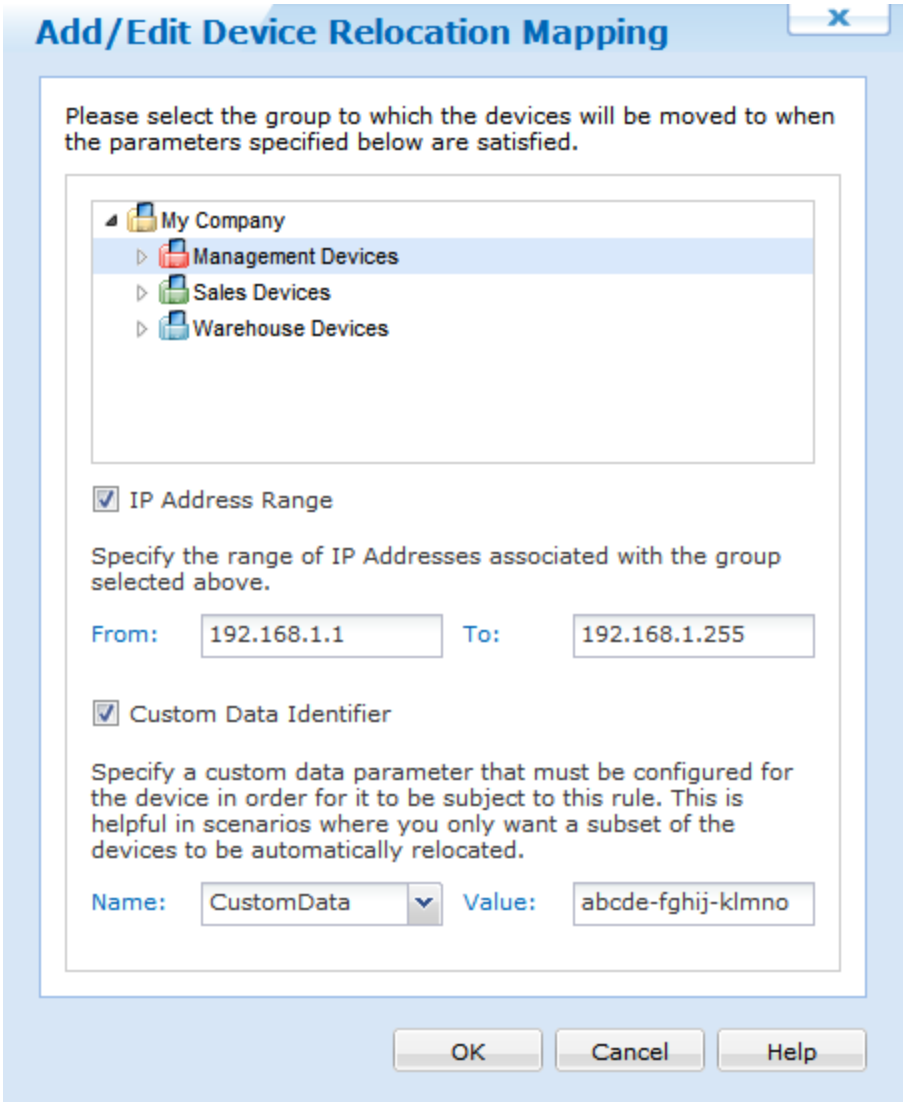


Device Relocation Mappings dialog box

The first two relocation mappings in the previous screenshot have been defined: one is for relocating all devices with IP addresses between 192.168.1.1 and 192.168.1.255 to the Management Devices group and another mapping for relocating all the devices for which the custom data item "Location" has a value of "Region A" to the Warehouses group. Since the relocation mapping with the IP address filter is listed above the mapping with the custom data filter, the IP address mapping will take precedence. If a device satisfies both conditions (e.g. has an IP address 192.168.1.10 and a value "Region A" for "Location"), it will be relocated to the Management Devices group.

3. Add or edit device relocation mappings.

   A relocation mapping includes the target or destination group (which can be a virtual group) to which the devices would be relocated. It also includes the conditions or the relocation parameters that must be satisfied for a device to be relocated.



Add/Edit Device Relocation Mapping dialog box

The **target group** is the group, sub-group, or virtual group to which devices will automatically be relocated when connecting to the Deployment Server if the conditions specified in the relocation parameters are met.

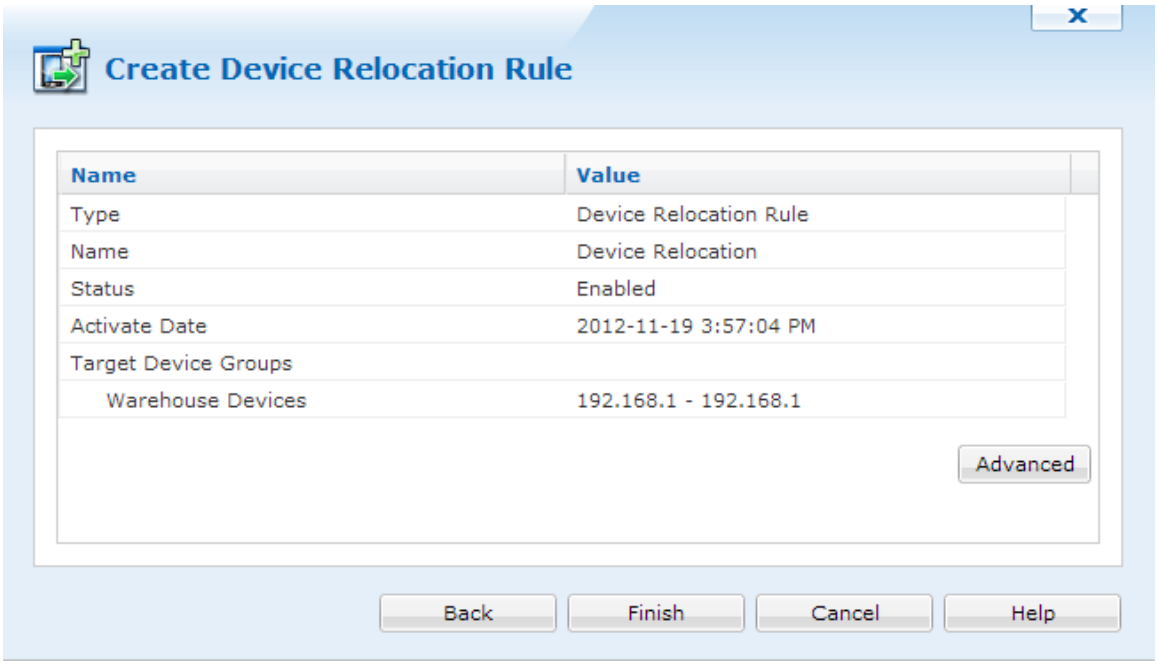
Multiple **relocation parameters** can be specified to manage the dynamic relocation of devices. A single parameter can be specified or both parameters can be used for a relocation mapping, in which case the device will be relocated if it satisfies both parameters.

The following table describes the fields of the **Add/Edit Device Relocation Mapping** dialog box:

Field Name	Description
IP Address Range	Devices can be automatically relocated based on the IP address information of the device at the time it connects to a Deployment Server. A range of IP addresses can be specified and if the device's IP is within that range, the device will be relocated to the target group.
Custom Data Identifier	You can use a custom data value as one of the criteria for relocating devices from one device group to another. MobiControl allows you to retrieve arbitrary data from the device's registry, files on the device and other sources using custom data. Please see the "Windows Mobile Custom Data" topic on page 700 for more information.

4. Review the summarized settings.

   This page gives you an opportunity to review the settings of the device relocation rule before committing them to the database. If you wish to make any corrections, click the **Back** button, otherwise click **Finish** to complete the wizard.



Device Relocation Rule Summary dialog box

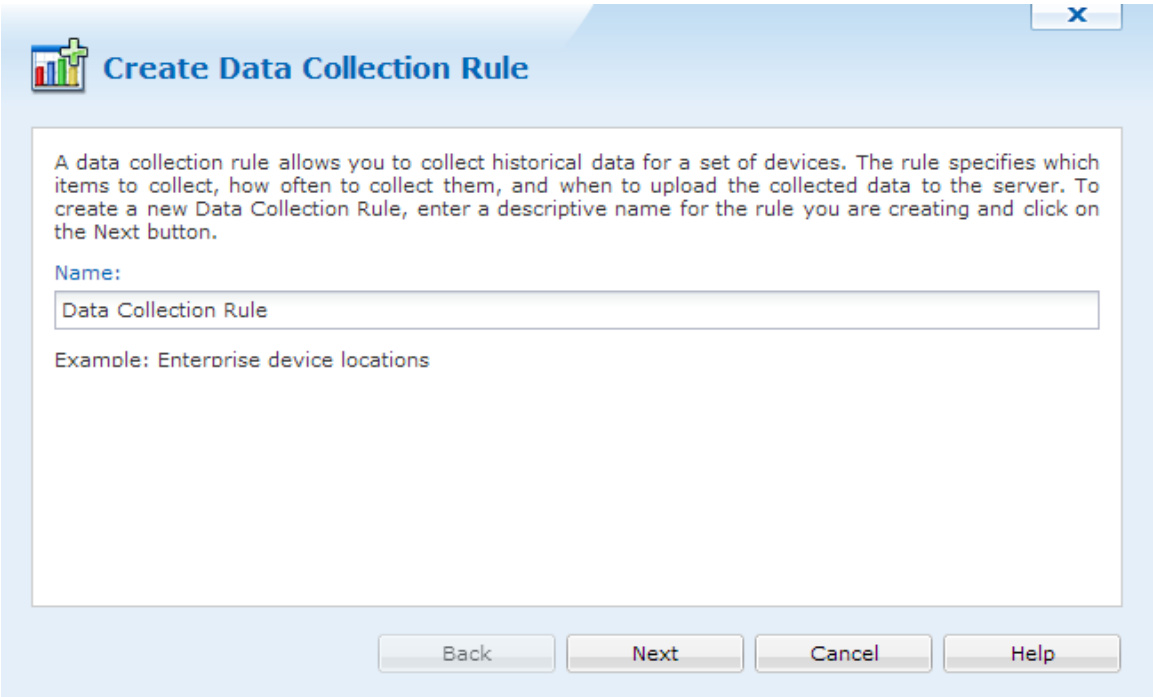
Android+ Data Collection Rules

Data collection rules allow administrators to automatically collect a variety of data from mobile device(s).

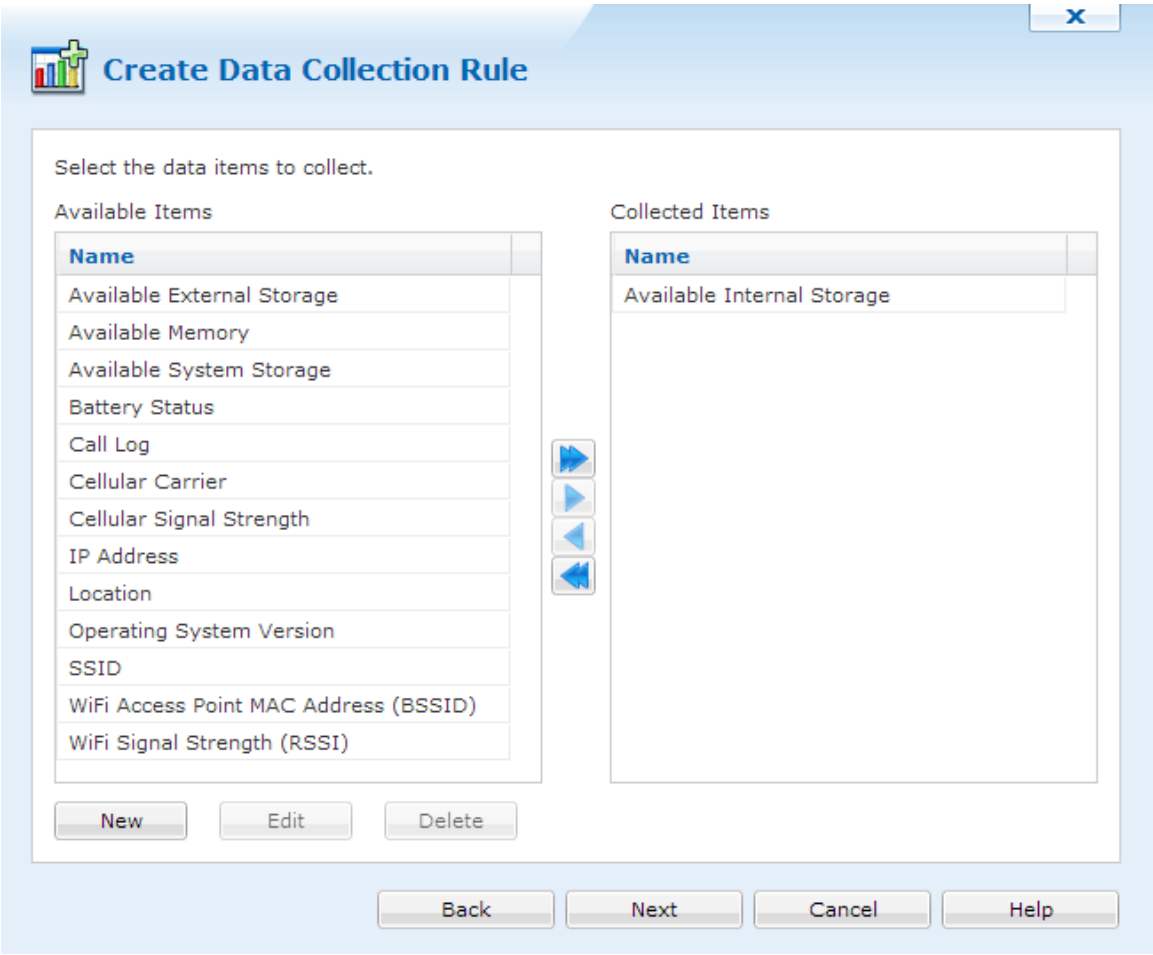
The following series of steps describes how to use the Create Data Collection Rule Wizard to create a data collection rule:

1. Start the wizard.

   From MobiControl Manager, select the Rules view (tab), then click **Rule,** click **Create Rule,** and click **Data Collection Rule**. Enter a meaningful name for your new data collection rule and then click **Next**.



2. Select data items to collect.



Select individual items or all items from the **Available Items** list by highlighting and then select the corresponding direction arrow(s). These items will move to the **Collected Items** list. If you have added something that you would like to remove from the **Collected Items** list, simply select the

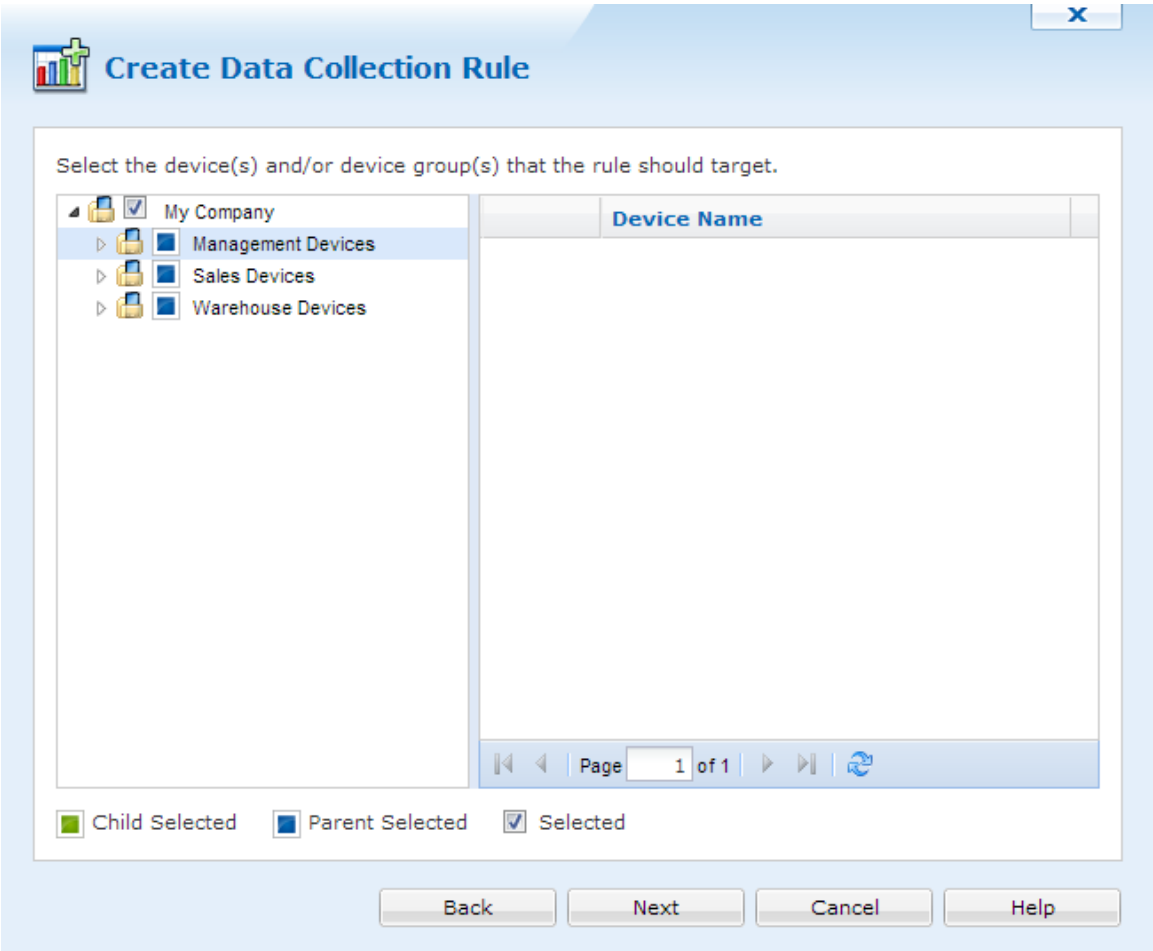
item and then click the direction arrow(s) to place the item(s) back into the **Available Items** list.

Item Name	Description
Available External Storage	Shows the amount of external storage available on the device
Available Internal Storage	Shows the amount of internal storage available on the device
Available Memory	Shows the amount of RAM the device has available
Available System Storage	Shows the total amount of system storage available on the device
Battery Status	Shows what percent the battery was at the time the data collection rule ran
Call Log	Shows the call log of the device. i.e. What numbers were dailed outbound and inbound.
Cellular Carrier	Shows what carrier the device is connected to at the time the data collection rule ran
Cellular Signal Strength	Shows what the signal strength is of the device at the time the data collection rule ran
IP Address	Shows the IP address of the device at the time the data collection rule ran
Location	Collects the location of the device
Operating System Version	Collects the version of the operating system currently on the device.
SSID (Wi-Fi Name)	Shows the SSID that your device is currently connected to
RSSI (Wi-Fi Signal Strength)	Shows the signal strength of a wireless connection. A value of 0 is collected when there is no Signal listed in Manager
BSSID	Shows the MAC address the device is connected to

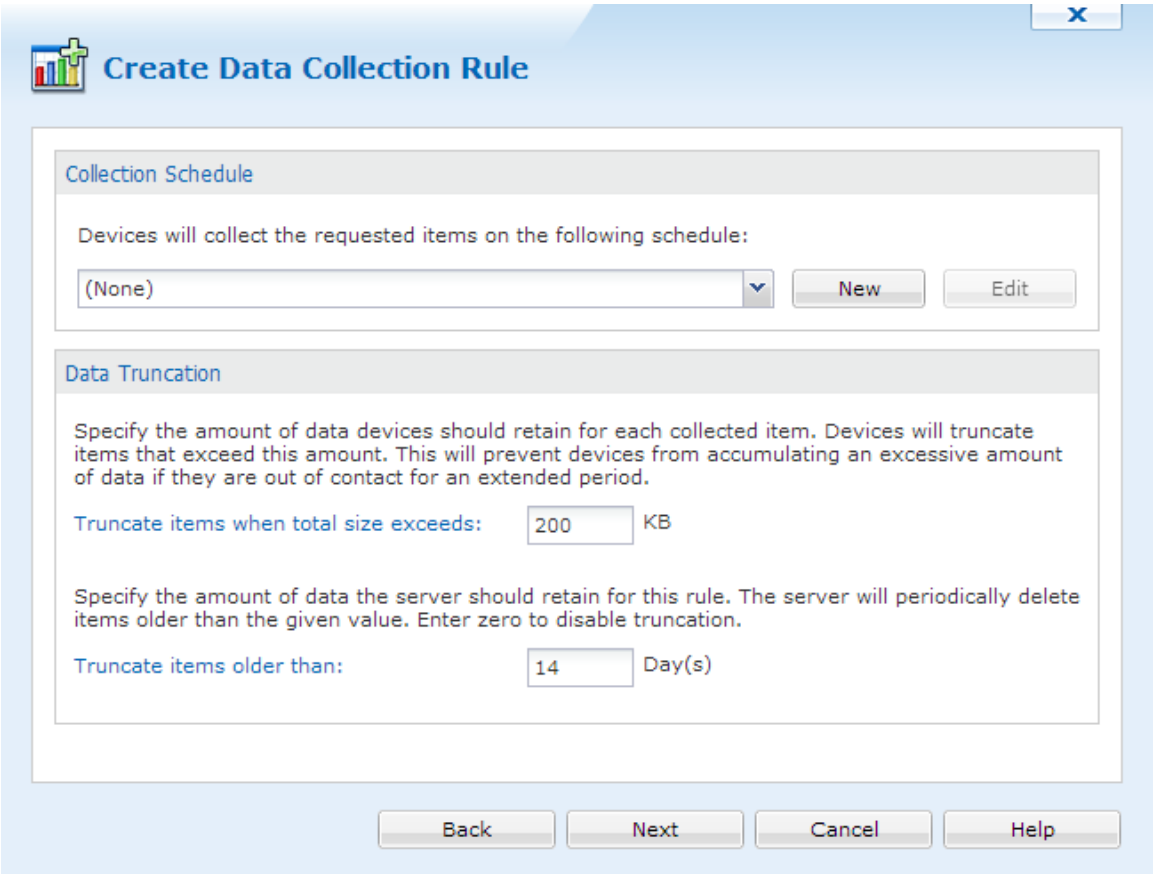
After selecting the choice(s), click the **Next** button.

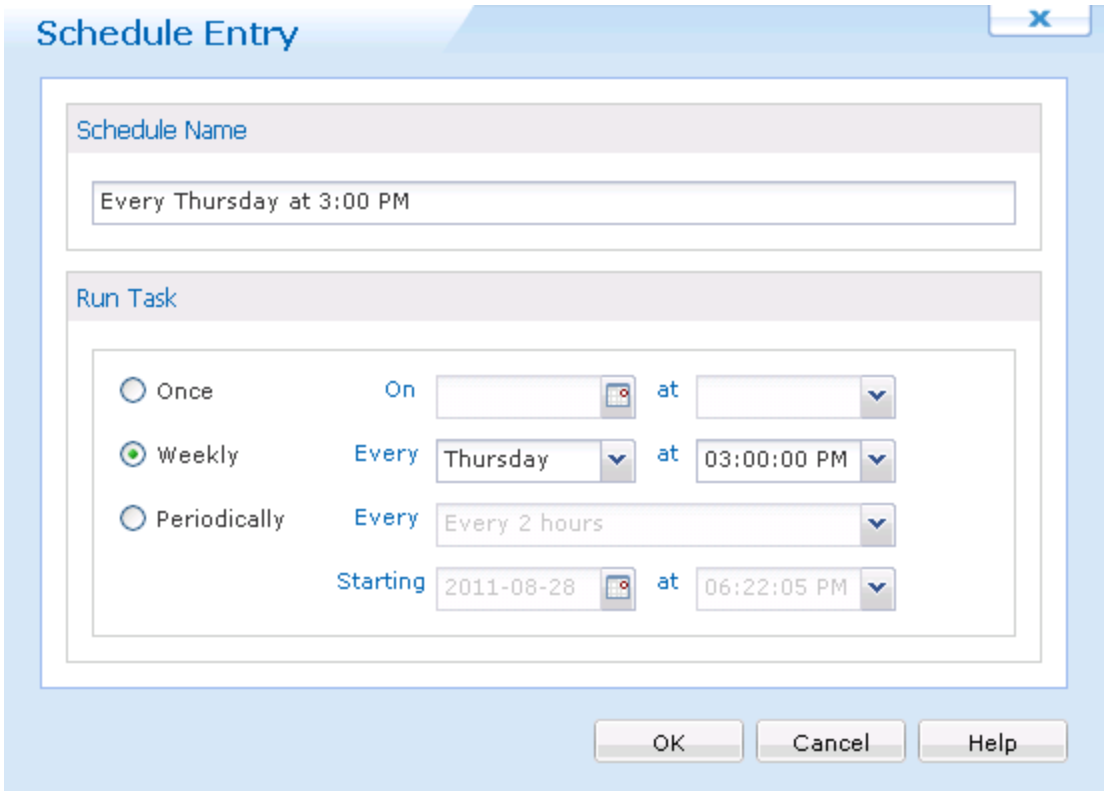
3. Select devices.

   Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



4. Configure data collection rule schedule and optional settings.




Schedule Entry
Schedule Name
Every Thursday at 3:00 PM
Run Task
Once
On
at
Weekly
Every
Thursday
at
03:00:00 PM
Periodically
Every
Every 2 hours
Starting
2011-08-28
at
06:22:05 PM
OK
Cancel
Help

Section Name	Description
Collection Schedule	This option enables you to create a custom data collection schedule with a custom date and time. Select the **New** button to create the new schedule. This will open up the second dialog box above. If you already have a previously created schedule, you can select edit to open the second dialog box above.
Schedule Name	Enter a meaningful schedule name that will be used to identify your custom schedule(s).
Run Task	Select the frequency for which you want to initiate the data collection on your device (s).
Delivery Schedule	This option will deliver the data collected from the device to the Deployment Serverbased upon the set update schedule. Currently, this option uses device schedule as the delivery schedule and is not configurable.

NOTE:

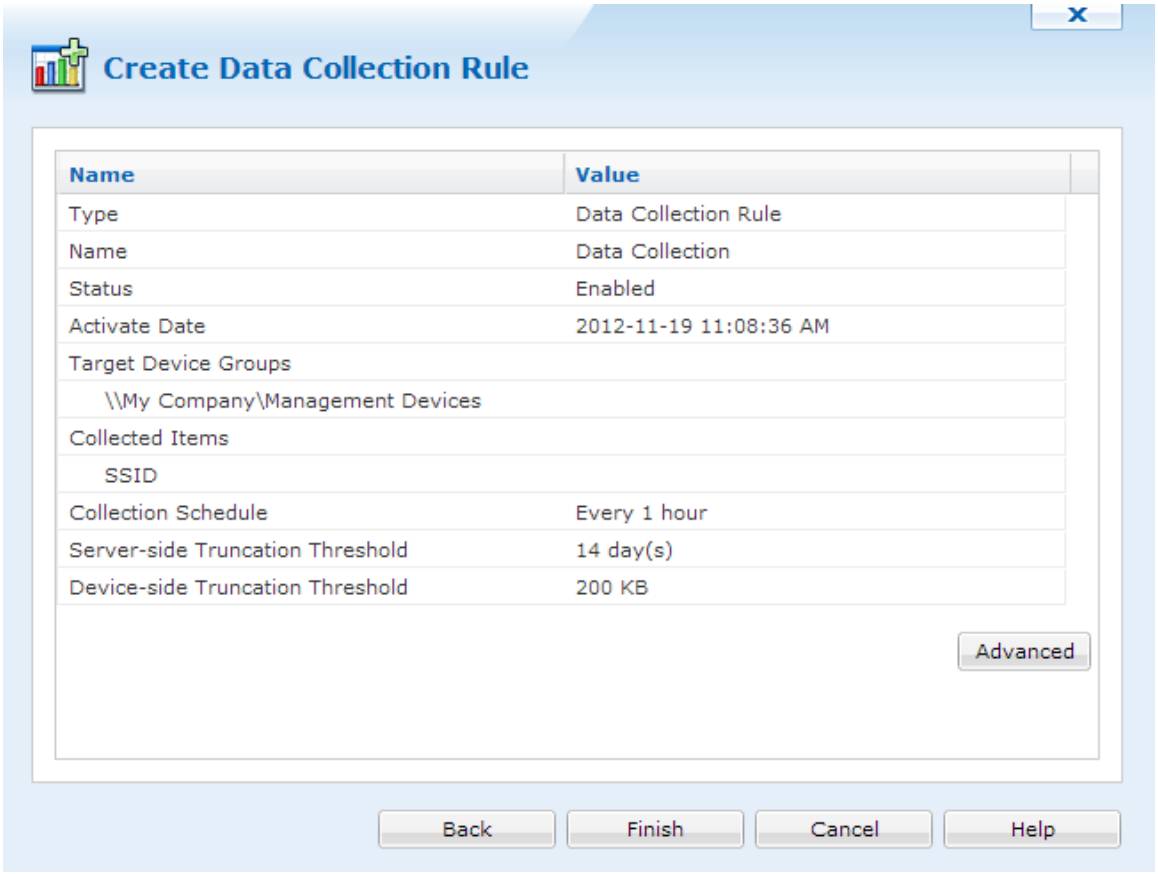
Creating a frequent collection schedule may affect the device's battery life. Also, frequent data collection can be managed with the truncation options available. This will help control how much data is kept on the device and in the database.

Choose the size of the data being collected. This helps control memory used on the device and the number of days you would like to retain the data in the database.

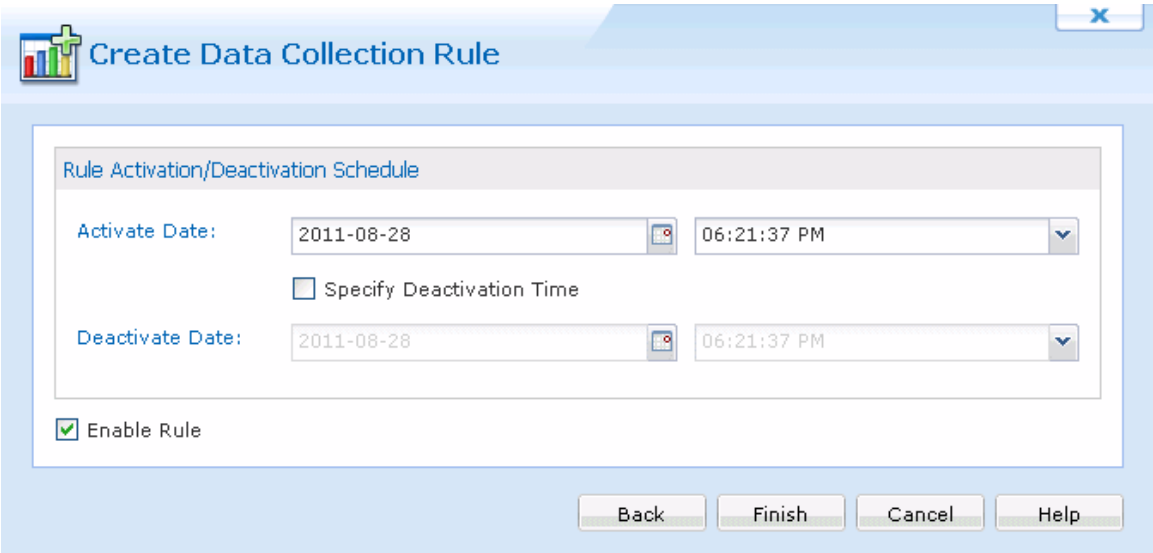
Section Name	Description
Device-Side Data Truncation	Specify the maximum size of data to be stored from the data collection ruleon the device(s).
Database Data Truncation	Specify the number of day(s) that you would like to retain the information in your database. Data collected older than the number of days listed will be deleted from the database

After entering your choice(s) in the above dialog box, click the **Next** button.

5. Review the summarized information.



By clicking on the Advanced button, the data collection rule Advanced window will appear. By default the rule will be activated immediately upon completion of the wizard. If you wish to delay the activation, you can modify the activate date. A deactivate date can optionally be entered to specify a date from which the rule will be disabled. A data collection rule can also be explicitly disabled by clearing the checkbox next to Enable Rule.



Section Name	Description
Activate Date	This option enables you to define a date and time when the rule will start collecting data from the selected devices
Deactivate Date	If the **Specify Deactivation time** box is checked, you can define the time at which you wish the data collection to stop.
Enable Rule	You can use this option to enable or disable the rule. This option is also available by right-clicking the rule.

The data collection rule can be deployed real-time or at a pre-set time. The data collection rule, although set to be activated at a scheduled time, can also be set to be deactivated. The deactivation setting is optional.

Click **Finish** to complete the wizard.

Android+ Alert Rules

Alert Rules allow Administrators to be notified when events of interest arise on the system. This notification system allows Administrators to quickly and effortlessly communicate an event message to large groups of people via email, and notifies users via the MobiControl Manager Alert tab. For every type of scenario, whether it is a Rule Change or a Device Error, the system will rapidly deliver your message to a designated audience.

NOTE:

The Deployment Server must be online in order for Alerts to be generated and sent out.

The MobiControl Web Console allows you to create Alerts based on the Devices Operating System (OS). Some Alerts are specific to the OS Tab that has been selected . For detailed information on the Alerts Available please see below.

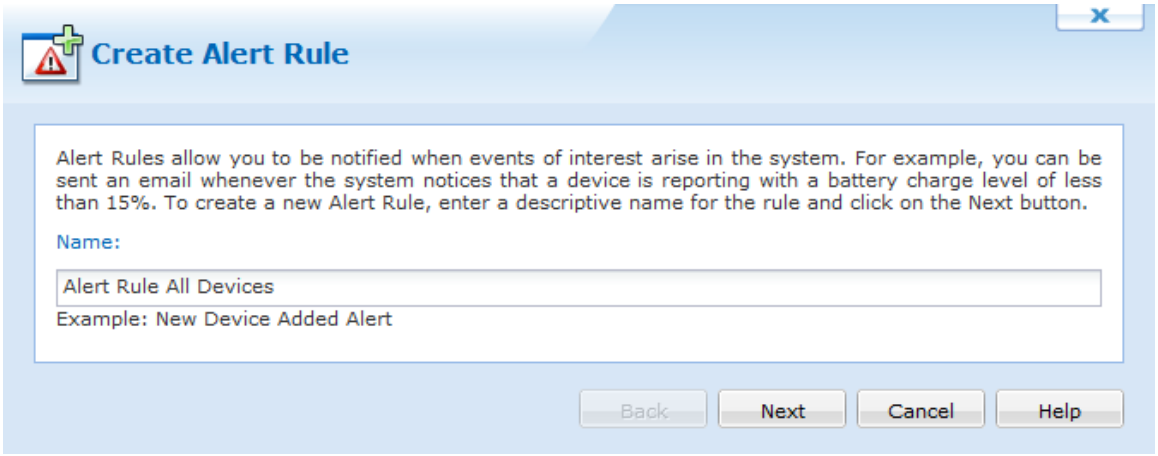
Type	Description
Device Event	Trigger alerts based on an assortment of device specific conditions.
Device Status and Custom Data	Trigger alerts based on Custom Data vales that you have configured.
Geofence Event	Trigger alerts based on devices entering or exiting geofenced areas.

The steps below describe how the Create Alert Rule Wizard can be used to create an Alert using the MobiControl Web Console:

1. Start the wizard.

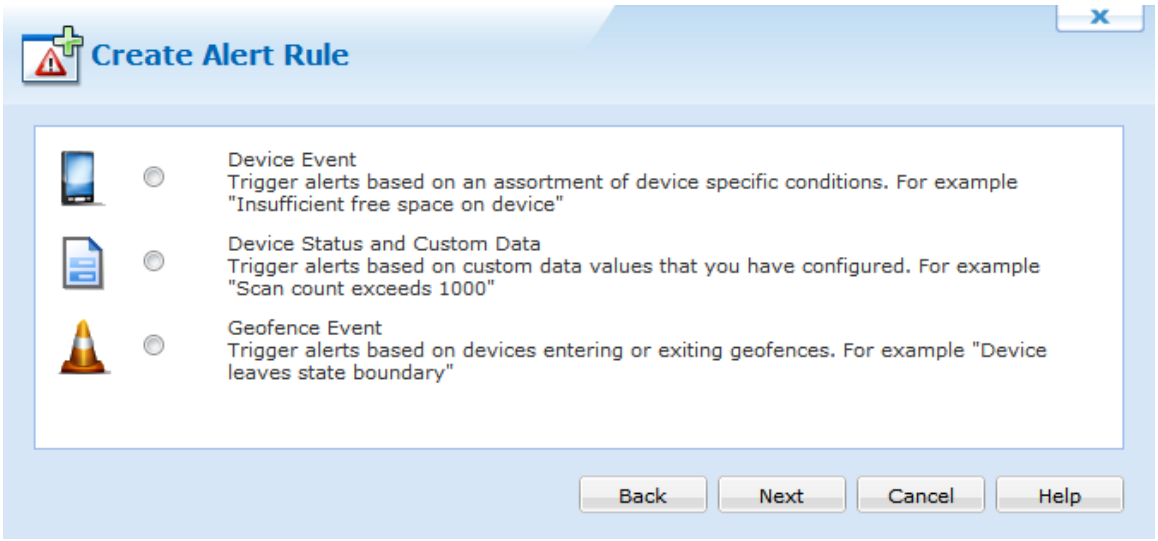
   Select the All OS's Tab, then select the Rules tab, then Right click on the **Alert Rule** folder, and select **Create Alert Rule**. The first page of the Create Alert Rule Wizard will be displayed.

   Enter a descriptive name for the Alert Rule you are creating and click **Next.**



First page of the Alert Rule Wizard

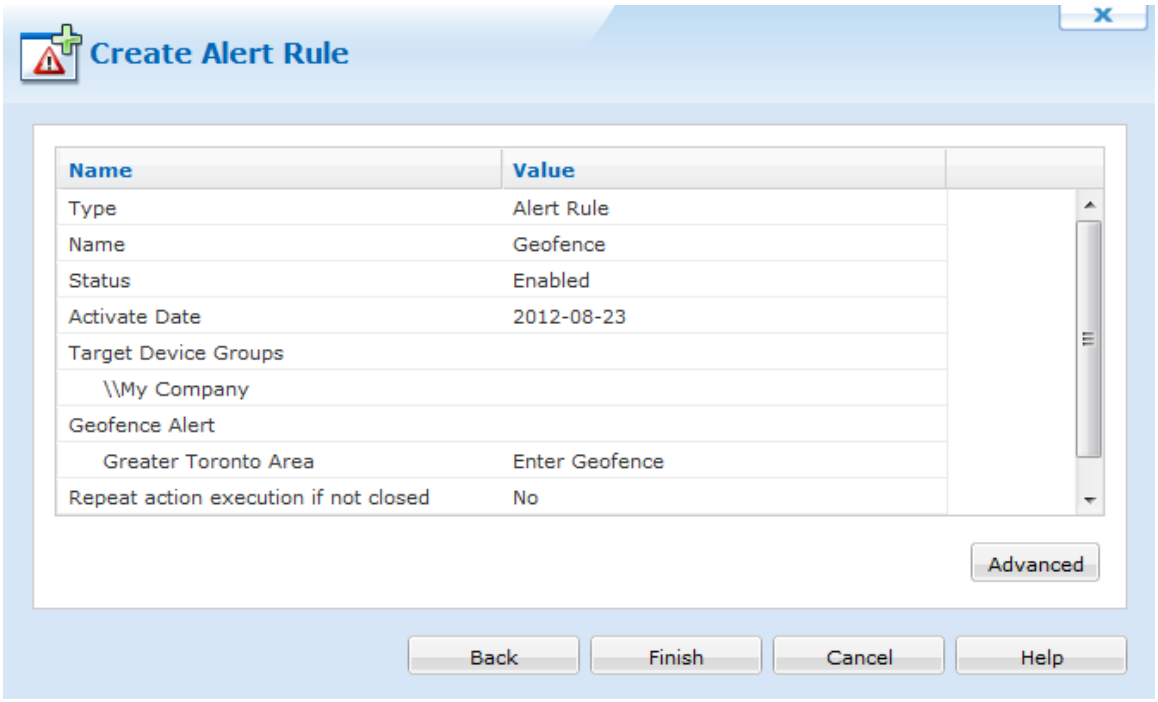
2. Select the Alert Rule Type.



Select the Alert Rule Type and click Next. After Clicking Next you will be asked to specify the Alert Options for the selected Alert Type. Select the type of alert below for more information on the Alert Options available.

Type	Description
Device Event	Trigger alerts based on an assortment of device specific conditions.
Device Status and Custom Data	Trigger alerts based on Custom Data vales that you have configured.
Geofence Event	Trigger alerts based on devices entering or exiting geofenced areas.

3. Review the summarized information.



Click **Finish** to complete the wizard.

Android+ Geofence Event

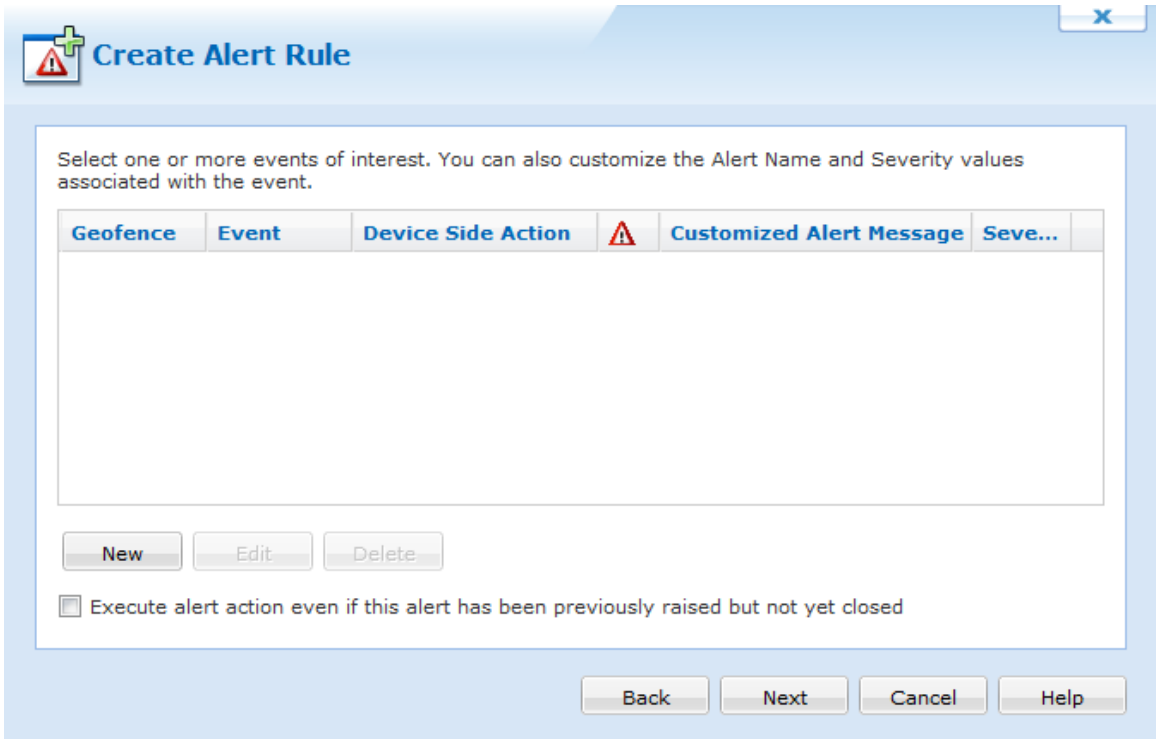
A Geofence Event is an alert trigger based on a GPS enabled device entering or leaving a Geofenced area defined by MobiControl administrators.

EXAMPLE:

If there are devices that should not leave a building complex, a geofence alert rule can be created to ensure that MobiControl administrators are alerted if these devices do leave the complex. Geofence areas can be as small as a house, or a big as a continent.

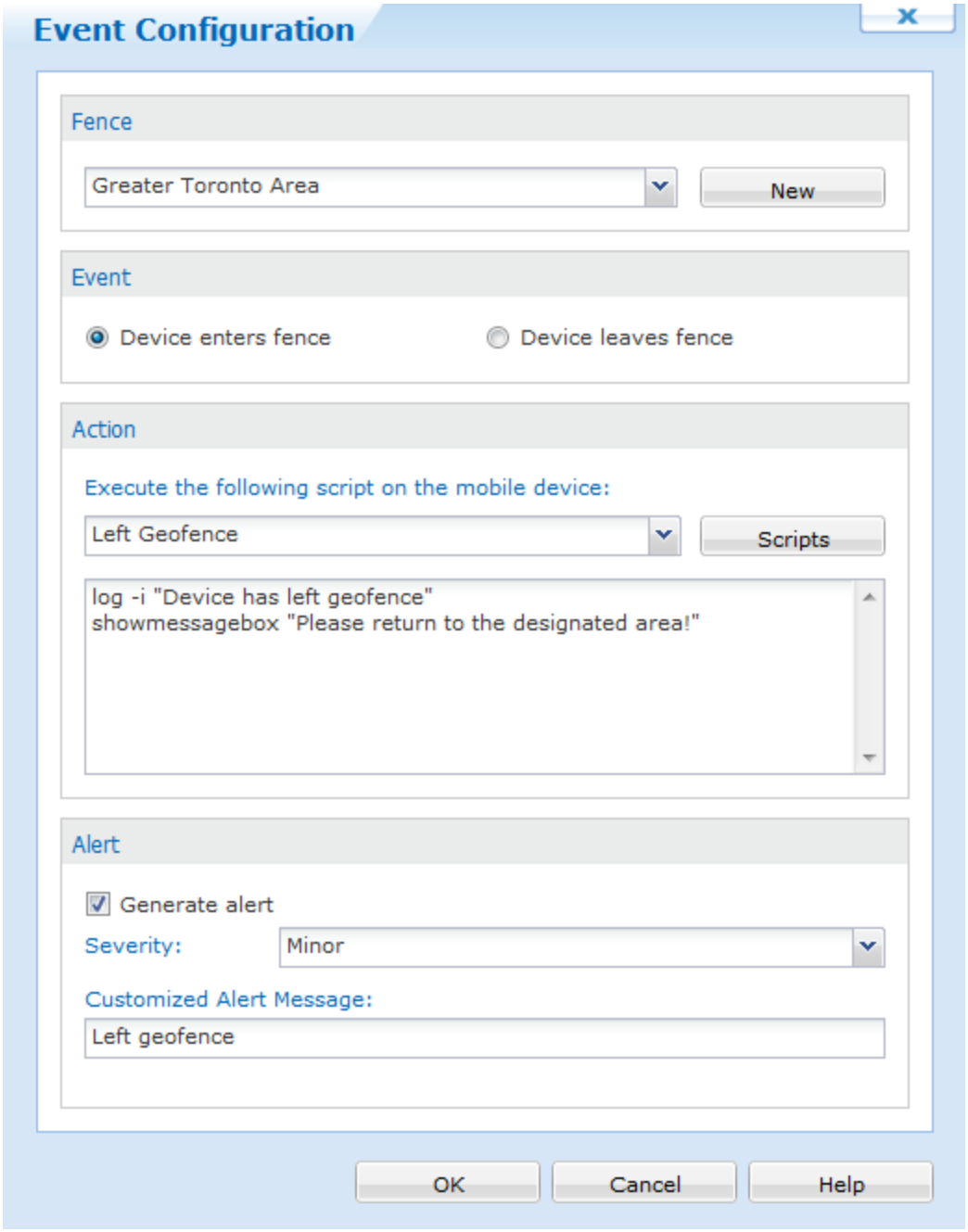
In order to create a Geofence event, an Alert Rule is needed with the Geofence Event type. Please see the "Android+ Alert Rules" topic on page 1434 for assistance with creating an alert rule.

After selecting the Geofence alert type, you will be presented with a window that has all previously created Geofences. If no Geofences have been created click the **New** button.



Geofences

Clicking new brings up the Event Configuration window. Here we can create a new geofence.



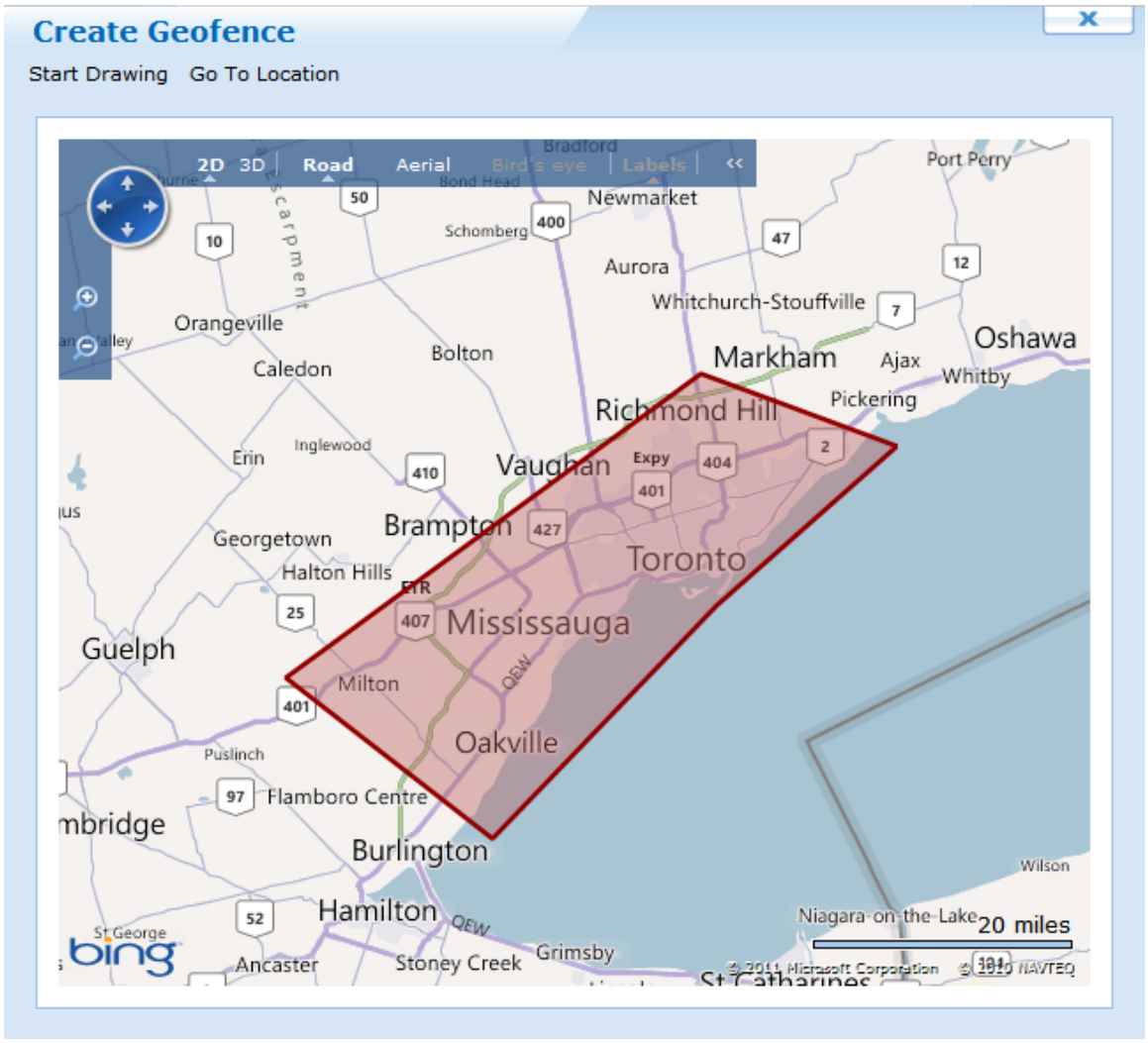
The **Fence** section allows you to create a geofence by clicking on the New button in the dialog box.

The **Event** section allows you to configure if this event should be triggered on entry or exit of a fence.

The **Action** section allows you to configure what script you want to run on the mobile device when the event is triggered. This is optional, but you have for example the ability to run an Activate Connection, Log Event, Show Message or even wipe the device completely.

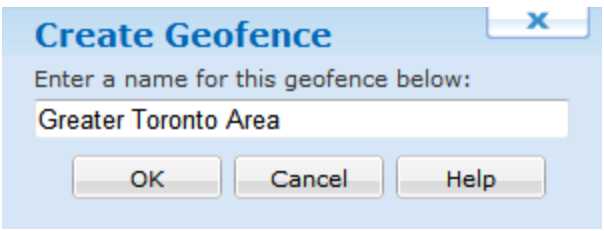
The **Alert** section allows you the option to Generate an alert, configuring its Severity (Minor, Serious and Critical) and add a Customized Alert Message, such as "Left geofence".

When you click on the **New** button in the **Fence** section, the following Geofence Creation dialog box appears:



The two options available are to Start Drawing and Go to Location.

The **Start Drawing** option allows you to begin drawing on the map below the button. The area drawn on the map will be defined as the Geofence. The defined area must be a complete geometric shape, which means the Start Drawing point will be the same as the End Drawing point. When you have completed a proper geometric shape you be asked to name your geofenced area.



Prior to selecting the Start Drawing button, you have the ability to use the view control buttons in the map in order to move to a desired location, zoom in and out, switch to 3D, Road, Aerial and Bird's eye views among the many options. This allows you ease to create an appropriate view for your geofence.

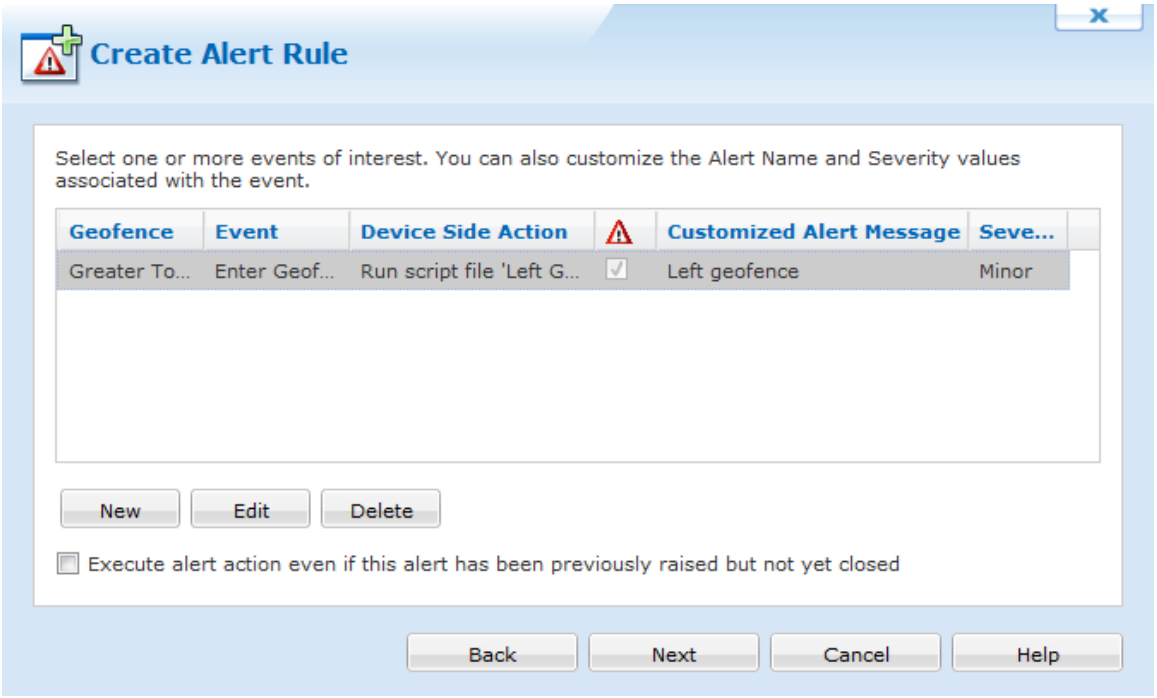
Alternatively to identify the appropriate view of the map, you can click on **Go to Location** which will allow you to specify a street address, location, landmark, or an existing geofence.

EXAMPLE:

- 350 Fifth Avenue, New York City
- Rome
- SFO (San Francisco International Airport)

Once you have the appropriate view displayed, you can click on Start Drawing and you are now able to create a fence. The first click of the mouse is first point of the fence. In order to complete the fence, you must have at least 3 distinct points selected on the map. In order to complete your fence, the last point must end off at the first point so it completes the closure of the fence. Once the last point is selected, a pop-up requesting the name of the geofence is shown. Here you should enter a meaningful name for that specific geofence in case you would like to use it again.

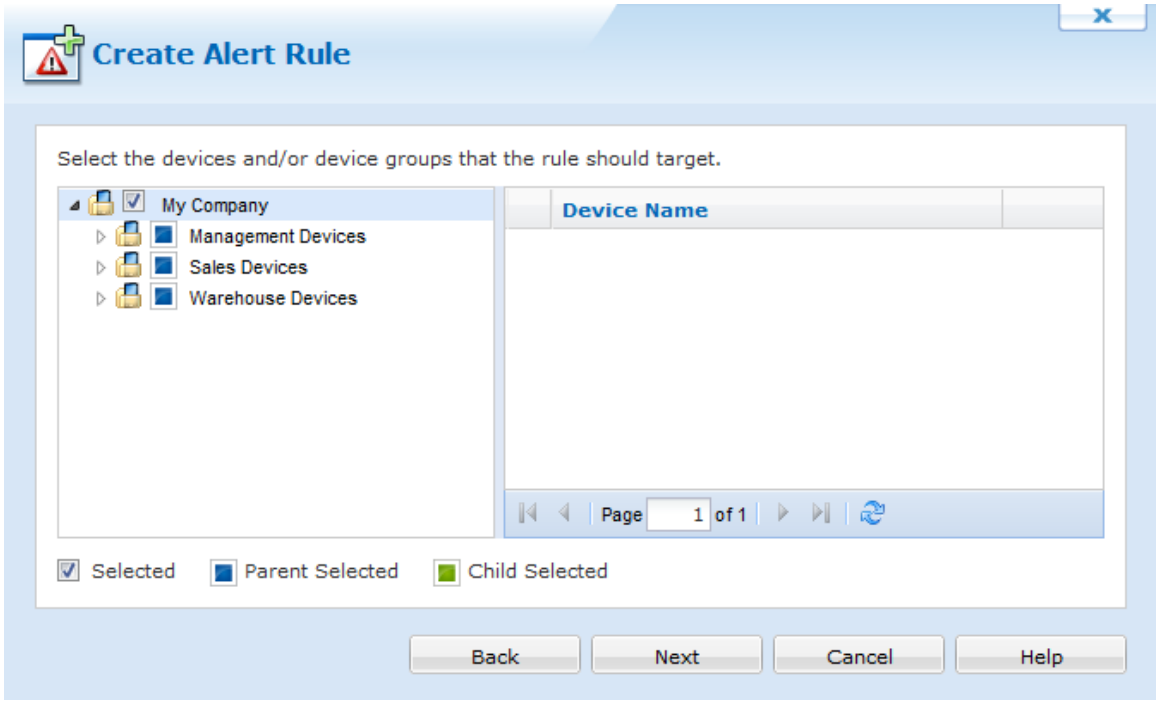
Select Geofence



Once the event is configured it will display as shown in the above diagram. Here you have the ability to create new events, edit existing events or delete events. Also, on this dialog box, there is a checkbox at the bottom allowing you to determine whether or not you want to Execute alert action even if this alert has been previously raised but not yet closed.

Select Devices

Select the devices to which the rule will be applied. Apply the rule to all devices in your device tree or simply individual group(s) and/or device(s). Once you have completed this section, click the **Next** button.



Select Power Policy

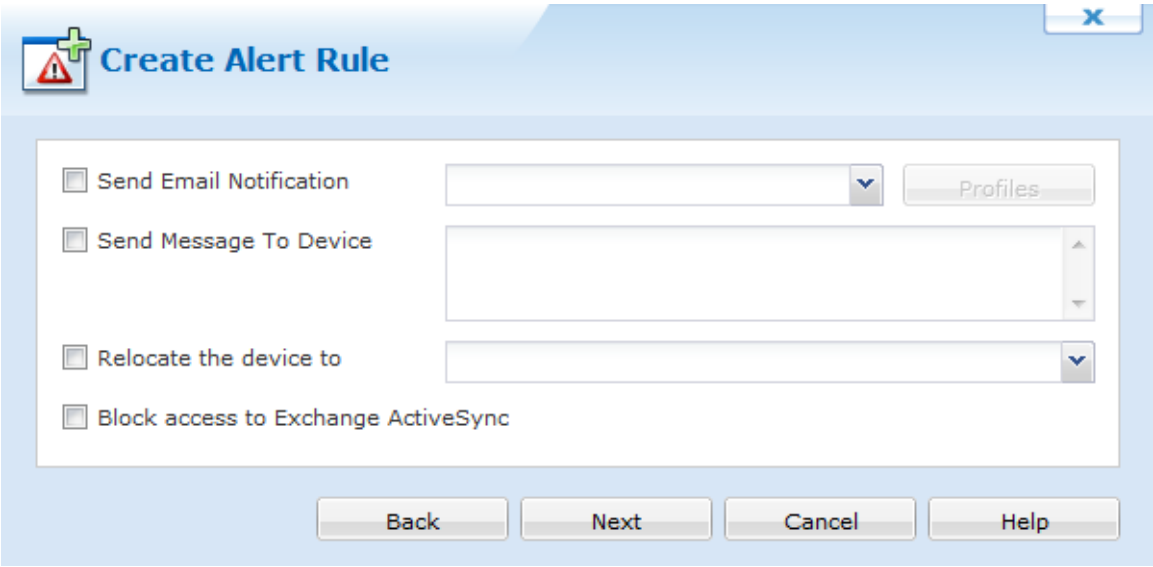
Clicking Next moves you to the Power Policy section as seen below.

The options available for the Power Policy are Continuous and Periodic.

Power Policy	Description
Continuous	This indicates the GPS radio is always on and the location will be monitored in real time. It is best to use this option with devices that have an external power source or are vehicle mounted because this option takes up a lot more power.
Periodic	This will turn on the radio based on a schedule that you define. Based on your business requirements, this can be as responsive as every 2 minutes, or every weekday all the way up to every year. It is best to use this option when you have battery powered devices in order to minimize the amount of power consumed with having this feature on.

Action Settings

Once the power policy is selected, you must select your an action to be done.



Select any action to be done when the Geofence alert has been triggered. MobiControl gives the option to send an email to administrator groups, send a message to the device, relocated the device to a different group, or block access to Exchange Active Sync. One or many of these options can be selected. After selecting your actions, click Next and continue the Alert Rule Wizard here.

Android+ Telecom Expense Management

The Telecom Expense alert rule allow MobiControl Administrators to monitor how much data and minutes a group of devices/individual devices use based on a company data plan. This rule allows Administrators to set a soft threshold along with a hard threshold. When data or voice minutes reach

either the soft or hard threshold, devices can automatically be relocated to another group and have either data or voice disabled. An email can also be generated and sent to a configured email address when a soft or hard threshold is reached.

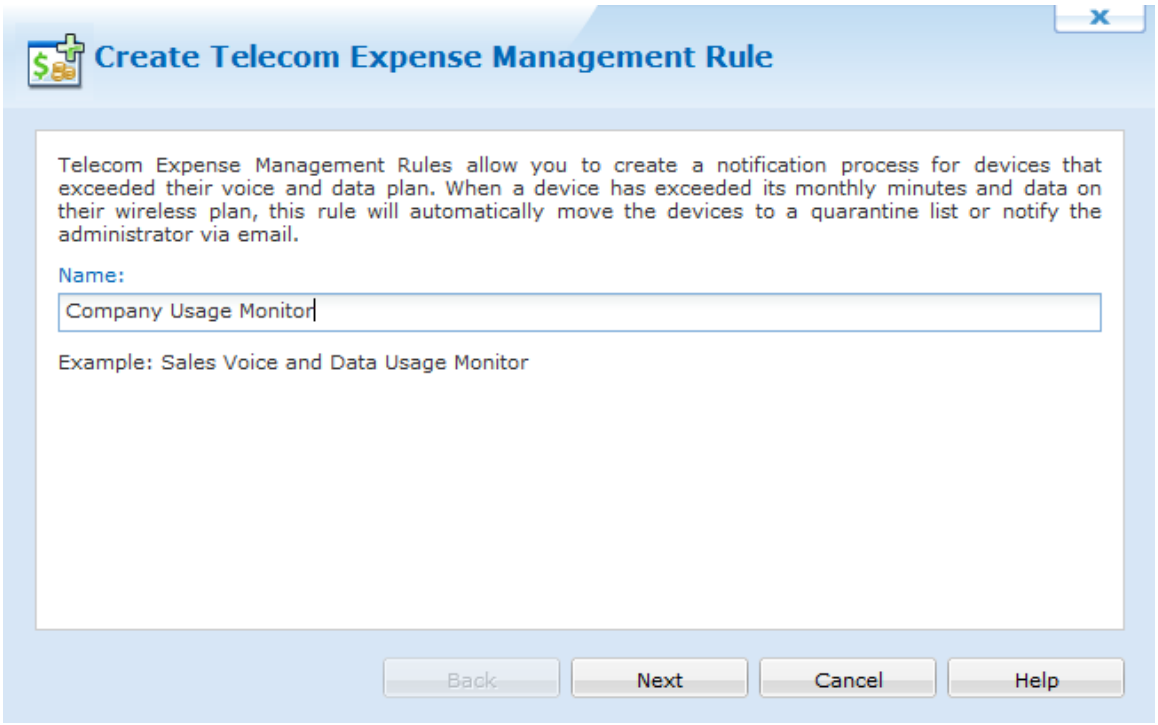
This allows enterprises to better manage company data and voice minutes.

The steps below describe how the Create Telecom Expense Management Wizard can be used to create an Telecom Expense Alert using the MobiControl Web Console:

1. Start the wizard.

   Select the Android+ Tab, then select the Rules tab. After, right click on the **Telecom Expense** folder, and select **Create Telecom Expense Management Rule**. The first page of the Create Telecom Expense Management Wizard will be displayed.

   Enter a descriptive name for the Telecom Expense rule and click **Next.**



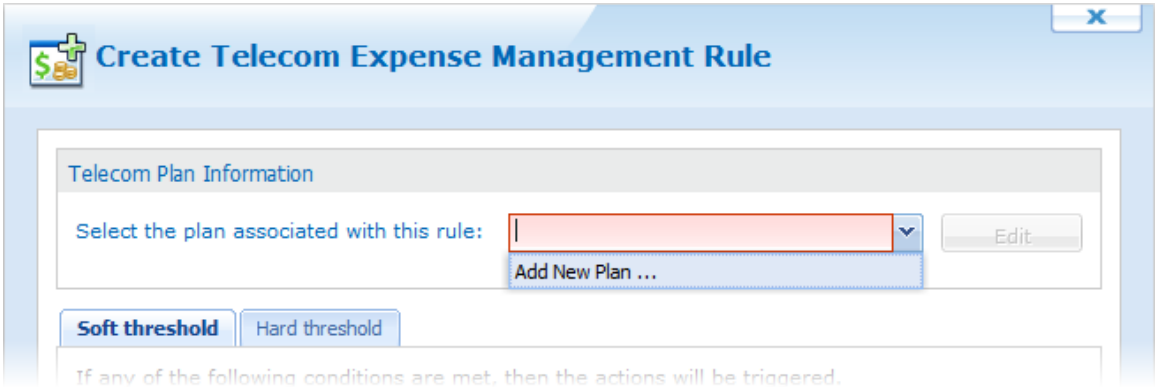
Enter a descriptive name for the Telecom Expense Rule

2. Select the target for the rule.

Here, we can select which group or device will be monitored with the Telecom Expense Management rule. Groups or devices that have ■ means that they are automatically selected because their parent group is selected. Groups that have ■ means that a child of that group is selected. Click **Next** to continue.

3. Telecom Expense Management configuration

On this screen, we are able to create a new data plan that will be associated with this rule, or choose an existing one. To create a new plan, choose the **Add New Plan** from the very top drop down menu.

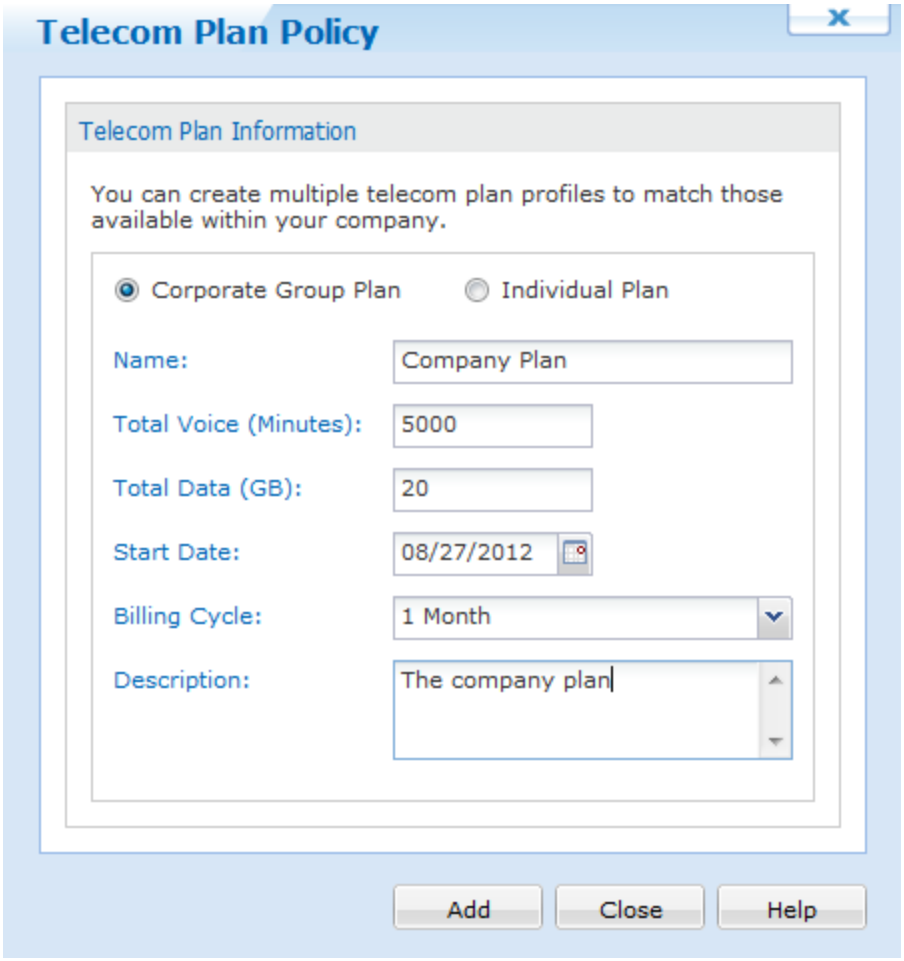


Adding a new Telecom plan

When **Add New Plan** is selected, the Telecom Plan Policy window is shown. Here we can choose whether this plan should be for a Corporate Group plan or an Individual Plan.

It is recommended that Corporate Group Plan is selected if the Telecom Expense Management rule is targeting a group of devices.

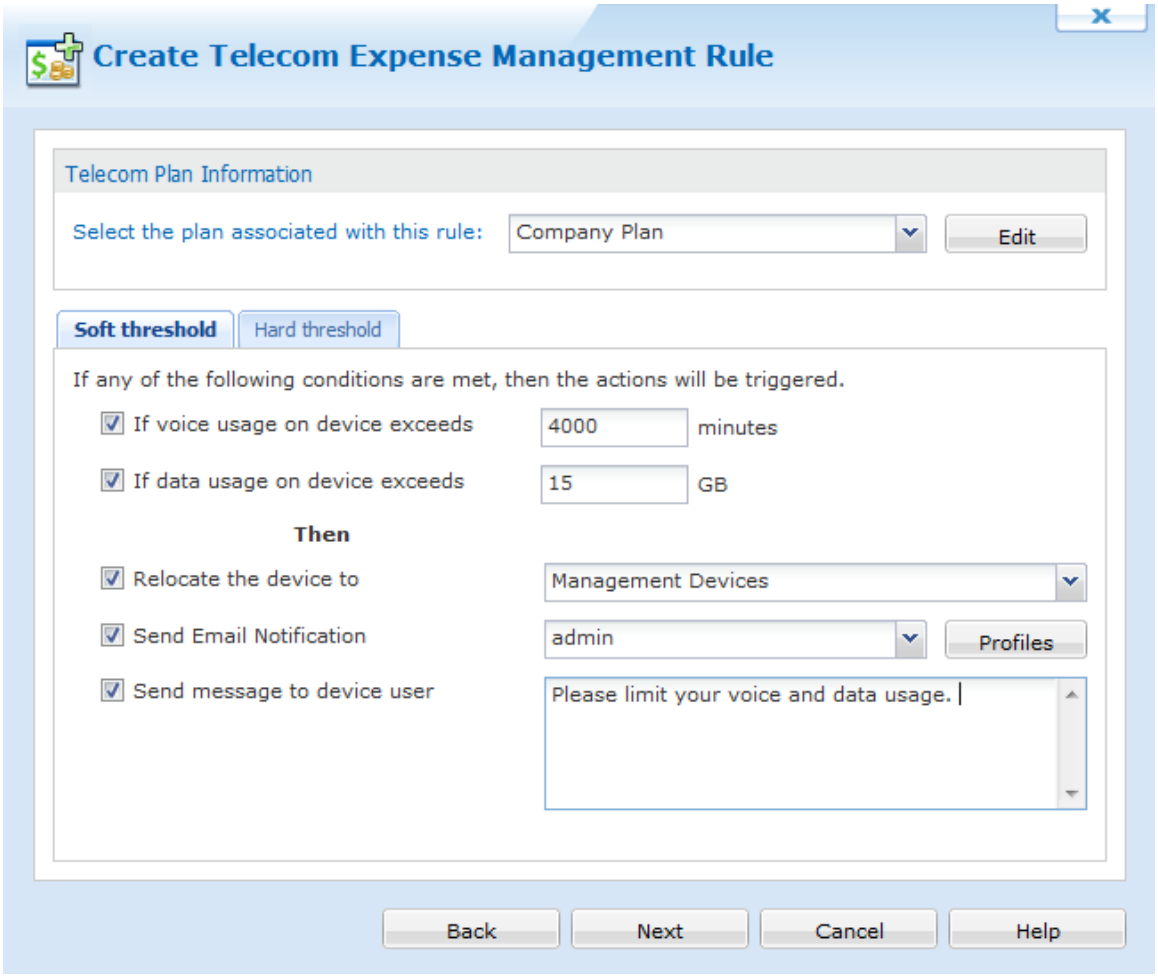
- A name and a billing cycle must be entered to add a plan.
- Voice is calculated in minutes, while data is calculated by gigabytes. If either of these are left blank, then unlimited is automatically listed.



Telecom Plan Policy

When a plan policy is created we can then configure the soft and hard threshold for the rule. Think of the soft threshold as a warning, and the hard threshold as critical. If the "voice usage on device exceeds" check box is selected, MobiControlwill check if a device or devices reach the number specified. The same rule applies for monitoring data usage. If any of the numbers are reached, MobiControl can then move the device to a new group, send an email notification, or send a message to the user.

After setting up the configurations here, click **Next**.



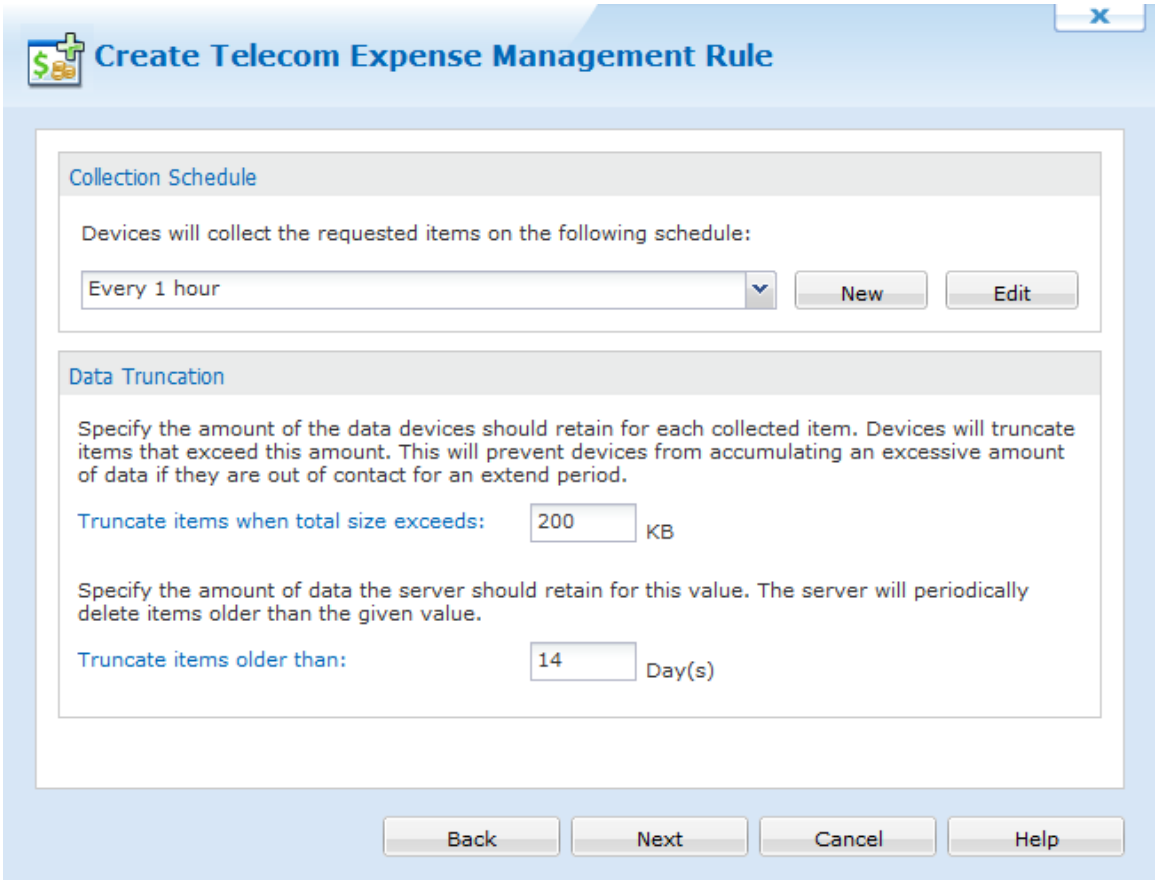
Telecom Expense configuration

4. Configure Data Collection and Optional Settings

Here, we can set how often the data is to be collected. Options include every 30 minutes, every hour, every two hours or daily. We also have the ability to create a custom collect schedule.

Data truncation specifies the amount of data that each device should retain. Any amount of collected data that goes above this number, will be truncated. This can be left as the default value.

After specifying the collection schedule and data truncation settings, click **Next**.

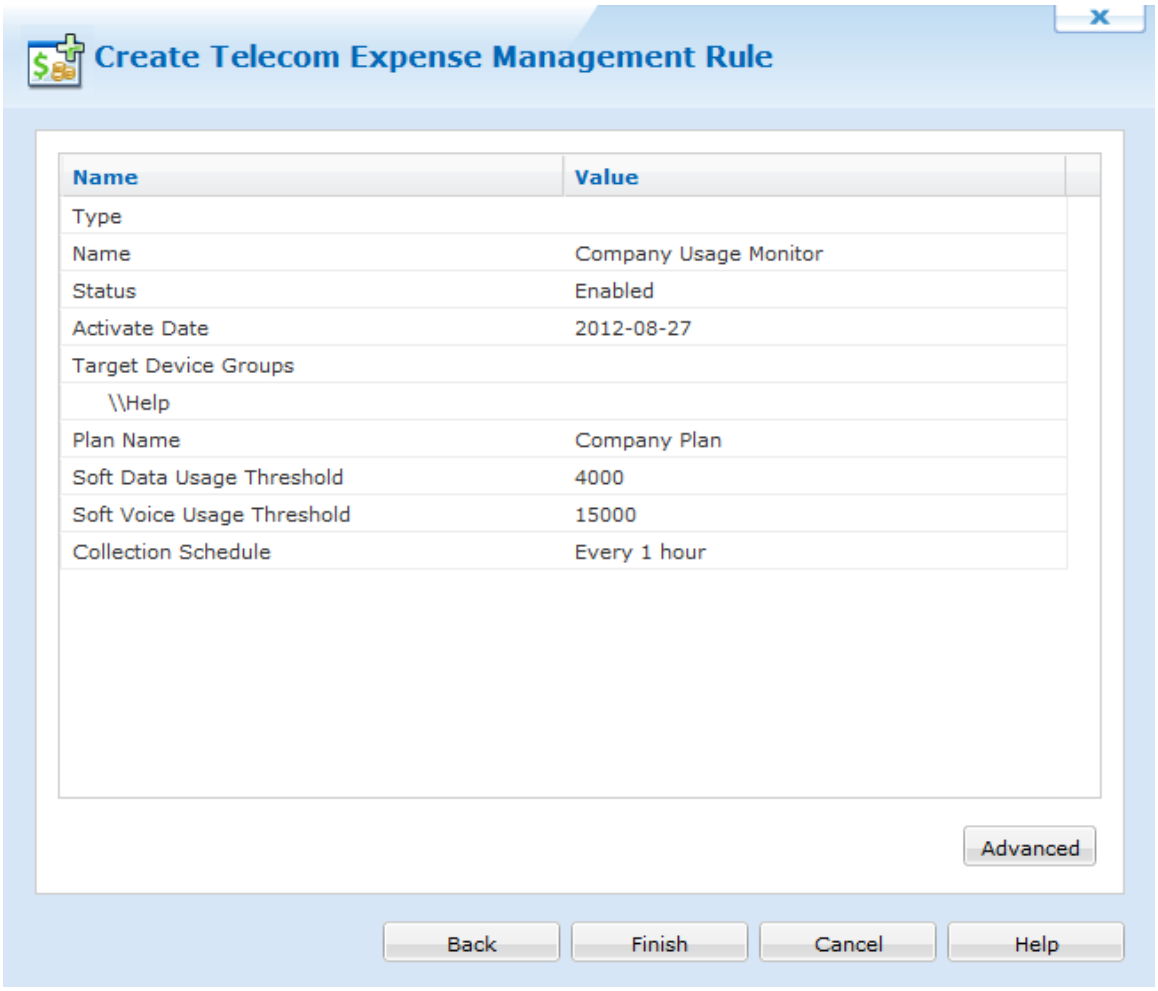


Data collection and optional settings

After specifying the collection schedule and data truncation settings, click **Next**.

5. Review the summarized information.

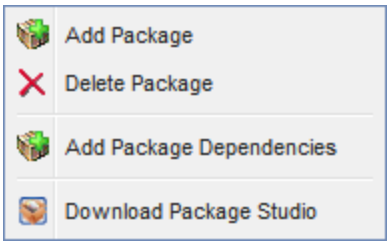
   The summary page will show all options and configurations that was specified in the previous steps. If something is needed to be changed, just click back and change the setting.



   Once everything is confirmed, click **Finish** to complete the wizard.

Packages Tab

The Packages view (tab) provides a list of the packages that have been imported into the MobiControl system, and the status of their distribution to the devices in the deployment. From this tab you can:



- Upload a Package
- Delete a Package
- Download Package Studio
- Create a Package Dependency

The left panel lists all of the packages that have been imported into the MobiControl system. Package are created using MobiControl Package Studio. Please see the "MobiControl Package Studio" topic on page 413 for more information.

If multiple versions of a package have been imported, each is listed with its own unique version number. The version number is set when creating or editing a package using MobiControl Package Studio.

Adding or Deleting a Package

To add a package to MobiControl, click **Package,** and then click **Add Package.**

To delete a package from MobiControl, select the version number node for the package, click **Package,** and then click **Delete.**

Download Package Studio

Package Studio must be downloaded in order to create packages. The Package Studio is typically installed with the thick client, but if you are using Web only then you can download Package Studio to work with on your desktop.

Package Dependencies

Package dependencies are a way to ensure the correct sequence of installation of packages on a device. To establish a package dependency, click **Package,** and then click **Add Package Dependencies.**

Panels in the Packages Tab

Info Panel

The Info panel provides detailed information about the package that is currently selected in the listing panel. Information includes the meta-data associated with the package that was specified when it was created, for example, processor, platform or OS version, and vendor information. Please see the "Create Package Project" topic on page 415 for a detailed explanation of these fields.

The content displayed in this panel is stored in the MobiControl database. You can select **Refresh** or press F5 on this tab to retrieve updated information from the database.

Devices Panel

The Devices panel lists the devices that have the selected package installed, or marked as pending for installation/uninstallation.

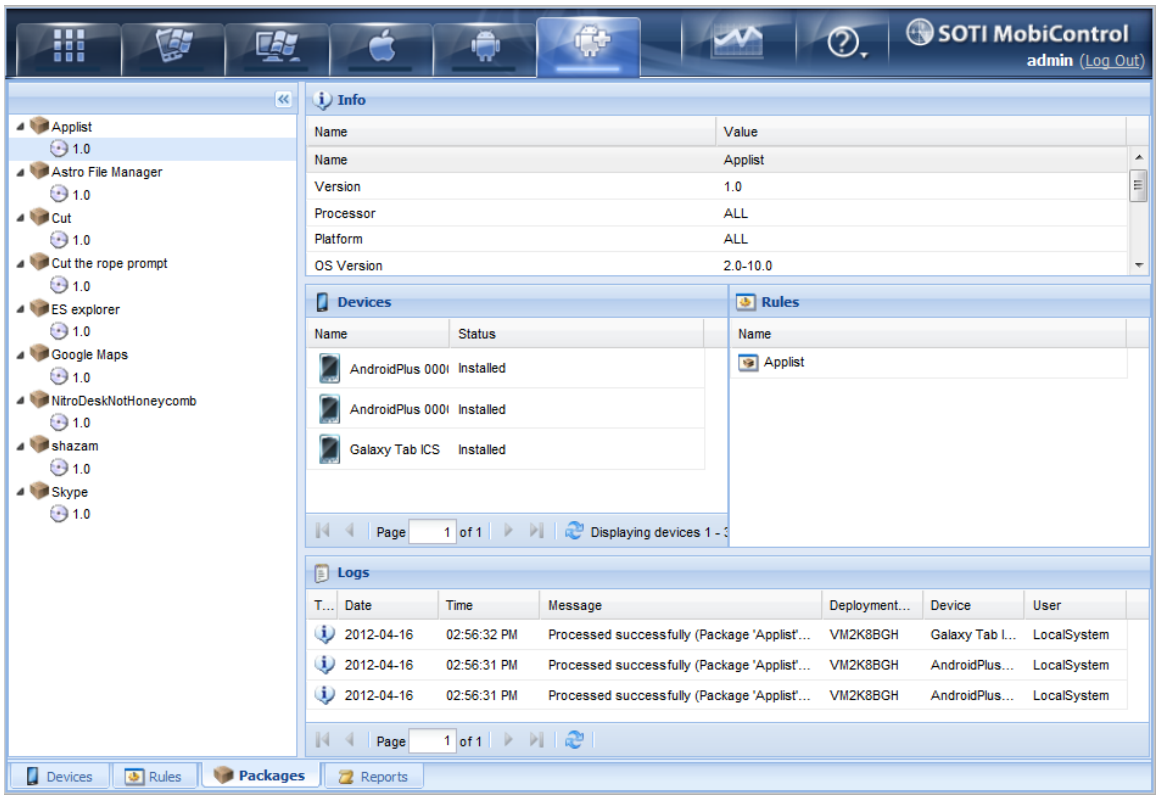
Rules Panel

The Rules panel lists the deployment rules that are configured to deploy the selected package.

Logs Panel

The Logs panel lists events occurring in the MobiControl system. This listing is filtered based on the package that is selected in the package listing.

You have the option to enable or disable logging, as well as adjust the maximum number of logs displayed and frequency with which the Manager should refresh the log panel.

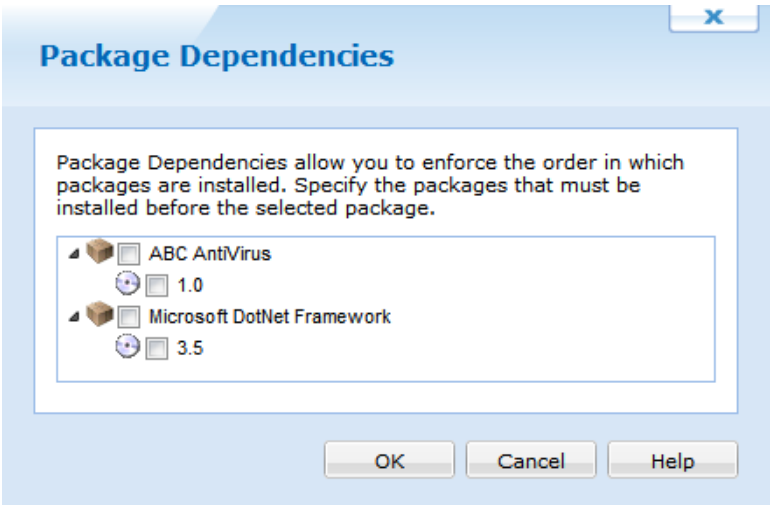


MobiControlPackages Tab Packages view (tab)

Package Dependencies

Package dependencies provide a mechanism to enforce the order in which packages are installed on a device.

To display the **Package Dependencies** dialog box, right-click on the package and select **Add Package Dependencies** from the pop-up menu. The **Package Dependencies** dialog box lists the configured dependencies.



Package Dependencies dialog box

Adding Package Dependencies

To add a package dependency, select the package(s) and version(s) upon which the target package is dependent.

EXAMPLE:

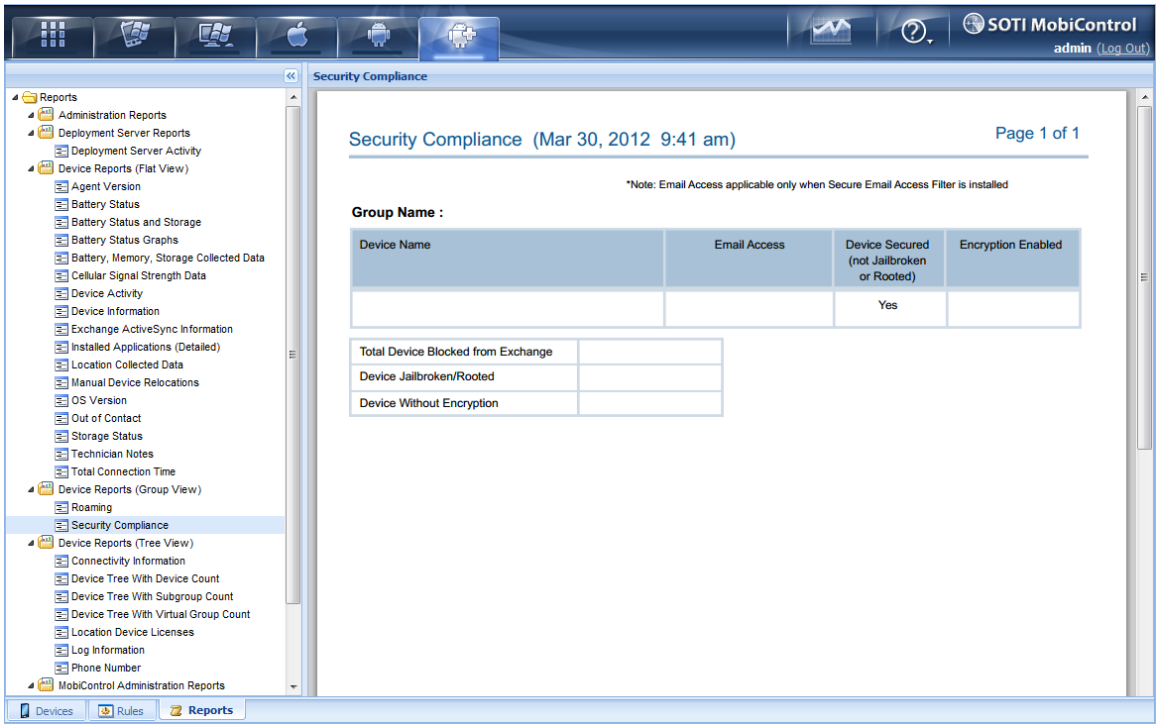
Packages A and B need to be installed, but it is mandatory that A is installed before B. Configure a dependency for package B: when editing the package dependencies for package B, select package A.

NOTE:

If a package depends on another package that is scheduled to install at a later time, then the Deployment Server will not push the package unless it is also scheduled to install at the same time or later. Please see the "Windows Desktop Package Deployment" topic on page 897 for more information about installation schedules.

Android+ Reports Tab

MobiControl includes an advanced reporting engine—Crystal Reports—that gives detailed information about all aspects of system operation. The product includes a set of canned reports that provide information about key areas of system operation. Reports can also be customized as well as new reports can be created and added to the system as needed.



MobiControl Manager Reports view (tab)

The MobiControl Web Console allows you to generate Reports based on the Devices Operating System (OS). Some Reports are specific to the OS Tab that has been selected. For detailed information on the Reports available please see the specific Reports that can be created below:

Report Types

The following reports are included with MobiControl:

- A **deployment server activity report** is a detailed report for deployment server activity over a specified time period.
- A **deployment rule report** is a detailed report of deployment rules and all devices.
- A **Battery and Storage Report** is a detailed report of the battery and storage of the selected devices.
- A **Cellular Signal Strength Data Report** is a detailed report of the cellular signal strength of the selected devices.
- A **deployment rule summary report** is about deployment rule exceptions, showing how many devices have executed the rule successfully, are pending, or have encountered an error.
- A **Deployment Server activity report** is a detailed report of Deployment Server activity over a specified time period.
- A **device activity report** provides information about the device activity during a specific time period.
- A **device custom data report** provides information about devices with the custom data values of selected custom data fields.
- A **device note report** provides information about the notes for your devices.
- A **device package report** provides information about packages installed on your device.
- A **device program report** provides information about all the programs installed on your devices.
- A **device relocation rule report** provides information about all the relocation rules for your devices.
- An **out of contact devices report** provides information about devices that have not connected to the system since the specified date.
- A **package deployment report** provides information about package deployment.
- A **Location Collected Data Report** is a detailed report of the location data collected for the devices.
- A **Connectivity Information Report** is a detailed report regarding device's connectivity.
- A **Device Tree Report** provides information about the device tree structure.
- A **Device Tree with Virtual Groups Report** provides information about the device tree structure along with the virtual groups.
- A **Log Information Report** provides information about the device logs.
- A **Phone Number Report** provides information about the phone number of devices.
- A **Alert Summary Report** provides summary of the alerts.
- A **deployment rule report** is a detailed report of deployment rules and all devices.
- A **Geofence Report** provides detailed report based on the Geofence.
- A **Uninstalled Mandatory Applications Report** provides information about the mandatory application not installed on the devices.
- And many more.
- A **Roaming** and **Security Compliance** report has been added to cater to the Android+ devices allowing the administrator to see how often the devices are roaming and if their security has been violated (ie Rooted).

Generating a Report

1. In MobiControl Manager, select the Reports view (tab).
2. Select a report in the left pane of the Reports view (tab).
3. Click the **Generate Report** button.
4. For some reports, a window will appear requesting additional parameters (e.g. time period) that may be required.

Saving a Report

1. Generate a report.
2. On the report screen, click the **Export Report** button. (It is the first icon in the toolbar, beside the **Print Report** button.)
3. Select the desired file type. Available file types are:
    - Adobe PDF (`.pdf`)
    - Crystal Reports (`.rpt`)
    - HTML 3.2/4.0 (`.html`)
    - MS Excel 97-2000 (`.xls`) or Data only (`.xls`)
    - MS Word editable RTF (`.rtf`)
    - ODBC
    - Record-style (columns of values with or without spaces) (`.rec`)
    - Report definition (`.txt`)
    - Rich text format (`.rtf`)
    - Comma-separated values (`.csv`)
    - Tab-separated text (`.ttx`)
    - Text (`.txt`)
    - XML (`.xml`).
4. Select the location to which you want to export the report. The options available are:
    - Application
    - Disk file
    - Exchange folder
    - Lotus Domino
    - Lotus Domino Mail
    - MAPI (Messaging Application Programming Interface)

Printing a Report

1. Generate a report.
2. On the report screen, click the **Print Report** button. (It is the second icon in the toolbar, beside the **Export Report** button.)
3. The print menu will pop up. Select the desired printer and the report will be printed there.

Generating Custom Reports

It is possible to create custom report files on any available statistic you desire. The Deployment Server database is a standard SQL database and can be queried by writing a custom query. Also, it is possible to create additional reports that are built into MobiControl. For more details, please contact us.

Other Tools

These other tools are available through the toolbar:

- The **Stop Loading** button stops the report generation process
- **Refresh** regenerates the report. If parameters were required to generate the original report (e.g. time period), a window will appear requesting the additional parameters
- The **Search Text** button searches the body of the report for a specified text string
- The **View Zoom** field allows the user to select view magnification, page width, and whole page views

Secure Content Library

The MobiControl Secure Content Library allows users to upload files through the web console so that it can be distributed to devices.

With the Secure Content Library we are able to specify file properties when it is uploaded. These properties can range from delivery methods to expiry dates.

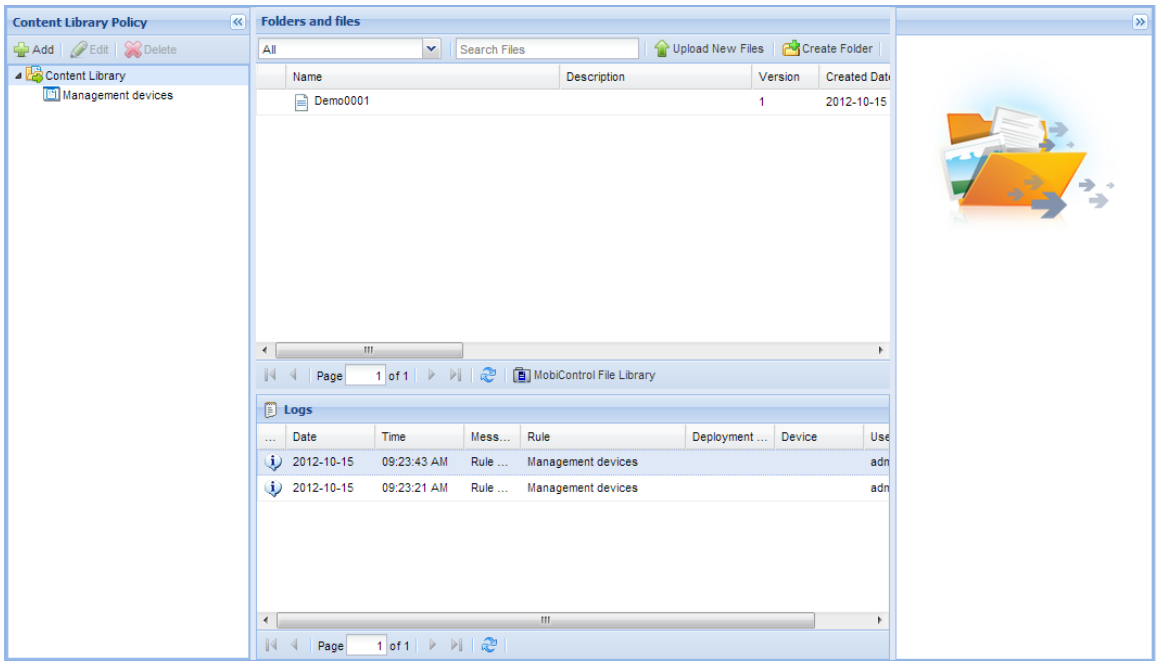
NOTE:

The Secure Content Library is only available for iOS and Android devices.

NOTE:

If the file sync rule is enabled for iOS devices, all those files will appear in the same panel as Content Library files. Files sent by the file sync rule cannot be configured by Content Library settings.

To go to the Secure Content Library, click the Content Library tab at the bottom of the device tab.



Secure Content Library

There are 4 main panels in the Secure Content Library. Starting clockwise, there is the Content Library Policy, Folders and Files, Deployment status, and logs. The Content Library Policy allows us to select which devices get files. Folders and files panel allows us to upload new files and create new folders. The deployment status shows us how many devices downloaded files, and the logs panel shows the logs related to the Secure Content Library.

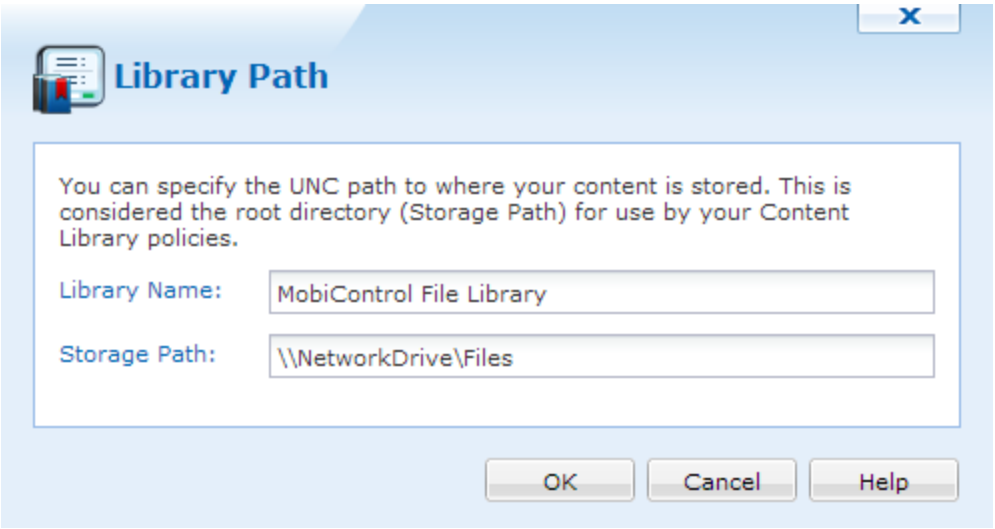
Library Path

When we first open the Secure Content Library tab, we will be prompted with a dialog asking us to name the Content Library and where to store the files.

The Storage Path could be anywhere the deployment has access to. Be it a shared folder on the network, or a folder on the hard drive. All files uploaded will be placed here.

NOTE:

The recommended Storage Path should be a network drive where both the Deployment Service and Management Service have access to.



Library Path

NOTE:

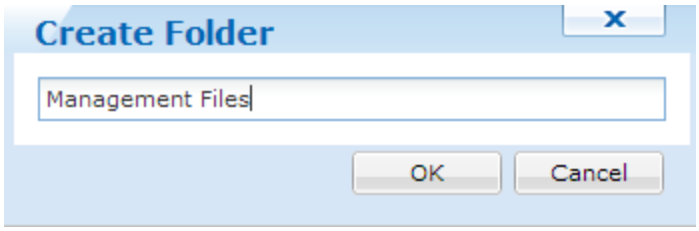
We can change the Library Path at any time. To do this, click the icon at the bottom of the Folders and files panel.

Folders and Files

After choosing the Library name and the Storage Path we are ready to create our folders and upload our first files.

Creating Folders offers a way to organize files. If a folder is wanted to be created, click Create Folder.

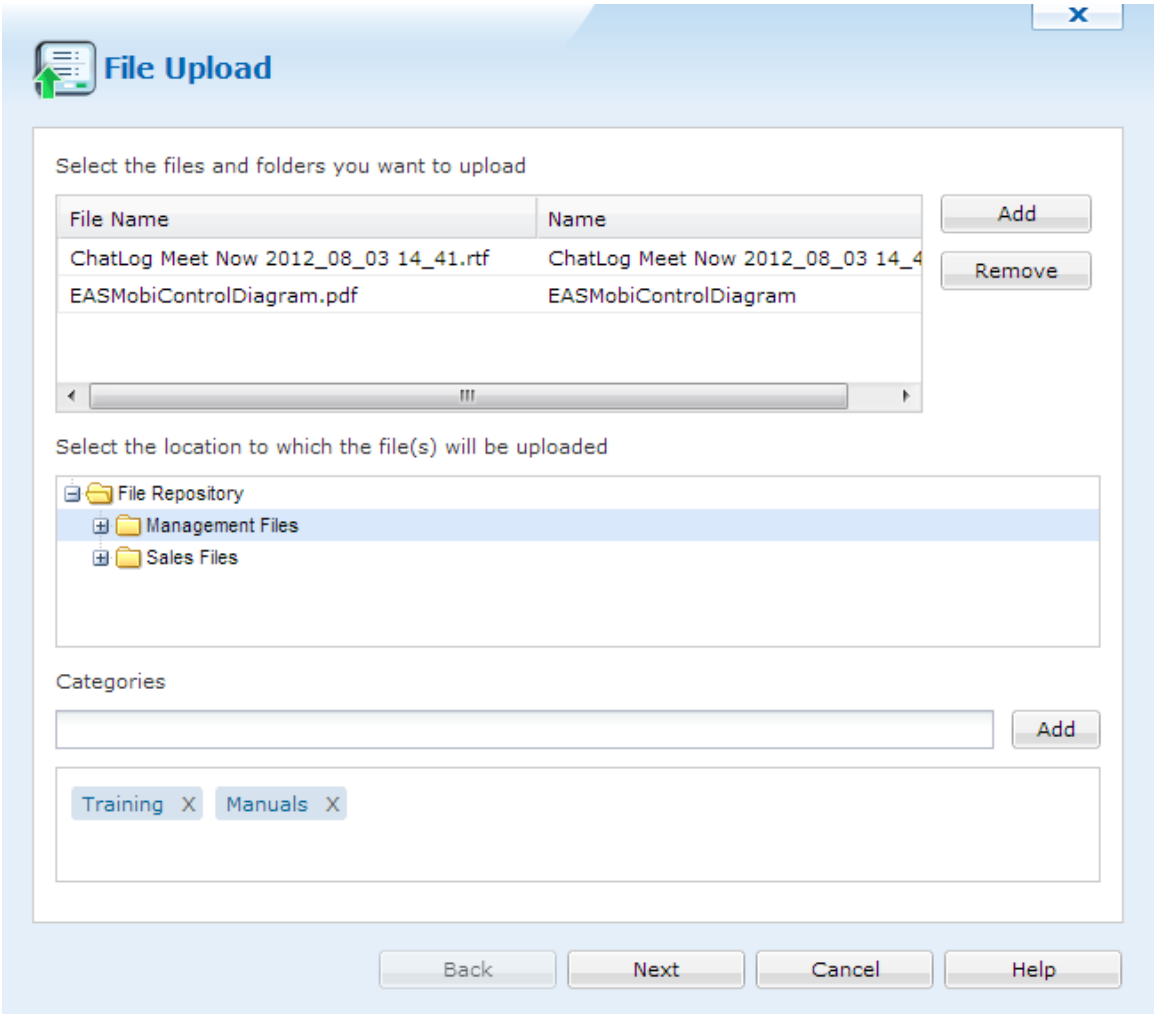
When the Create Folder dialog appears, enter a name and click OK.



Create Folder dialog

File Upload

After creating any folders needed, we can now upload files. To do this, click Upload New Files .



File Upload

Click the Add button to select a file and upload it. We can upload multiple files from here. If a file isn't needed, select it and then click Remove.

After uploading the files, we can select where these files will be placed in the Secure Content Library. File Repository is the root directory, then listing all folders that were created.

When a folder is chosen, we can add categories to these files. Categories are special tags that label each of the files. If we categorize these files for training, we can filter them based on these tags.

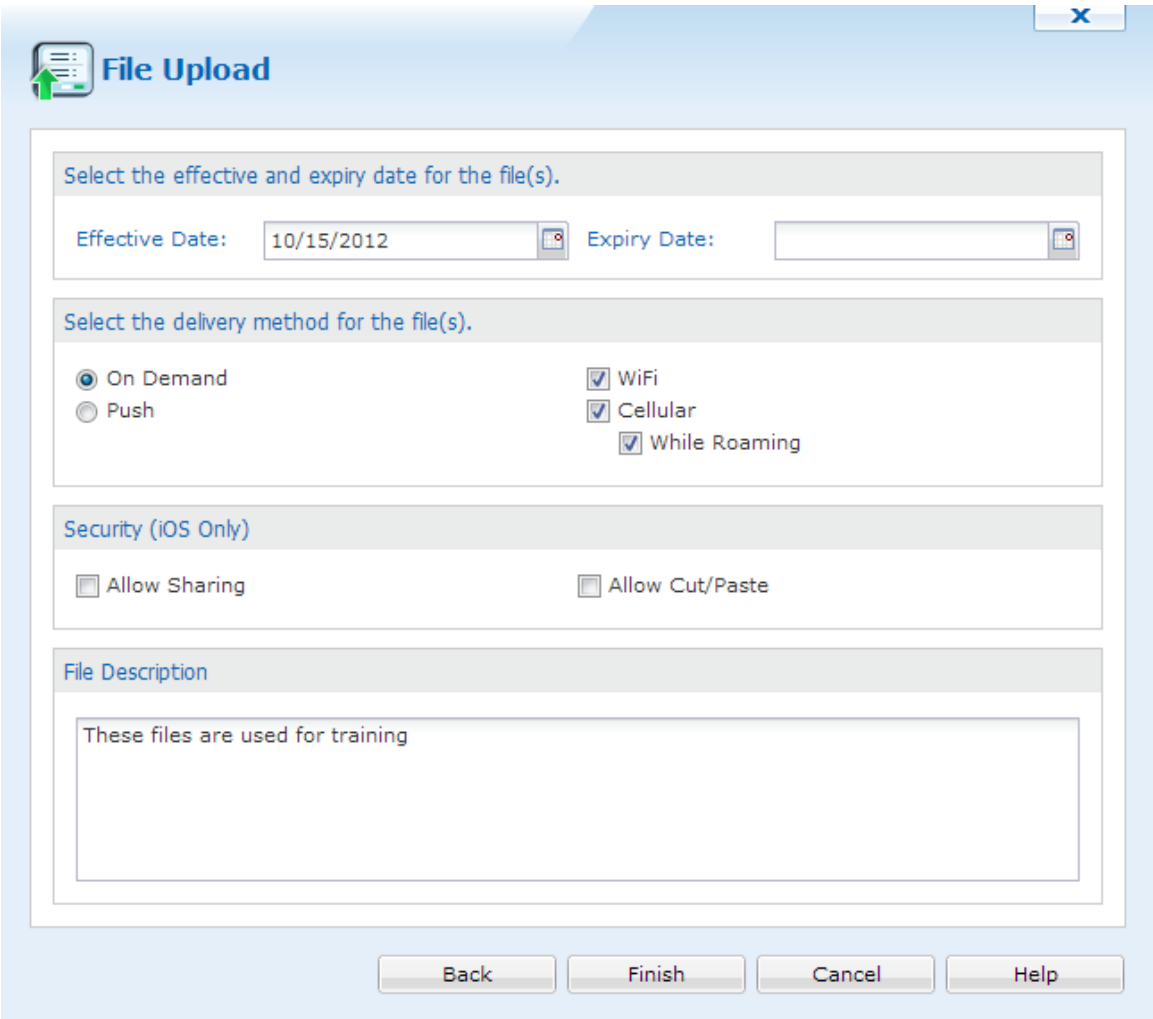
To add a category, just type it into the text field. If categories were created before, MobiControl will find them and we will be able to select them. If a category wasn't created, click Add to create this category.

When everything is configured and set, we can click Next to go to the next page.

File Upload Properties

This panel will allow us to modify the properties of the uploaded files.

We can select the dates the files are effective for, the delivery method, security and description.



File Upload Properties

NOTE:

If the Expiry Date is not needed, please do not click the field. This will ensure that the files will never expire.

If we select On Demand as the delivery method, then files will not be automatically pushed to the devices. Selecting Push will allow the files to be automatically downloaded to the devices.

We can also restrict the way the files are downloaded.

iOS devices offer additional security where these files cannot be shared or cut and pasted.

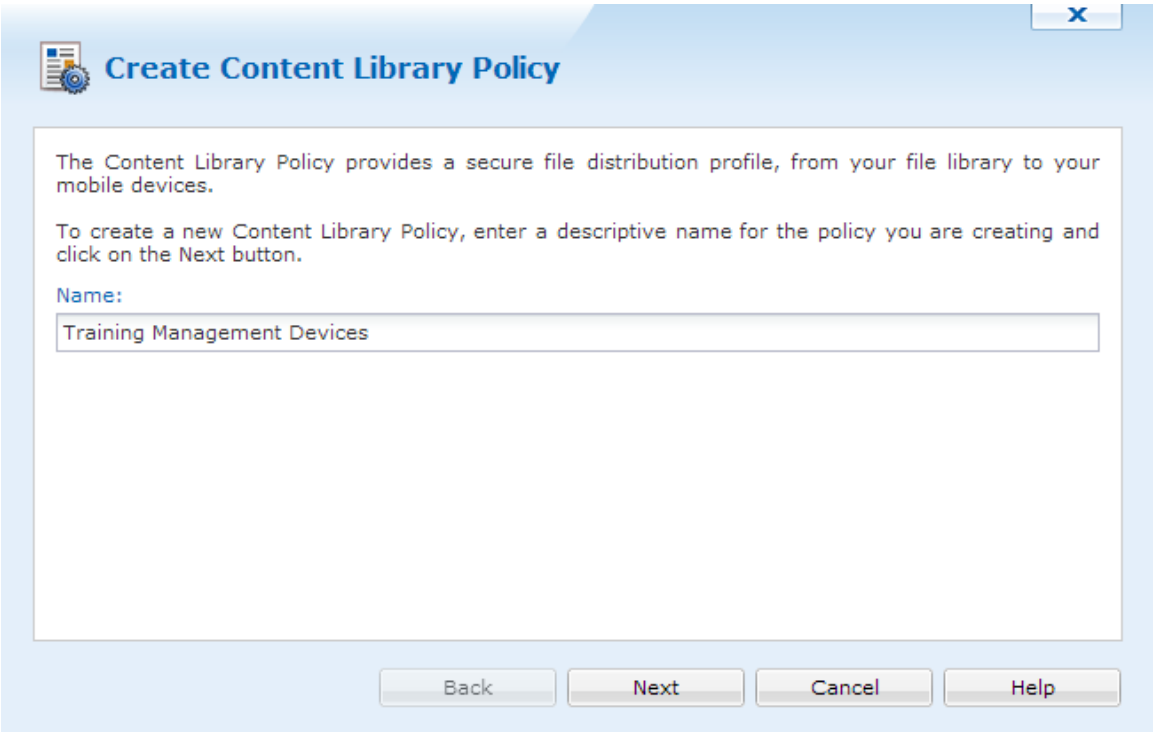
After all properties have been set, click Finish. The files are now uploaded to the MobiControlDeployment Server.

Content Library Policy

The Content Library Policy provides a secure file distribution profile, from the file library to mobile devices.. We can create as many policies as needed. To create a new Content Library Policy, click Add.

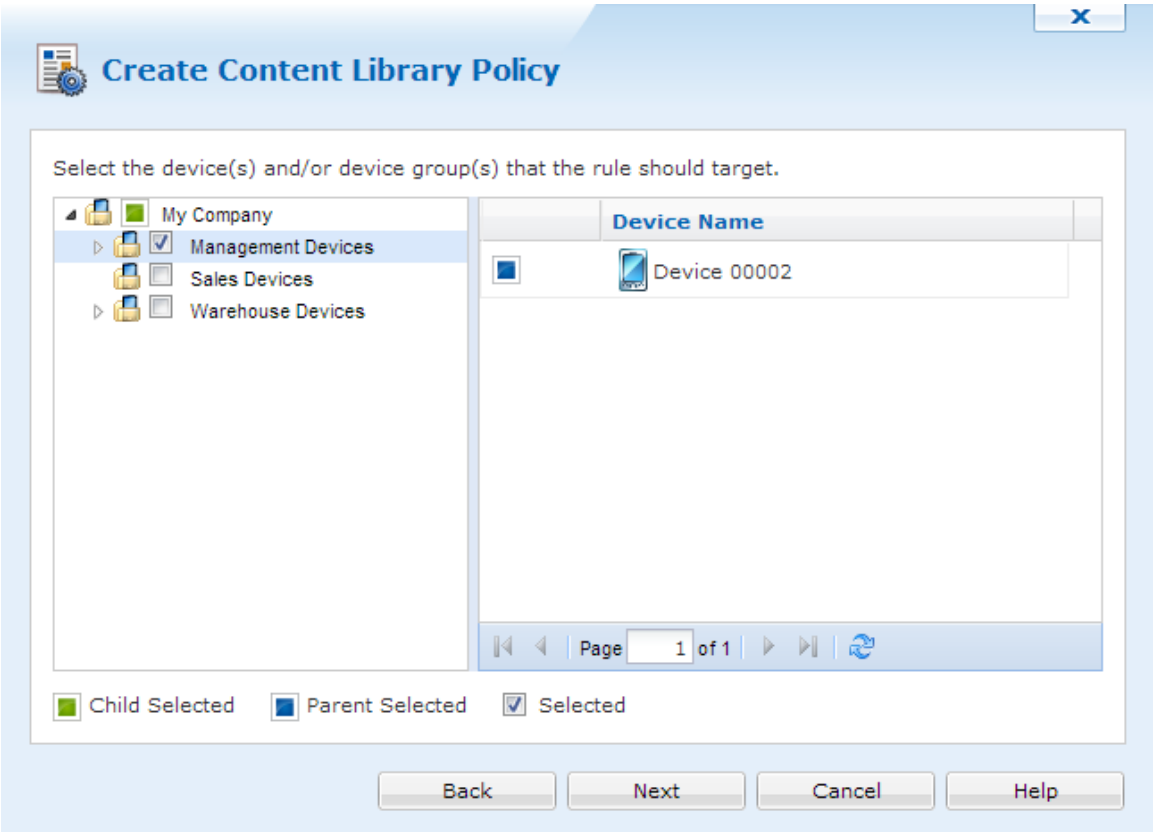
Create Content Library Policy

When we clicked Add, the Create Content Library Policy dialog appeared. In the first panel, enter a name, then click Next.

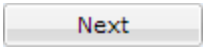


Create Content Library Policy

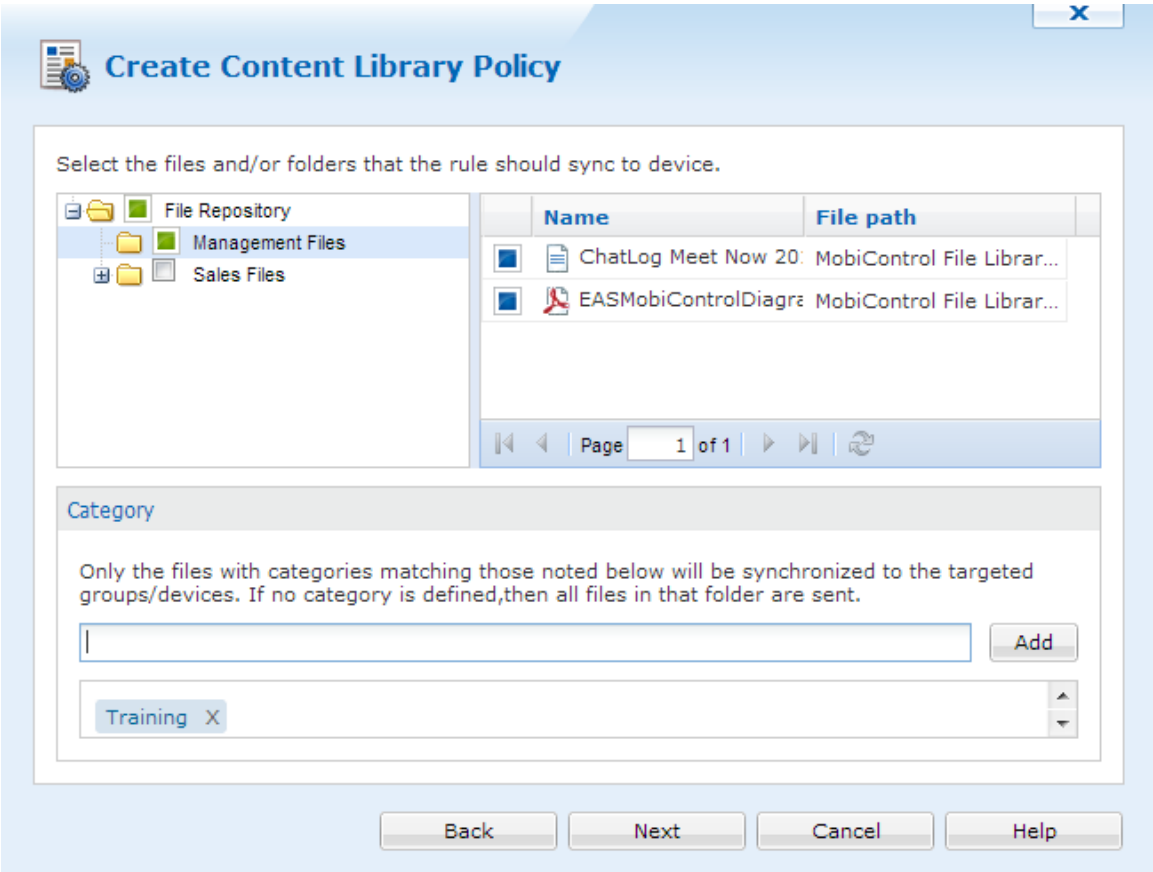
On the next panel, we can select which devices or groups will receive these files.



Select devices and groups

Click  to advanced to the next panel.

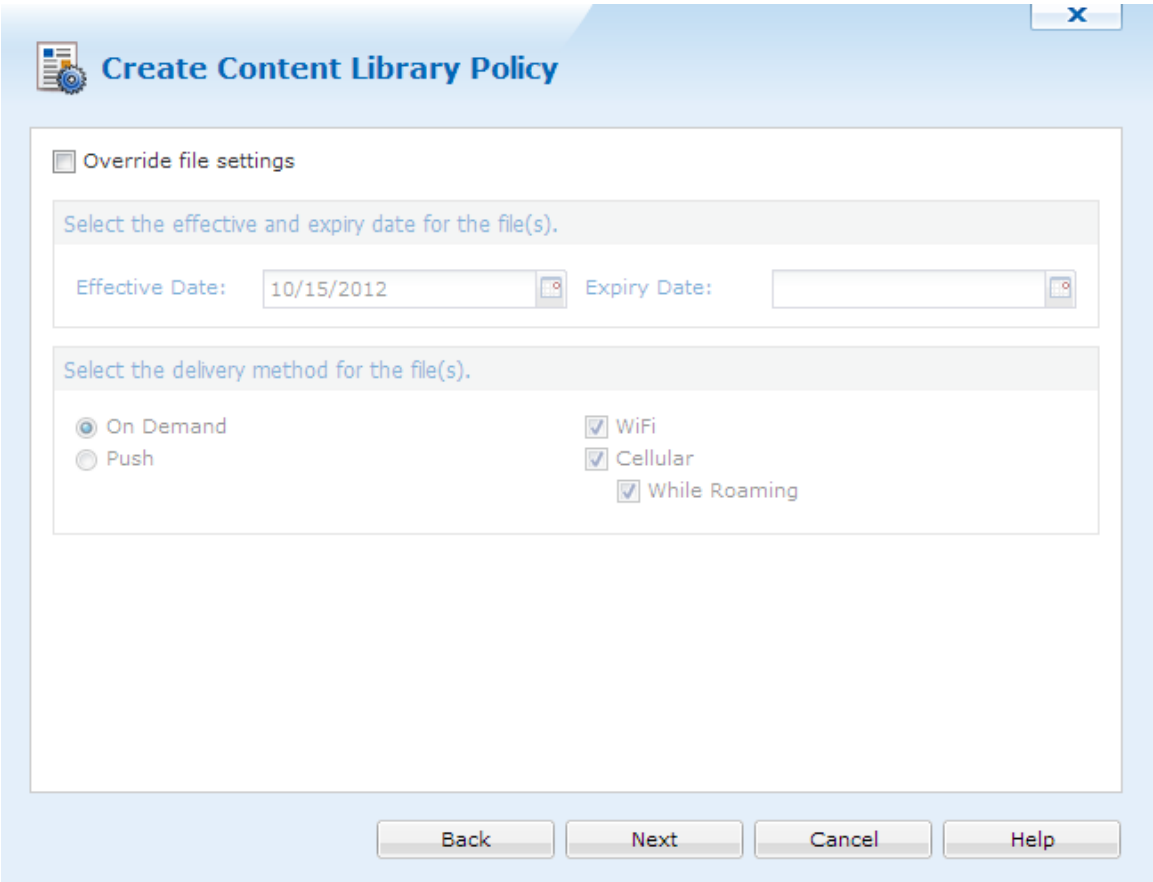
On this panel we are able to select which files are going to be accessible on the devices. If categories were made before, we can just type a category and all files with that tag will be selected.



Source Files

After the files are selected, click Next.

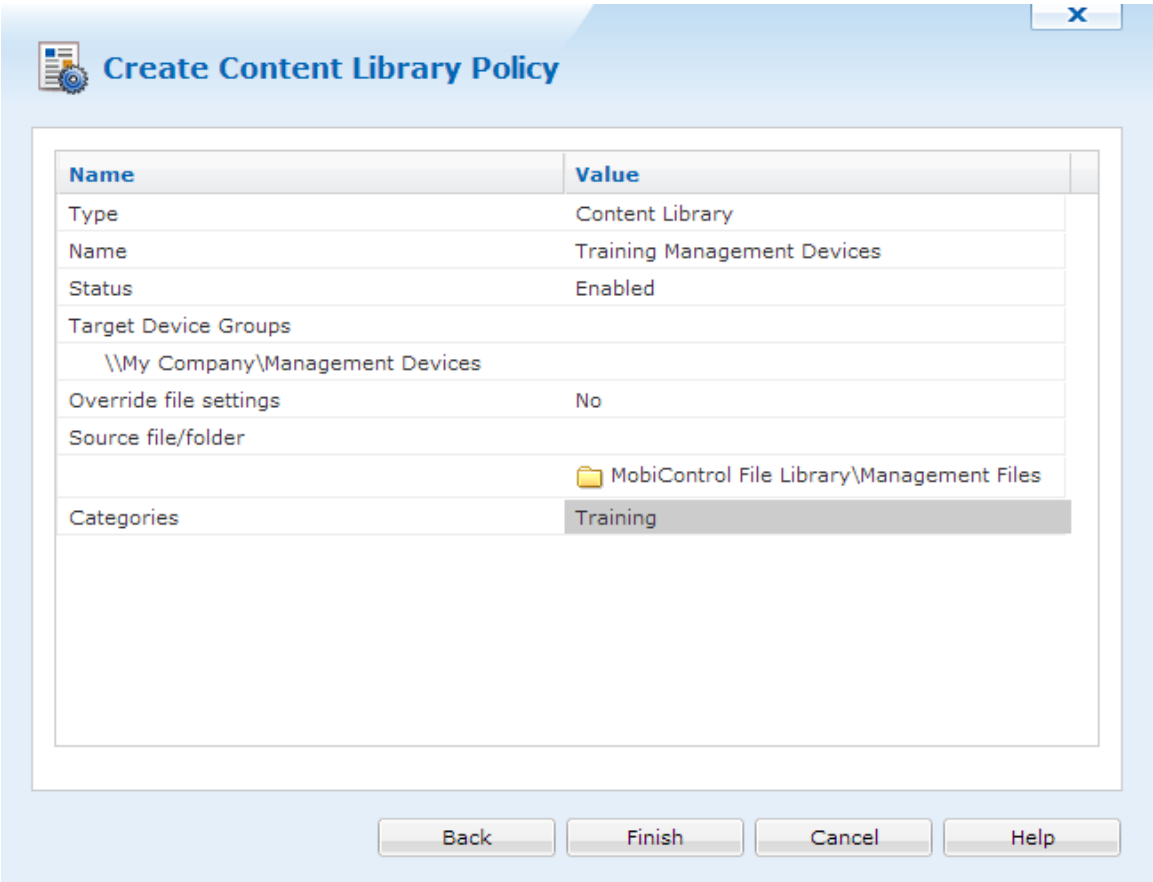
The next panel will allow us to override the file settings. If these settings need to be set, click the Override file settings checkbox.



Override File settings

Once the settings have been set, click Next.

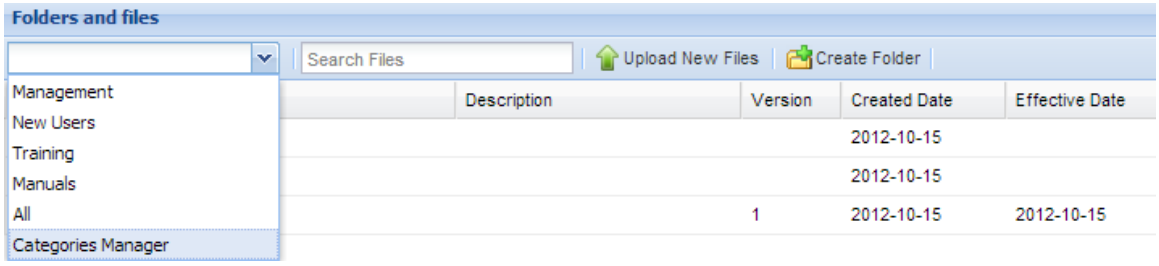
The final panel will show us a summary, click Finish to save and create this policy.



Content Library Policy summary

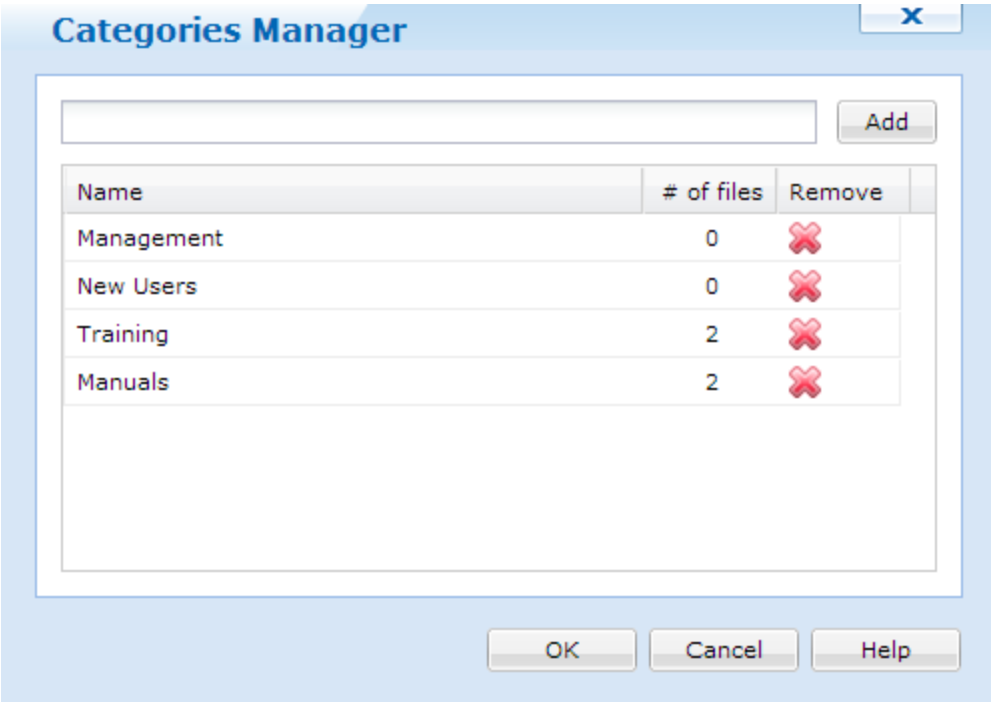
Categories Manager

To gain access to the category manager, click the drop box and select Categories Manager. This drop down list is located in the Folders and Files panel.



Categories Manager selection

Once selected, the Categories Manager dialog will open. Here we can delete previously created categories, and create new ones. We can also see how many files a category was tagged in.



Categories Manager

File Context Menu

When files have been uploaded to the Secure Content Library we are given additional options when we right click a file. Please see the "Secure Content Library - File Context" topic below for more information.

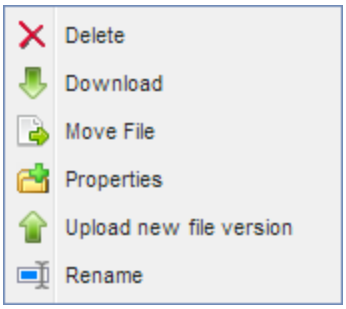
Secure Content Library

File Context Menu

When files have been uploaded to the Secure Content Library we are given additional options when we right click a file.

These options include:

- Delete
- Download
- Move File
- Properties
- Upload a new file version
- Rename

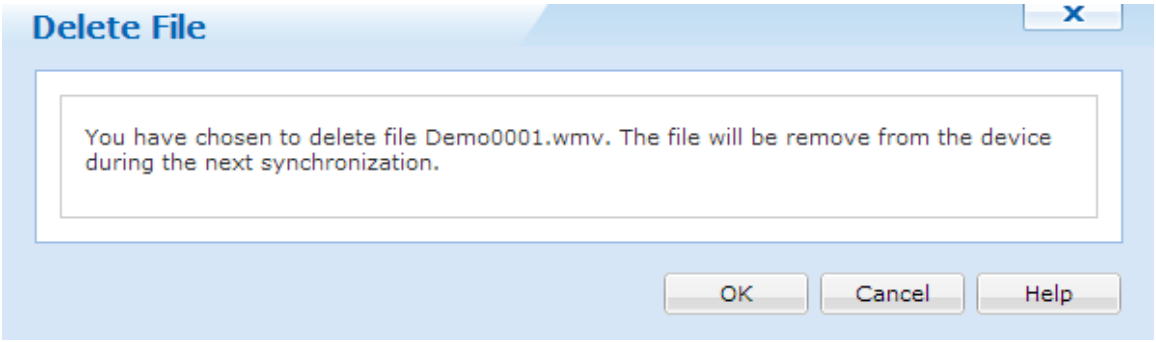


File Context Menu

Delete

Selecting delete will delete the file from the Secure Content Library. A confirmation dialog will appear asking for confirmation.

When a file is deleted from the Secure Content Library and it was already pushed to devices, the file will be removed from devices on the next synchronization.



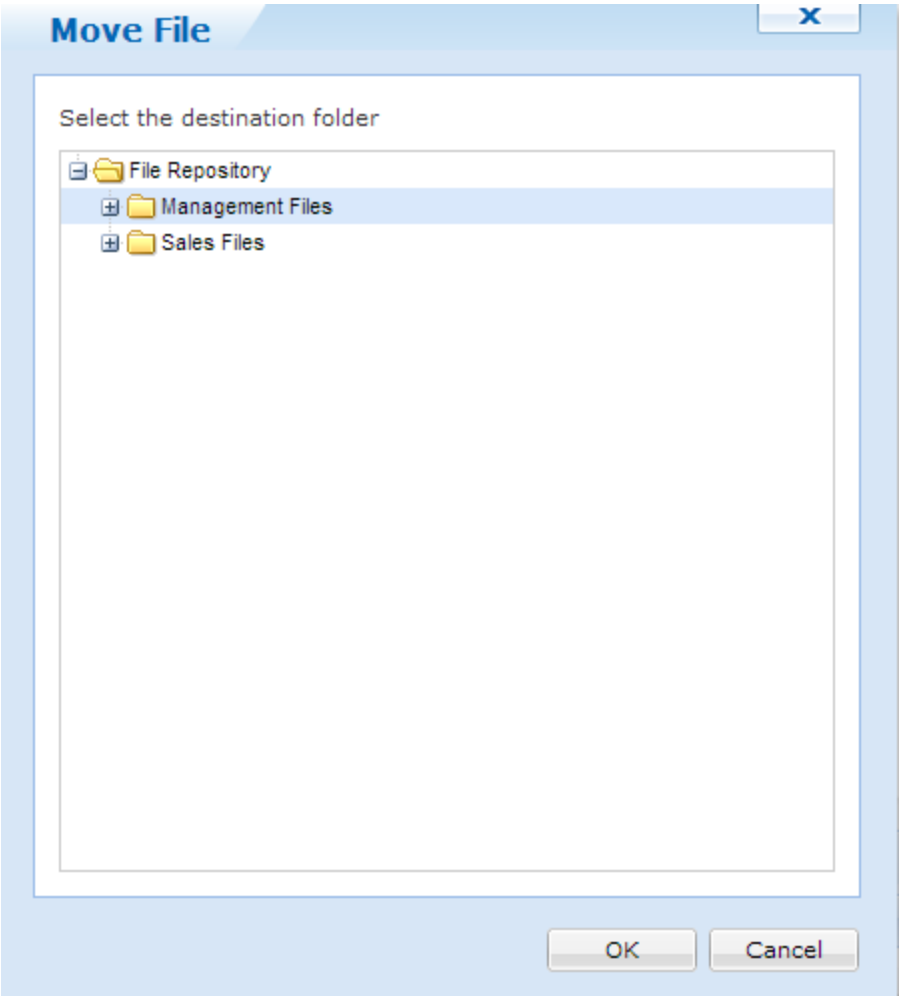
Delete dialog box

Download

Selecting download will download the selected file into the default download directory for your browser.

Move File

Selecting Move File will allow us to move the selected file to a different folder in the content library.



Move File dialog

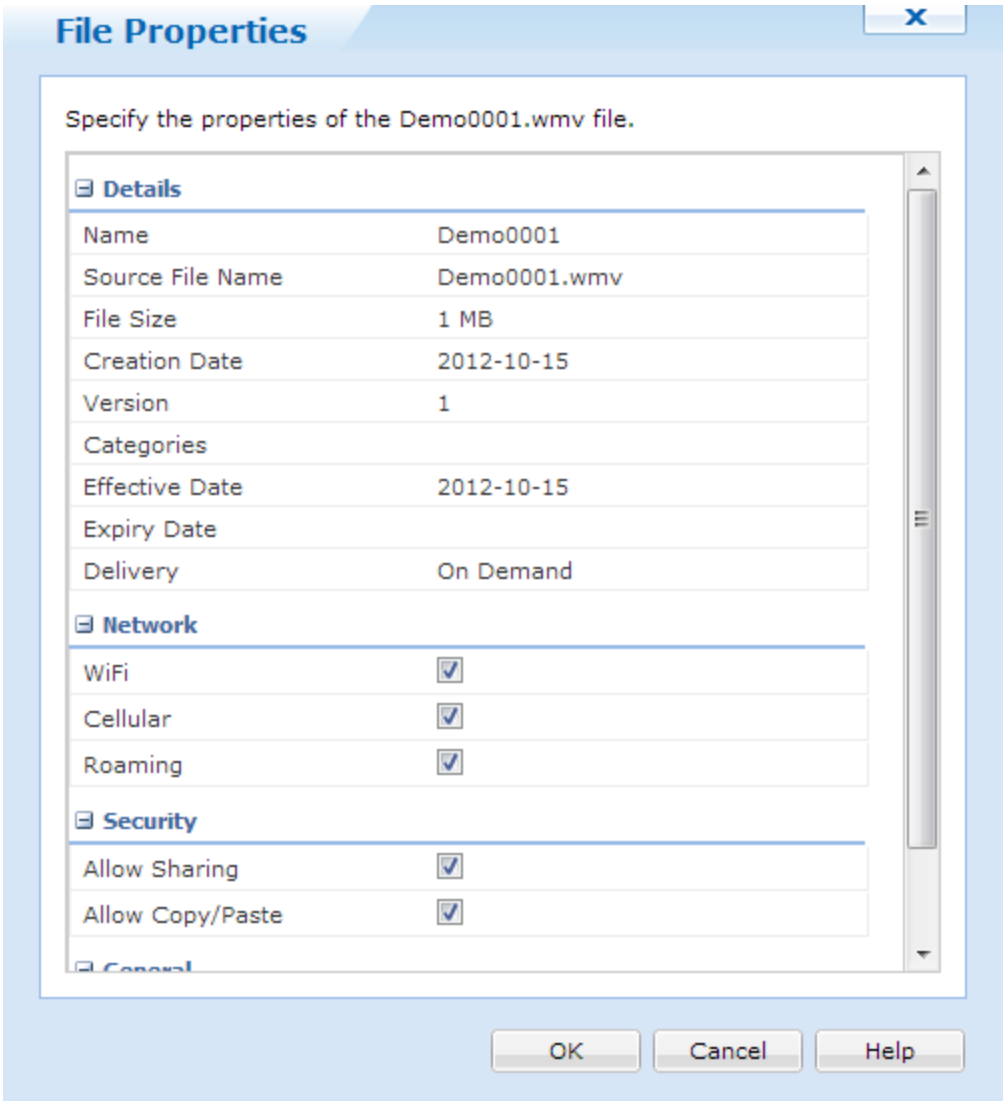
Properties

Clicking Properties will bring up the File Properties dialog. Here we can see all properties that is associated with this file.

Most of the settings here can be configured or edited.

NOTE:

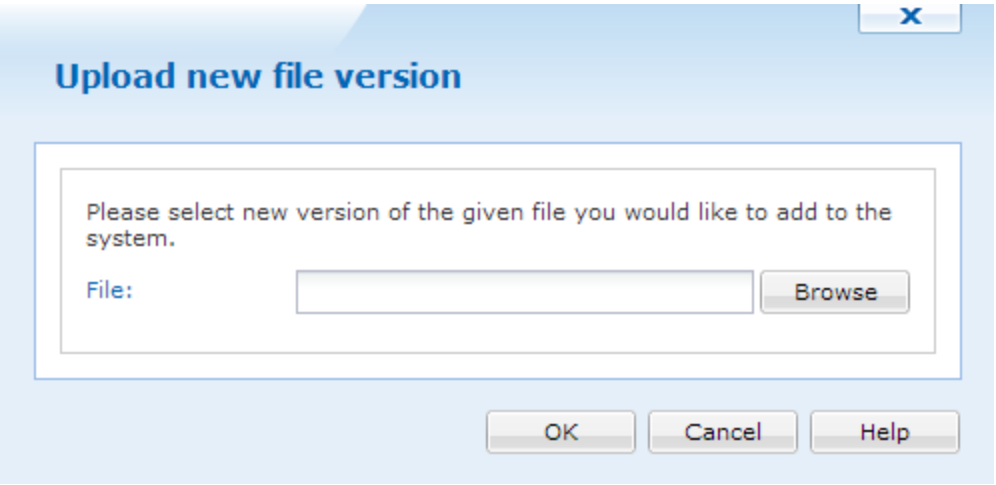
Security settings are only available for iOS devices.



File Properties

Upload new File Version

When we select the upload button, we are given the option to upload a new version of the specified file. When a new file version is uploaded, devices will be able to download the latest version.



Upload New File Version

Rename

Renaming allows us to change the display for the file type. This will not change the actual file name.

Dashboard

The MobiControl Dashboard offers a high level overview of the MobiControl Deployment. It provides high level device and server information on such items as Battery Status, Storage Status, and Out of Contact Devices.

Item	Description
Online vs. Offline Devices	Shows online vs. offline devices in a pie chart
Total Devices by Platform	Shows the total count of each type of device in MobiControl
Battery Status	Shows the % of battery available across all devices
Out of Contact Devices	Shows the devices that have not connected to the deployment server over the last 30 days
System Statistics	Shows the MobiControl Deployment System Health
Storage Status	Shows the % of storage available across all devices

Forgot Password

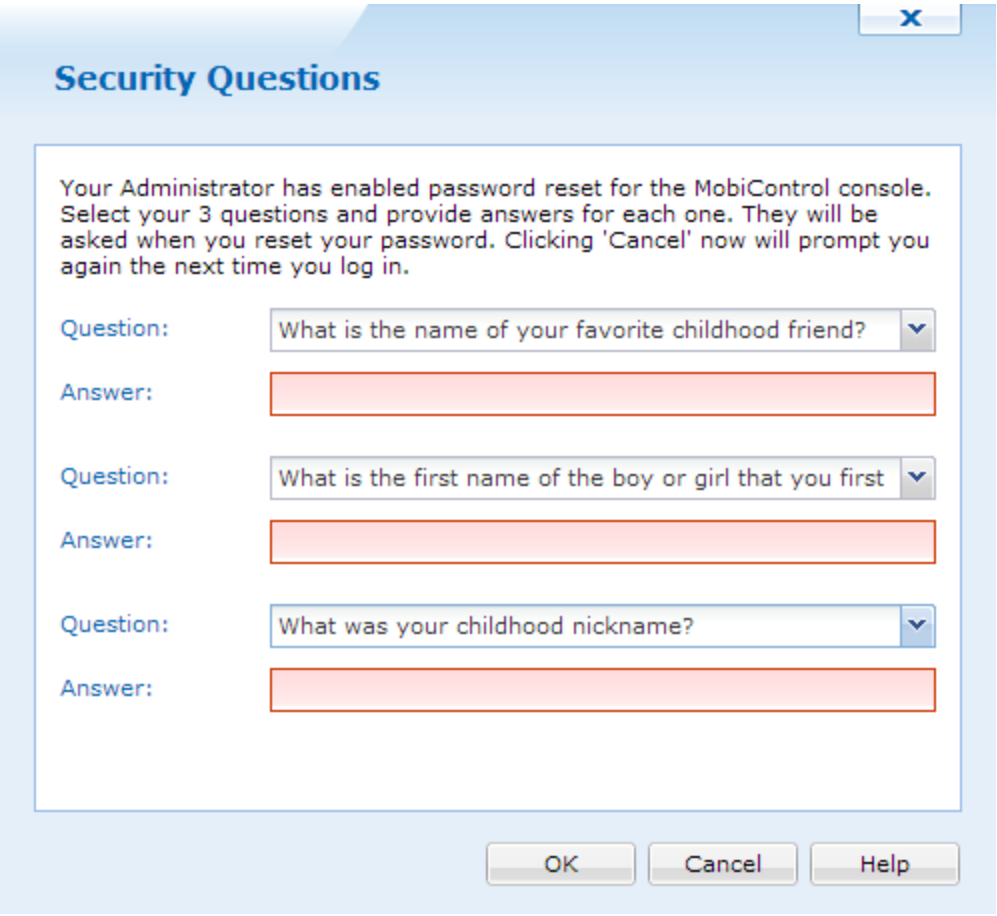
MobiControl has a built in feature that allows users to reset their passwords if they forget it. To enable this feature the "Allow users to reset forgotten passwords" option must be selected in the Access Control Policies. For more information on how to set up Web Console Access Control Policies Please see the "Console Security" topic on page 586.

NOTE:

Forgot password is only available for MobiControl user accounts, not LDAP accounts. If your LDAP account is locked out, please contact your IT department to unlock your account.

Setting up Security Answers

When the Access Control policy is enabled, users who first log into the MobiControl Web Console will have a chance to configure their security questions.



Answering Security Questions

Changing Security Answers

When a user configured their security questions, and is wishing to change them, MobiControl has the ability to change already answered Security Questions.

To change the answers to Security Questions follow these steps:

1. Click the ? icon at the top right hand of the Web Console.
2. Click the Security Questions tab.

Changing security answers

A new window will appear similar to when the user first configured their Security Questions and from here, they can change their answers.

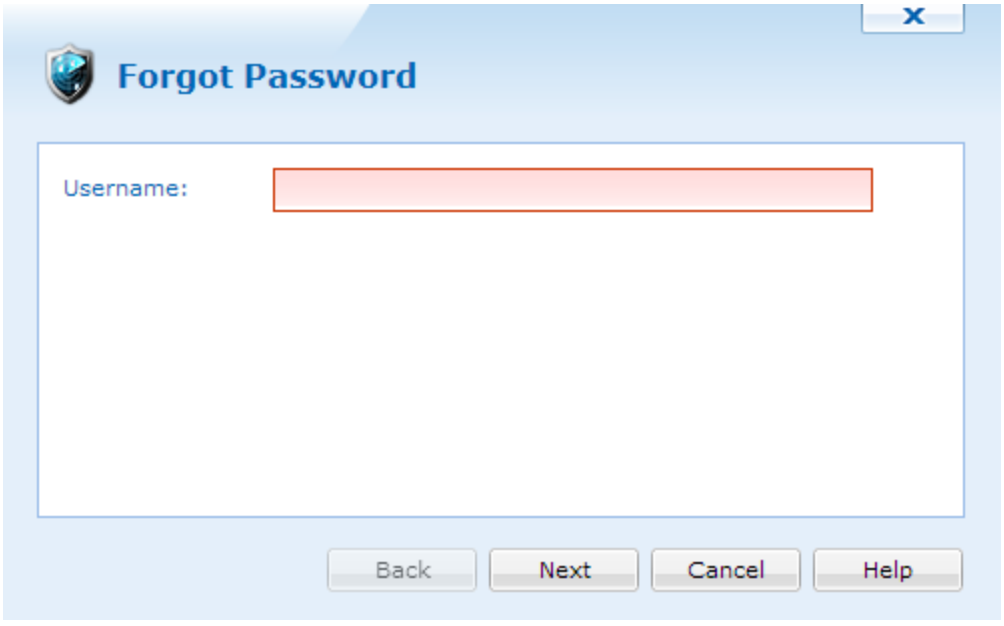
After a user's Security Questions has been answered, they can now reset their password from the log in screen of the MobiControl Web Console.

Using forgot your password

In the log in screen of the MobiControl Web Console, there is a link that will allow you to change your password. This link will only appear if the option "Allow users to reset forgotten passwords" is enabled in the Access Control Policies. For more information on how to set up Web Console Access Control Policies Please see the "Console Security" topic on page 586.

Forgot your password?

When you click Forgot your password, a window will appear asking you to enter your user name. If your user name is entered incorrectly, then MobiControl will show a pop up stating that an invalid user name was entered.

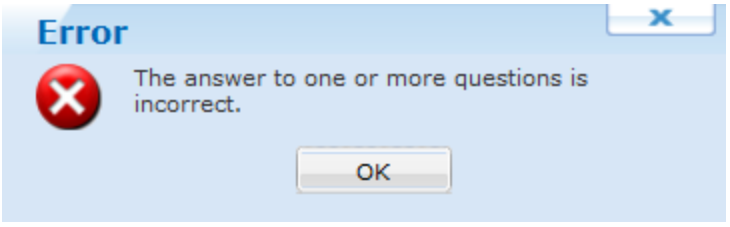


Enter your user name

Incorrect user name

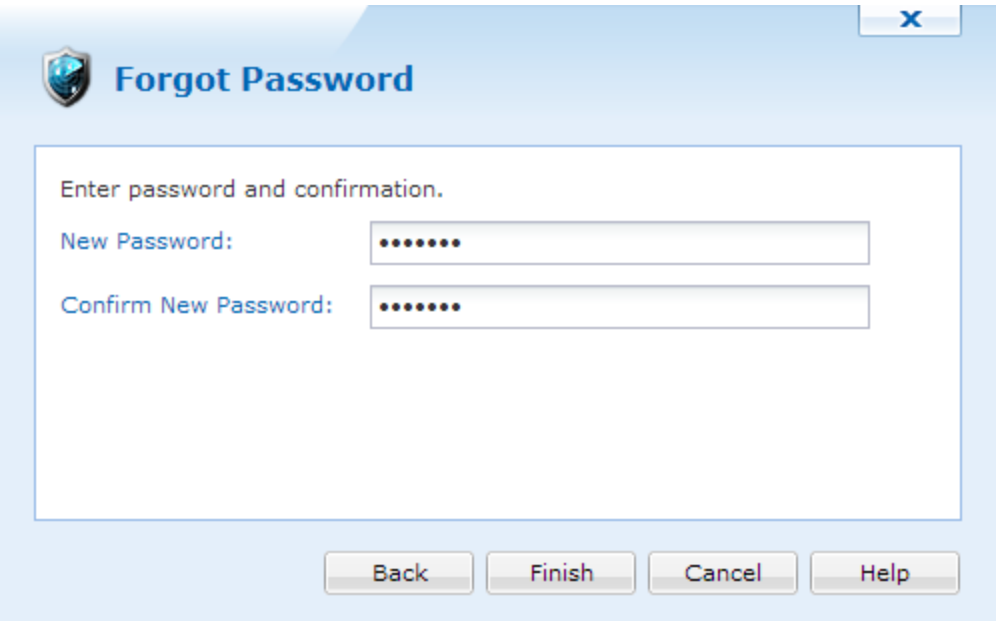
On the next screen, MobiControl will request that the Security Questions be answered. If a question is answered incorrectly, MobiControl will show a pop up asking to answer the questions correctly.

Answer security questions



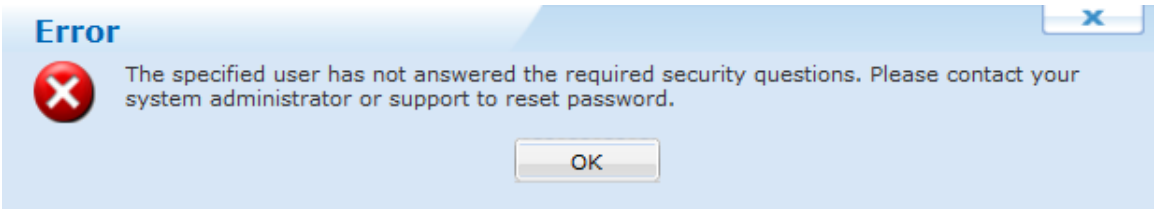
Incorrect answer

When all questions are answered correctly, a new password can now be entered.



Enter a new password

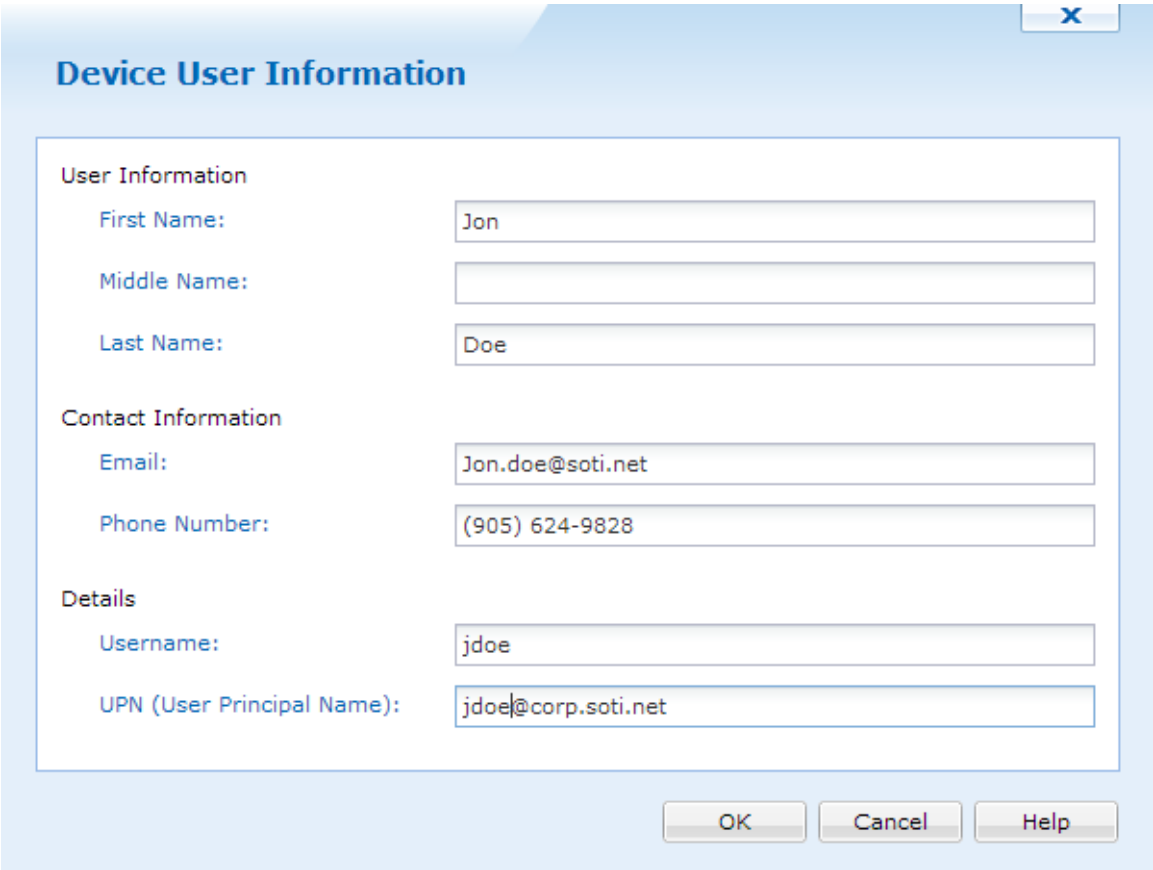
If a user has not set up their Security Answers, MobiControl will tell the user to contact their system administrator or to contact support to have their password reset.



Contact your local Administrator or support

Device User Information

If a device has not been enrolled with LDAP authentication, but you still wish to use certain policies that rely on this information, we can manually configure devices with user information.



Device User Information

To access this panel, we have to select either, Email Address, Username, or Full Name in the column select in the device view. Once the columns are shown, double click any of the columns to bring up the Device User Information panel.

Here we can change the First name, middle name, last name, email, phone number, username, and UPN for a device.

NOTE:

This can only be configured on a per device level, and not on multiple devices at the same time.

Self Service Portal

MobiControl offers a way for users to see what devices are currently enrolled in MobiControl and gives them a way to locate, lock, message and wipe them.

NOTE:

LDAP Console Security must be enabled to utilize the Self Service Portal. Please see the "Console Security" topic on page 590 for more information on how to set this up.

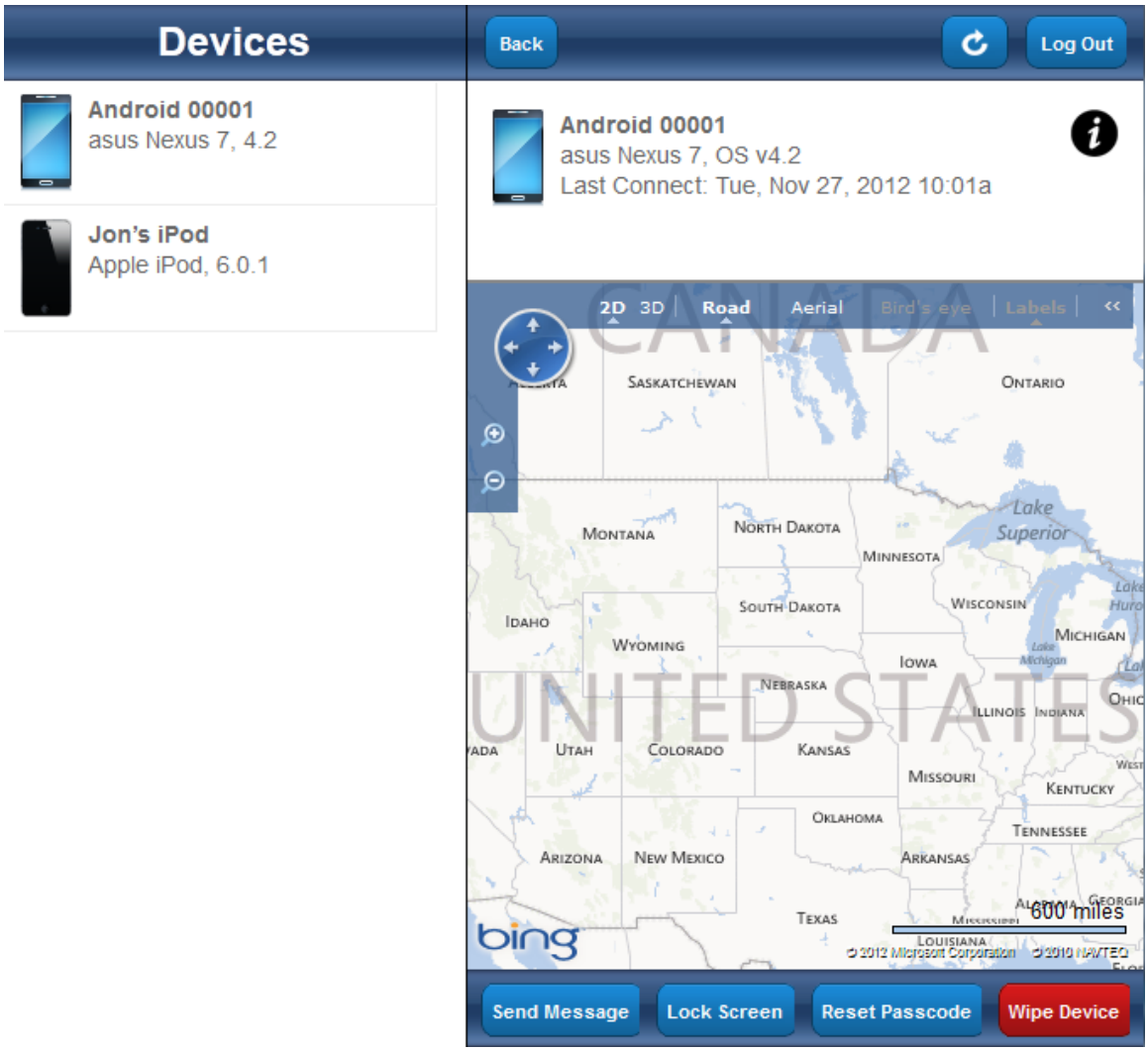
Devices must be enrolled with LDAP authentication, or the device user information must be changed for users to see devices in the Self Service Portal. Please see the "Device User Information" topic on page 1475 for information on how to set up device user information.

To access the self service portal, go to https://yourWebPortalURL/MobiControl/m, and log in with LDAP credentials that were configured in console security.

Self Service Portal Log in Page

Enter the same LDAP credentials used for device enrollment to log in.

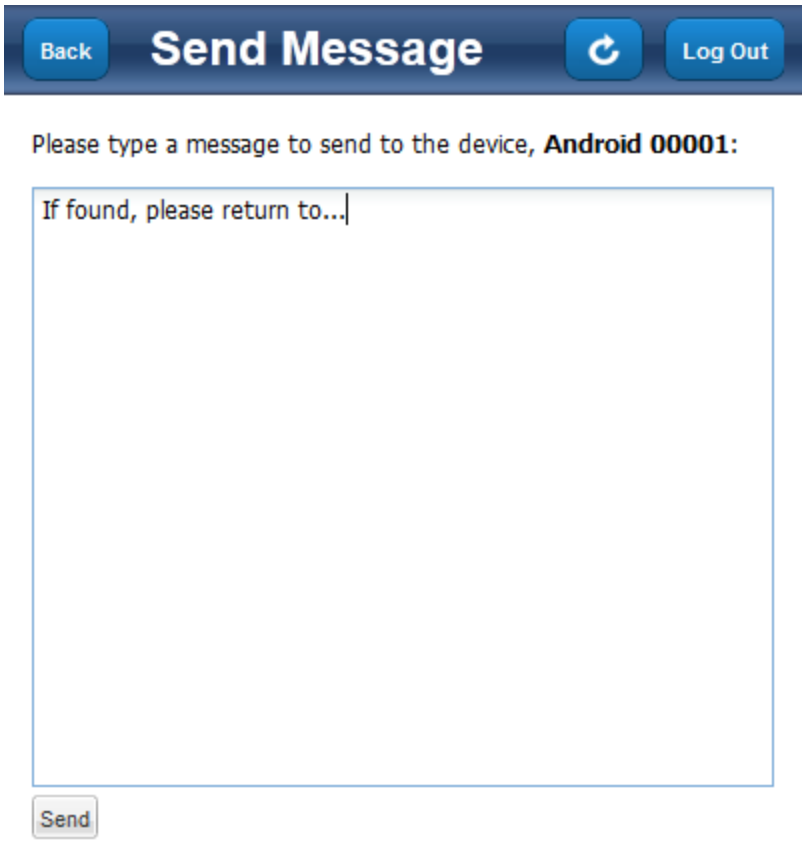
Once logged in, a list of devices that are associated with the username will be shown.



Self Service Device Page

For Android and Android+ devices, we can send messages, lock the screen, reset the password and even wipe the device. For iOS devices, we can send messages, lock the screen and wipe the device.

Clicking send message will open a new panel where we can type the message. Clicking send will then send this message through APNS (Apple Push Notification Service) or GCM (Google Cloud Messaging) to the device.



Sending messages

MobiScan

MobiScan is a tool that can be used to provision the MobiControl Device Agent on a device by scanning barcodes. All the necessary information is encoded into a barcode which will allow your device to connect to your MobiControl Deployment Server. MobiScan can also be used to include initial connection settings (WiFi, Cellular APN, etc) within the barcode which will allow the device to establish communication with a designated network.

SOTI provides software for its MobiScan application to generate the barcode and run on the computing device.

This includes:

MobiScan Barcode Generator - a desktop application included in MobiControl Management console.

Please see the Generating a Barcode section for further information regarding Barcode Generator.

MobiScan Agent - a device side application which processes the barcodes. It consists of one executable named MobiScan.exe

MobiScan agent will be included with your device firmware, depending on your hardware manufacturer.

Please contact your hardware manufacturer or SOTI Support for further details in regards to MobiScan Agent.

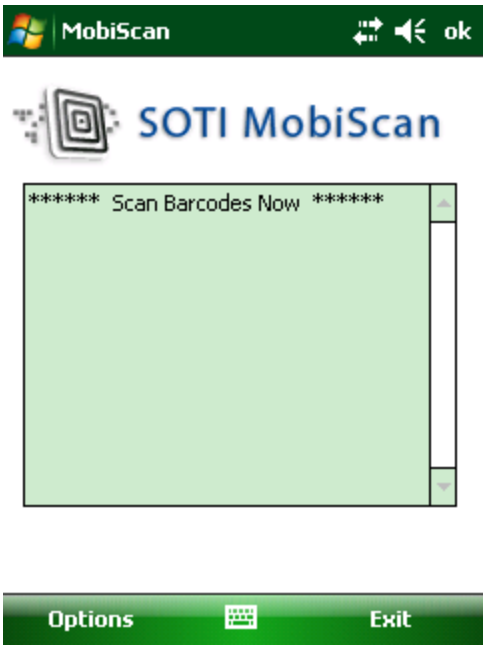
Scanning a barcode using MobiScan:

1. Enable Scan Wedge on the device

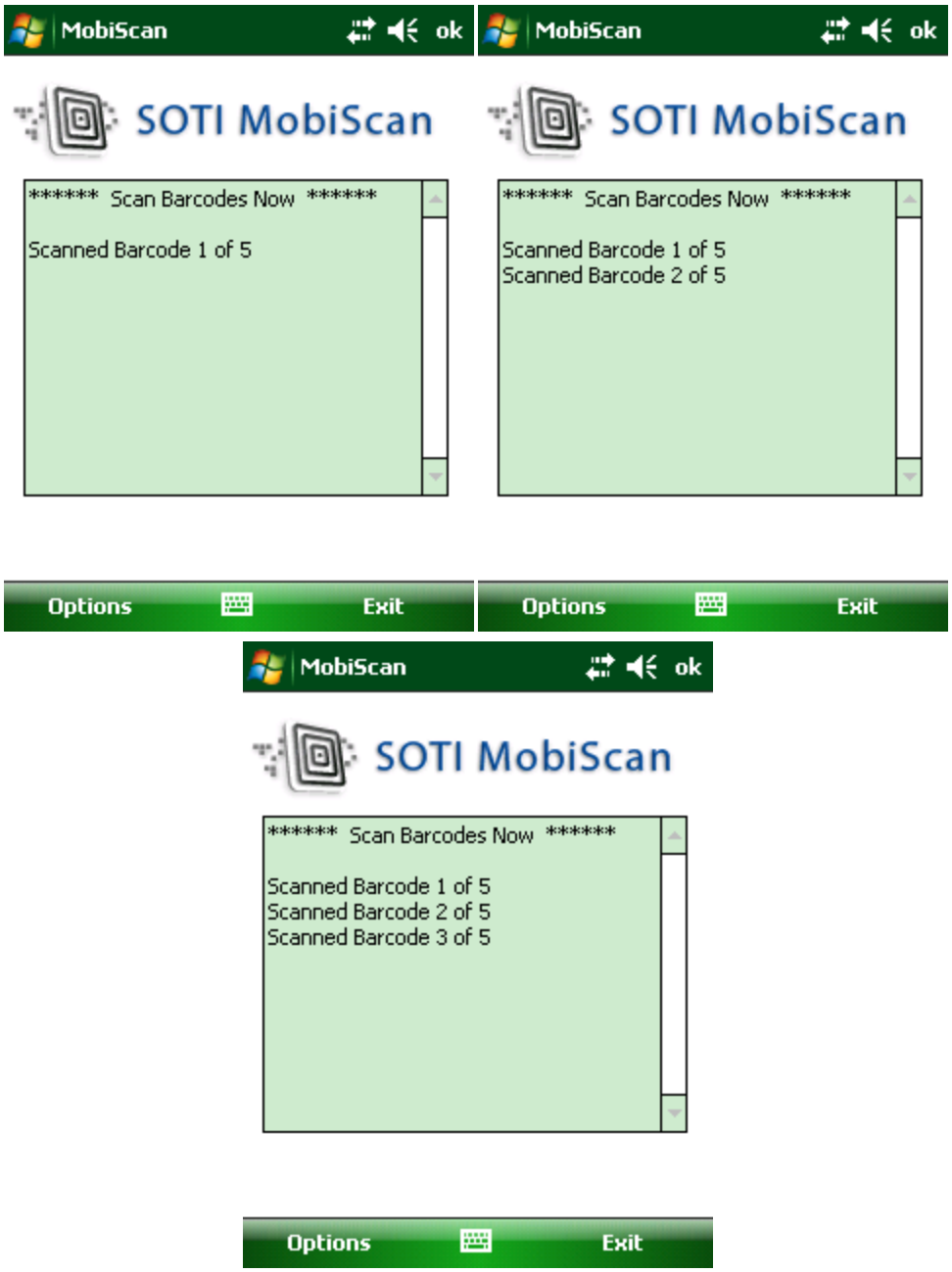
   This procedure varies depending on the device manufacturer and model. On some devices MobiScan will automatically handle this operation, and on others it must be launched manually. Please see your device manual for further details.

2. Launch the MobiScan executable from the device

   Once the MobiScan Agent has been successfully launched on the device, the following screen will appear:



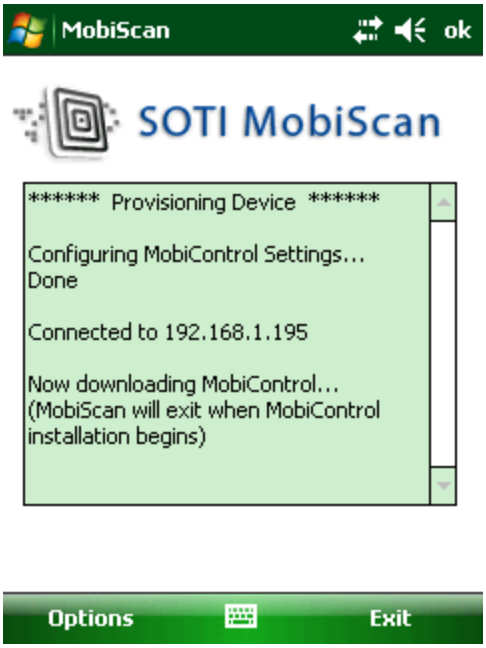
3. Scan the barcodes



NOTE:

Please ensure that all barcodes have been scanned.

The following screen will appear:



The MobiScan Agent will first configure the connection settings (Wireless, APN, etc..) according to the settings configured in MobiControl Manager, and then apply the MobiControl settings and will attempt to connect to the MobiControl Deployment Server.

Once a connection has been established, MobiScan will automatically begin downloading the CAB from the MobiControl Deployment Server.

MobiScan application will exit when MobiControl installation begins.

User Defined Values

Some commands will have the ability to handle user defined data, if this option is enabled when creating profile from MobiControl Manager.

The user will be able to edit the corresponding value on the device, after the barcode has been scanned.

The user can choose to either edit the field or leave it as the default value.

Storing Barcodes on the Device

Whenever a barcode is scanned, an encrypted copy of its contents is automatically saved on the device. The data file MSData.dat, may be found in the PdbPkg folder.

The PdbPkg folder is located in the directory specified by the "Stable Storage" field in MobiControl Manager.

If the option "execute after cold boot" is enabled in MobiControl Manager while generating barcode, the data for this barcode is stored as MSBoot.dat in the same Stable Storage folder.

NOTE:

The barcode is only saved on the device after MobiControl settings have been applied.

Command Line Usage

The MobiScan Agent can be launched from the command line to configure the device using a stored barcode.

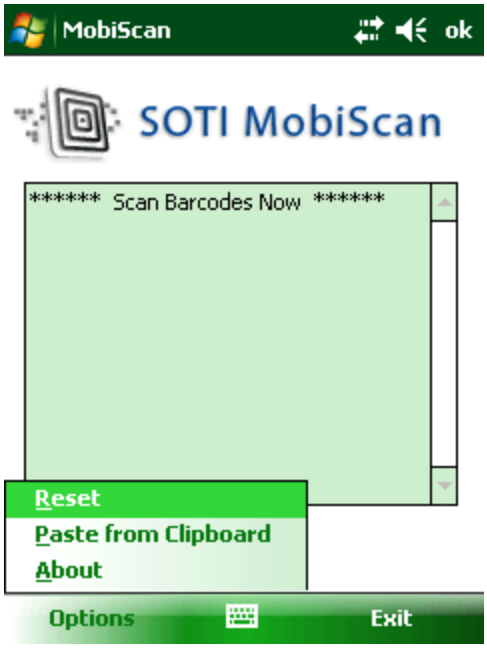
Syntax:
MS_Agent.exe -[p] -[m] [File Path]

-p: Silently execute barcode at [File Path]
-m: Silently execute barcode at [File Path]. This option skips configuring MobiControl settings.

The file path may be full path or a relative path. Example: MSAgent.exe -p 1:\SOTI\PdbPkg\MSData.dat

When MobiScan is launched in silent mode, default choices will be selected where applicable. If MobiControl has already been installed on the device, MobiScan will not attempt to re-install it.
If AES256 encryption has ben selected, the user will always be prompted to enter the password.

Options



Field Name	Description
Reset	This option will clear the stored barcode data from the device.
Paste from Clipboard	MobiScan Agent has the ability to execute the contents of the clipboard as a stored barcode. The data on the clipboard is the same as the data saved is MSData.dat and from the Barcode Generator using Ctrl + r in the "Generating Barcode" step.
About	This option gives the version and build information about the MobiScan Agent.

Generating a Barcode

Barcode Generator is a method that can be used to provision the MobiControl Device Agent on devices by scanning barcodes.

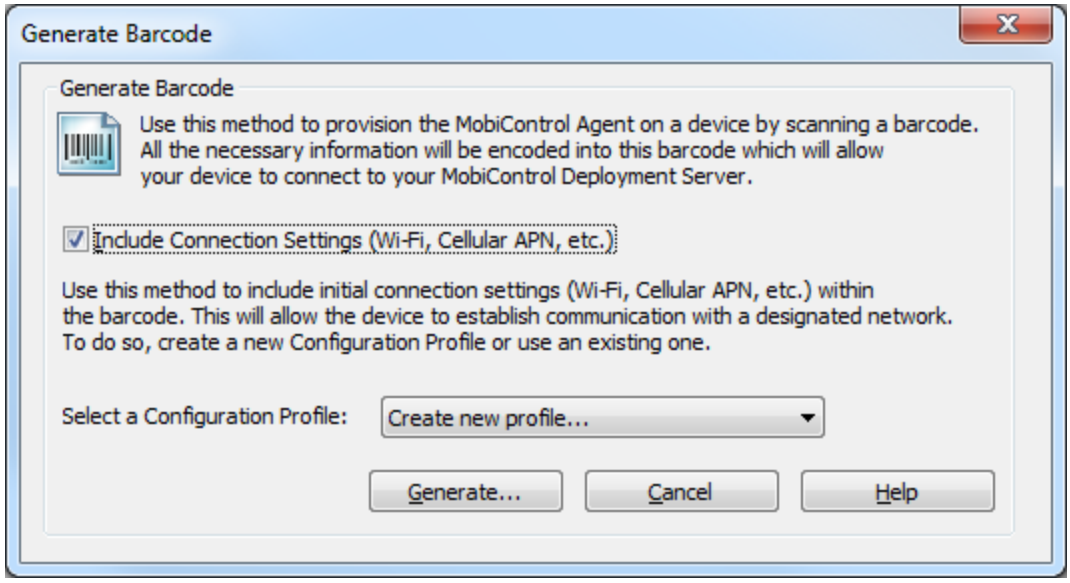
The generated barcode will encode all the necessary information to allow the device to connect to the MobiControl Deployment Server.

IMPORTANT
MobiScan requires .NET 3.5 to be installed to work properly. Click here to download .NET 3.5.

The following series of steps describes how to Generate a Barcode:

1. Start the wizard

   In **Device Agent Manager**, select the appropriate Device Agent, then click **Provision Device,** click **Generate Barcode:**



Option	Description
Include Connection Settings	This option enables you to include the initial connection settings (Wi-Fi, Cellular APN, etc..) within the barcode. The device can use these Settings to establish a connection with the designated network. Please review Configuration Profile Manager section for further details regarding these settings.

2. Select a Configuration Profile.

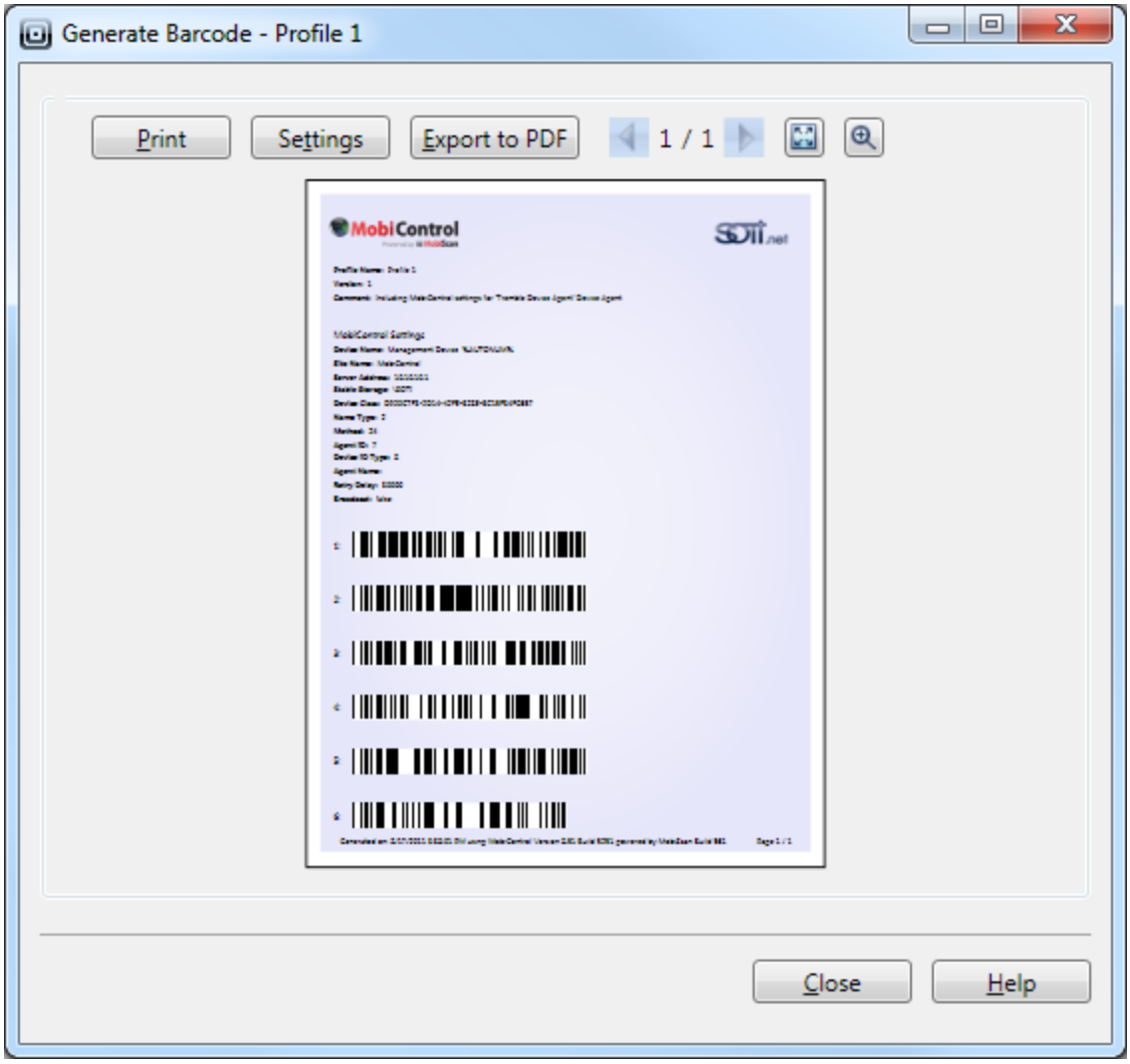
You can select a Profile available from the list or create a new Profile using Configuration Profile Manager.

3. Generate Barcode

Click on **Generate**

If a Configuration Profile is selected from the list, it will generate the Barcode with encoded settings according to that Profile.

If "Create new profile" is selected from the list, it will open the Configuration Profile Manager wizard to create a new Profile. The barcode will be generated at the end of this wizard.



NOTE:

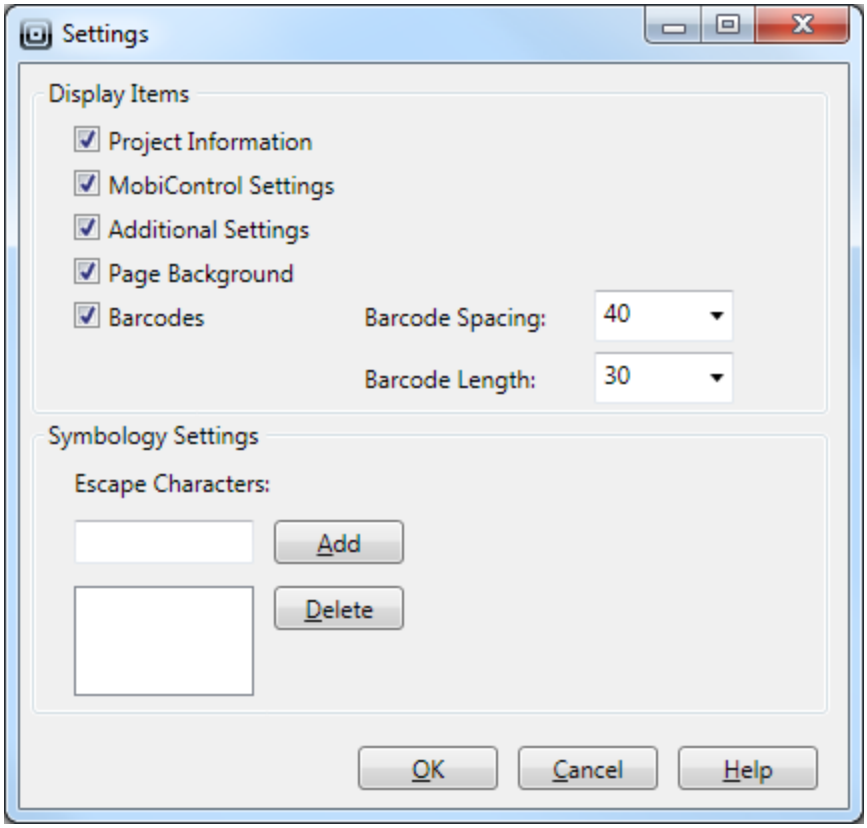
If you have not checked the Include Connection Settings option, the Barcode will be generated only with the MobiControl Device settings information.

Click on "**Print**" to print the current Barcode.

Click on "**Export to PDF**" to export Barcode to a PDF file, which can be forwarded or printed at a later date.

Click on "**Settings**" to modify the Barcode settings.

4. Barcode Settings



Field Name	Description
Project Information	Check this option to display the Project information (name, version, comment, etc..) in the page.
MobiControl Settings	Check this option to display the MobiControl Device Agent settings information in the page.
Additional Settings	Check this option to display the configured Settings included via Configuration Profile in the page.
Page Background	Check this option to display a background with the page.
Barcodes	Check this option to display the generated barcodes in the page. **Barcode Spacing:** Can be adjusted according to preference. **Barcode Length:** Can be adjusted according to preference.
Escape Characters	You can add **Escape Characters**, if required in your barcode.

MobiControl Frequently Asked Questions

General

G1. What are the system requirements for MobiControl?

G2. Can MobiControl be used on a Windows Vista or Windows 7 computer?

G3. How do I tell what version of MobiControl I am using and where do I view my licensing information?

G4. How do I minimize the battery drain on my device?

G5. What are recommendations for doing backups?

G6. How do I rename a device?

G7. How do I setup my devices to connect through an external network?

Installation, Upgrade, and Uninstallation

IU1. How do I install only the MobiControl Manager console?

IU2. Why is MobiControl running in trial mode when I am an existing registered user?

IU3. How do I safely upgrade MobiControl?

IU4. How do I move my Deployment Server from one machine or server to another?

Connectivity

C1. I created an add device rule, generated a Device Agent, and installed it onto my mobile device. Why doesn't it seem to connect to MobiControl?

C2. Is there a way to troubleshoot or test to see if my devices can successfully connect to Deployment Servers?

C3. What settings should I use for slow connections?

C4. Do dynamic IP addresses present a problem for MobiControl?

Device Agent

A1. I installed the Device Agent on my device but it is not showing up in the device tree. How can I make it appear?

A2. How can I make sure that the clocks on my mobile devices have the proper time?

A3. Why is the MobiControl Device Agent changing the server host name/IP address information that I am configuring on the device?

A4. Can I use MobiControl to manage my Windows-based computers, laptops, tablet PCs? If so, how can I create the agent?

Remote Control

R1. What settings should I use to remotely manage and establish remote control sessions to devices over cellular (e.g. GPRS) or dial-up connections?

R2. How can I use MobiControl to manage and/or remote control devices whose IP address is not reachable or not public (i.e. external or private addresses) as is often the case for GPRS connections?

R3. I need to remote control a device that is in the sleep or standby mode and is currently offline. How can I wake up the device and force it to connect to MobiControl?

R4. Why do I get a Rapi initialization timeout error when I try to remote control my mobile device?

Security

S1. How do I put pictures into my lockdown menu?

S2. How can I restrict what a user of the MobiControl Manager console can do?

Package Creation and Deployment

PD1. How do I deploy registry settings?

PD2. Do I need a second Deployment Server?

PD3. I am running my application on all my devices. From time to time I have to update some settings in my applications .ini file. I don't want to send the entire .ini file each time, is there a better way?

PD4. I need to create a script that I will use in the package I deploy to my devices. Is there a way to test the script before I deploy it to my devices?

PD5. Does MobiControl support a fault tolerance Deployment Server?

Scripts

SC1. Are there any APIs (Application Programming Interfaces) available so that I can call and execute a MobiControl scripts from a custom application?

Database

D1. What are recommendations for doing backups?

D2. Can I use a third-party reporting tool to generate my own custom reports?

General

G1. What are the system requirements for MobiControl?

Please click here to see the system requirements needed for MobiControl.

G2. Can MobiControl be used on a Windows Vista or Windows 7 computer?

Yes, you can use MobiControl on a Windows Vista or a Windows 7 computer. If you are connecting your device via USB to your computer, you need to download and install the Microsoft Windows Mobile Device Center on your computer first. Please visit Microsoft's website at http://www.microsoft.com/windowsmobile/devicecenter.mspx to download Microsoft Windows Mobile Device Center.

G3. How do I tell what version of MobiControl I am using and where do I view my licensing information?

In MobiControl Manager, from the menu bar, click **Help**, and then click **About MobiControl Manager** to view the version and build information. Also listed in this window is the licensing information, displaying the number of servers and devices licensed and how many devices are in currently used within your license.

G4. How do I minimize the battery drain on my device?

MobiControl has several settings that allow you to optimise the Device Agent behavior to minimize battery drain.

1. Device Connection Sensitivity

   (Right-click on the Deployment Server in the Deployment Servers view (tab) and select **Deployment Server Properties**). You can set the **Send Test Message to Devices** parameter to a higher interval to reduce the communication between the device and the server. This will increase the time it takes for the server to recognize a device as online or offline.

2. Device Retry Interval

   (Right-click on the device, select **Configure Device,** and then **Advanced Settings**. Set the device retry interval to a higher number. The lower the number, the more aggressively the Device Agent tries to connect to the Deployment Server. For example, if it is set to 300 seconds, when the device is offline, it will try to connect to the Deployment Server every five minutes.

3. Device Update Schedule and File Sync Schedule

   You can increase the time interval after which the device checks the server for updates, packages, or file synchronization (when it is online and connected to the server). For the device update schedule, right-click on the device, select **Configure Device** and then **Update Schedule**. Typically, in a test environment, the update schedule is set to a shorter interval to quickly see the results of test packages, etc. In a production environment, the devices may not need to download updates for hours/days. Similarly, the file synchronization schedule can be changed by editing the file sync rule under the Rules view (tab).

4. Connection Mode

   (Right-click on the device and select **Configure Device** and then **Advanced Settings**.) By default, the MobiControl Device Agent runs in the "Persistent" mode in which the Device Agent tries to maintain its connection to the Deployment Server whenever a data network is available. You may maximize battery life by changing the connection mode to "Scheduled" or "Manual" (depending on your environment), so the Device Agent only connects to the server within a limited time window (to download updates, synchronize files, for support, etc.). Adjusting the connection mode would achieve the highest battery consumption efficiency.

G5. What are recommendations for doing backups?

We recommend that you do a backup as often as possible. If you are running MobiControl v2.06 or earlier, you need to backup your file store and your database. If you are using MobiControl v3.00 or later, you only need to back up your database. To back up your file store, use the Microsoft File Explorer to copy the contents of the file store to a backup folder. To back up your database, if you are using the lightweight Microsoft SQL Server Desktop Engine (MSDE) you may need to purchase a third-party tool to backup your database. If you are running the full Microsoft SQL Server, you can back up your database using the tool provided with Microsoft SQL Server Enterprise Manager. Most database back up tools provide an automated back up system so that your database will be automatically backed up at regular intervals.

G6. How do I rename a device?

The device name is considered the user-friendly name for the device. It is not the unique identifier for the device in the MobiControl system (that is the role of the device ID). It is possible to have more than one device with the same name, although that is not recommended because it will lead to confusion. From the device list, right-click on the mobile device icon of which device you want to rename. A menu of device options will appear. Select **Rename Device** and enter your desired name for the mobile device. Note that you can also change the device name from the MobiControl applet in the **General** tab in the configuration options that runs on the actual device.

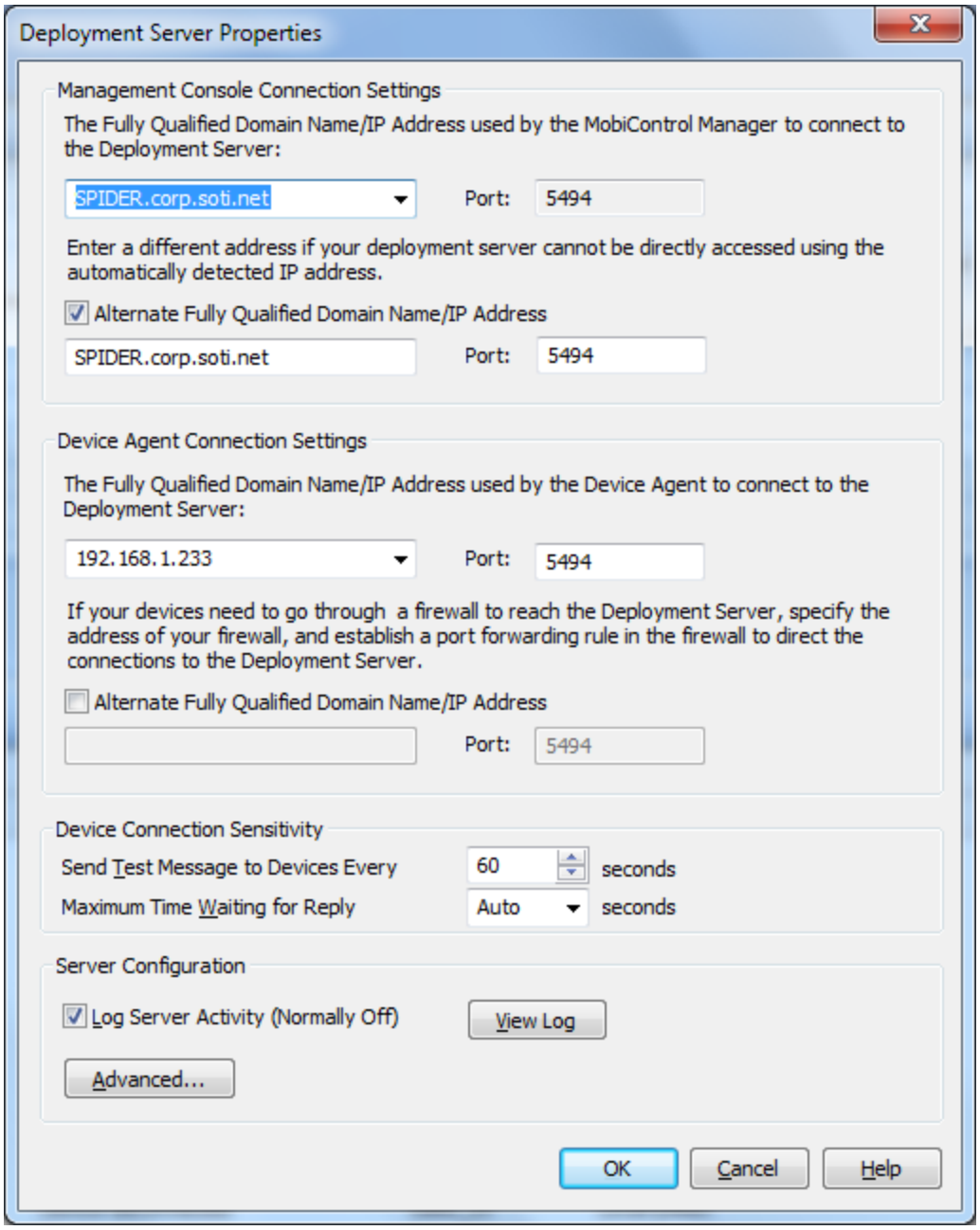
You can also have the mobile device have its name based on a custom data value. For more information, please see Q3. How do I use "custom" information to name my mobile devices (e.g. the device owner's name)? in the "Tips and Tricks" topic on page 1511.

G7. How do I setup my devices to connect through an external network?

When your devices are connected on an external network (GPRS/CDMA) they require a Public IP in order to communicate with your Deployment Server. In most situations companies have a corporate firewall on their Public IP address. You must configure your corporate firewall to allow devices to connect to the Deployment Server. Set up your firewall to port forward from Port 5494 publicly to Port 5494 internally. Port 5494 is used for Windows and Android device communication and is fully customisable by opening the MobiControl Manager, and going to the Deployment Server tab, right click on your deployment server, and select server properties.In the server properties window, you will be able to set a custom port for device communication as well as the public IP addresses the devices must use.

For example, if your Deployment Server has an Internal IP of 192.168.1.184 and your Public IP is 210.25.10.219 all incoming traffic on 210.25.10.219:5494 must be forwarded to 192.168.1.184:5494.

Open the MobiControl Manager, go to the Deployment Server Tab, Right Click on your Deployment Server and select Server Properties. In the Server Properties dialogue box place a check mark in the "Override Default IP" box, and the "Alternate IP Address" box. Enter the Public IP Address or Hostname in the Alternate IP Address box. When finished entering the new information, click on OK. The devices will receive this information upon a device update schedule or as they come online. This change instructs the device to attempt connecting to the deployment server using the Alternate IP Address/Hostname if it fails to connect at the IP Address originally provided. These settings get stored in the device agent and will take effect from now on. Each device MUST connect to the deployment server for these settings to get updated on the device.



Installation, Upgrade, and Uninstallation

IU1. How do I install only the MobiControl Manager console?

During the MobiControl installation, when you get to the **Select Features** option, there are three options listed: **MobiControl Manager**, **MobiControl Web Console** and **MobiControl Deployment Server.**Checking all of these options will install all the components of MobiControl, including the Deployment Server. The checking only one option is used to select the exact components you wish to install on the computer. Click **MobiControl Manager** and click **Next**. Select **MobiControl Manager** and click **Next**. The next process is to enter the database data in the **Data Link Properties** dialog box to finish the installation.

IU2. Why is MobiControl running in trial mode when I am an existing registered user?

For existing MobiControl users, it is necessary that you exchange your current registration code with a new registration code for MobiControl v6.00.

If you haven't obtained your new MobiControl v6.00 registration code, please contact us to exchange your registration code. (You will need to provide the company name and person to whom the product is licensed.)

IU3. How do I safely upgrade MobiControl?

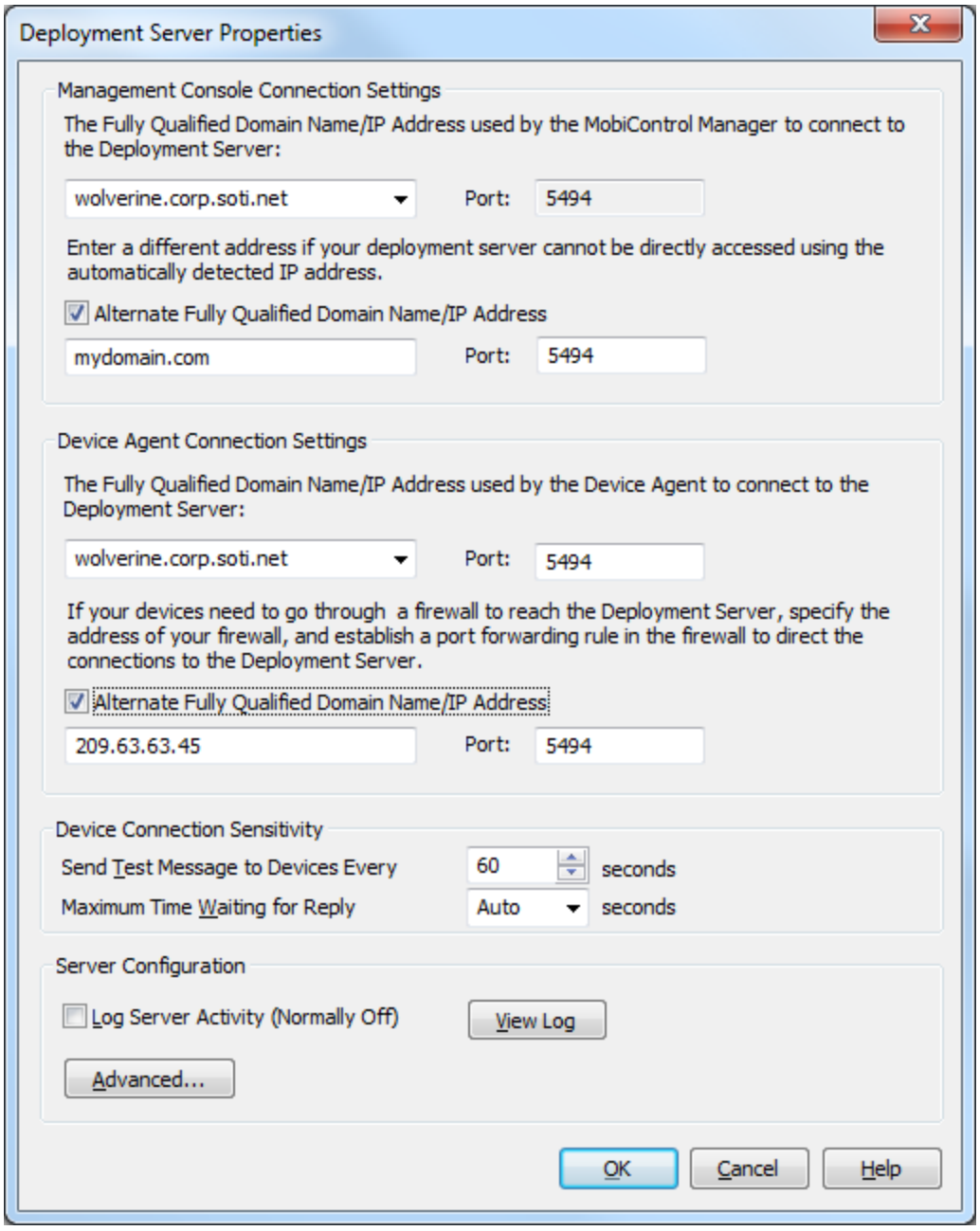
Please see the "Upgrading MobiControl" topic on page 553.

IU4. How do I move my Deployment Server from one machine or server to another?

You need to ensure that the Device Agents installed on the devices are updated with this information before you move the Deployment Server. To do this, add the IP address of the new Deployment Server as the **Secondary External IP Address** in the Deployment Server properties, while keeping the address of the old Deployment Server as the primary external IP address. Allow the settings to be propagated to the devices. Typically, these settings would be refreshed when a device disconnects and reconnects to the Deployment Server. Once all the devices have the new settings, disable the old Deployment Server (right-click on the Deployment Server and select **Disable** or **Shutdown**). Now, when you enable the new Deployment Server on the new server, the devices would be able to connect to the new Deployment Server (after they fail to connect to the old Deployment Server). After all your devices have connected, you can specify the IP of the new Deployment Server as the primary external.

If you are moving from your test server to a production server, we recommend that you create a brand new database:

1. Run the MobiControl installation file and install the new database on the new computer.
2. Launch MobiControl Manager when it is done.
3. Open the **Tools** menu and click **Options.**
4. Click the **Connection** button.
5. Change the appropriate settings in this window to point to the new server.



Connectivity

C1. I created an add device rule, generated a Device Agent, and installed it onto my mobile device. Why doesn't it seem to connect to MobiControl?

The most common reason why a MobiControl Device Agent cannot connect to a MobiControl Deployment Server is because there is a firewall between the device and the Deployment Server that is blocking the connection attempt from the device. By default, MobiControl Device Agents open TCP/IP connections to Deployment Servers on port 5494. If this port is being blocked by an intermediate firewall—personal or corporate firewall—then the device will not be able to connect to the server.

A **personal firewall** is one that on the computer that is running the Deployment Server. For example, the Windows firewall (typically running by default) blocks several TCP/IP ports including port 5494. If you are running a Windows or other firewall on a computer that is running a MobiControl Deployment Server, make sure that TCP/IP port 5494 is not being blocked.

If your devices are external from your corporate network and need to go through a **corporate firewall** to get to MobiControl Deployment Server(s), you will probably need to configure **external IP address(es)** for Deployment Server(s) and then set up firewall rules to map the connections from devices to internal Deployment Server IP addresses. The following steps describe how to configure external IP addresses for your Deployment Servers:

1. In MobiControl Manager, go to the Deployment Servers view (tab), right-click on the **Deployment Server** icon for a particular server, and select **Properties.**
2. In the **Deployment Server Properties** dialog box, enter the external IP address and port and click **OK.**

If you have multiple Deployment Servers, you need to configure a different external address for each server. Once you have configured external addresses, you need to generate new MobiControl Device Agents and install them on your mobile devices. The Device Agents will now use the external addresses to connect to Deployment Servers. To be able to establish remote control sessions to external mobile devices or devices whose IP addresses are not public, you need to set the MobiControl remote control profile for your devices to **TCP/IP (SERVER).** (The default remote control connection profile setting is just **TCP(IP).**) You can set the default remote control connection profile when creating device configuration rules or by right-clicking on a device group or device in the MobiControl Manager device tree and selecting the **Configure Device(s)** menu option.

NOTE:

MobiControl Deployment Servers always listen for connections on TCP/IP port 5494; this "internal" port is currently fixed. The Deployment Server properties dialog box in MobiControl Manager allows you to change both the external IP address and the external port for Deployment Servers. If you do assign external IP addresses and ports for your servers, you must create a firewall/proxy server rule to map the external address to the internal IP address and port (5494) of your Deployment Server computers.

EXAMPLE:

If you have configured a Deployment Server as follows:

Deployment Server External IP:Port = 209.151.100.111:2000
Deployment Server Internal IP:Port = 192.168.1.11:5494

You will need to configure a firewall rule to map the external TCP/IP address 209.151.100.111:2000 to the internal TCP/IP address 192.168.1.11:5494 of the Deployment Server computer.

C2. Is there a way to troubleshoot or test to see if my devices can successfully connect to Deployment Servers?

Here is how to test if the MobiControl Device Agent that is installed on a device can connect to a MobiControl Deployment Server:

1. Click on the **MobiControl** icon in the system tray of the device (in the bottom, right-hand corner of the home screen).
2. From the displayed menu, select the **Configure** menu item.
3. In the Configuration tool, select the **Sync** tab.
4. In the **Deployment Server(s)** section of the **Sync** tab, select the address of a server (i.e. tap on the address) and then click the **Test** button. A dialog box will be displayed that shows the status of the connection test as it proceeds.

If you have multiple Deployment Servers configured, you can repeat the above test for each Deployment Server in the list.

C3. What settings should I use for slow connections?

You can set the device connection sensitivity **Send Test Message to Devices Every** value to 60 seconds in the Deployment Server tray applet. This setting is used to control how often the Deployment Server is to check connections to devices to see if they are working properly. The Deployment Server does this by sending a test message to the device. When the device receives the test message, it sends the message back to the server. If the server does not receive the test message back within a certain time, it will terminate the connection to the device.

Another setting that will help slow connections is one that reduces the colors sent in images, which consequently reduces the amount of data that needs to be sent. You can change the remote control connection settings to view the device display in 16-color grayscale or 4-color grayscale instead of the default full-color display. Please see R1. What settings should I use to remotely manage and establish remote control sessions to devices over cellular (e.g. GPRS) or dial-up connections? below for more details.

C4. Do dynamic IP addresses present a problem for MobiControl?

A dynamic IP address automatically assigned to a host by a DHCP server is not a problem for MobiControl.

Device Agent

A1. I installed the Device Agent on my device but it is not showing up in the device tree. How can I make it appear?

Once the MobiControl Device Agent has been installed on your mobile device, click the **MobiControl Device Agent**icon on your mobile device. In the pop-up menu, select **Configure.** When the Device Agent menu comes up, on the General tab, you will see the Status field. If it says disconnected, click the **Connect** button to establish a connection with the MobiControl Deployment Server.

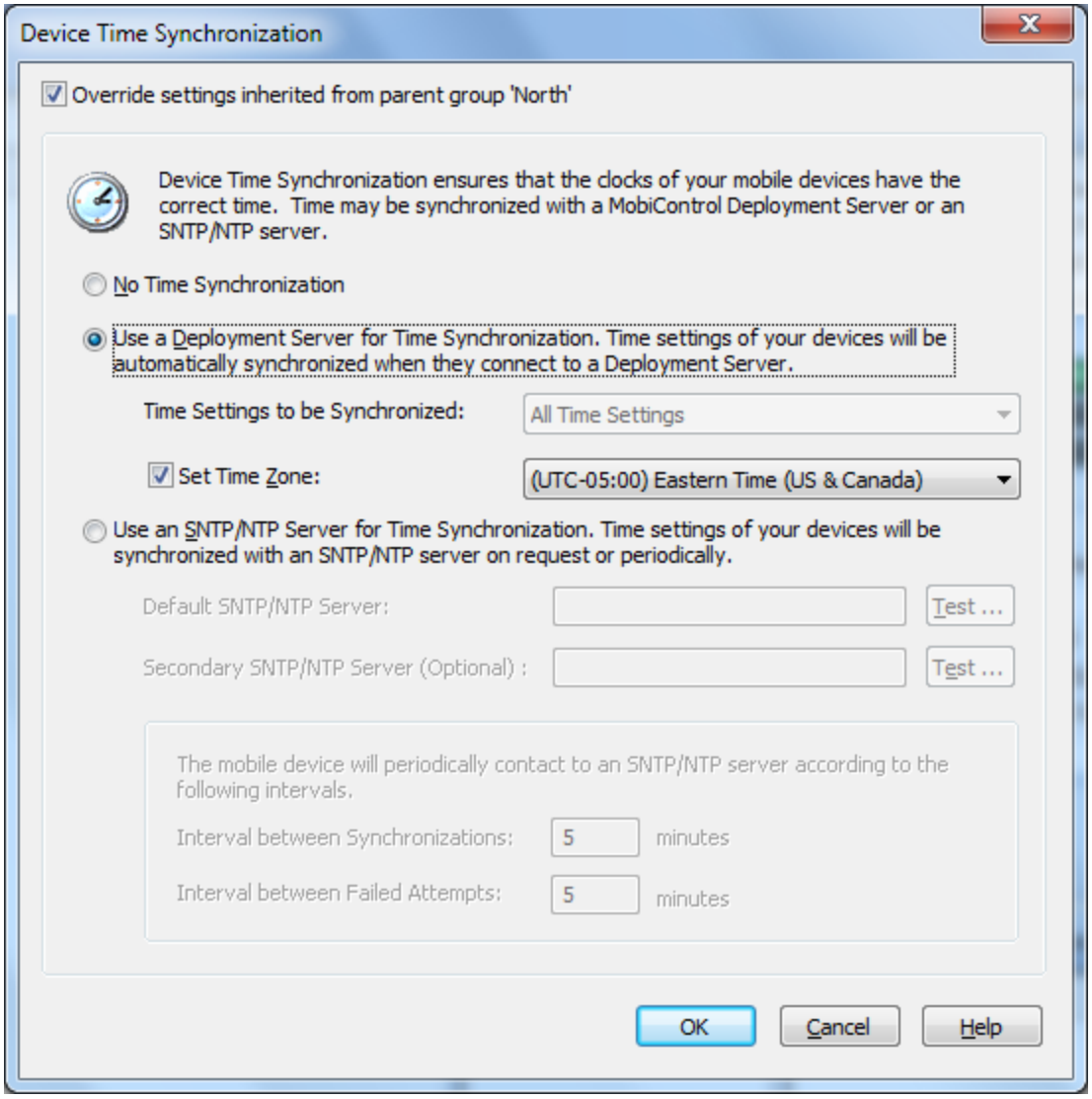
If the status shows "Connected," check MobiControl Manager to see if your mobile device is showing up or not. Once the connection is made, it can take a few minutes for the mobile device to show up in MobiControl Manager.

If the status shows "Disconnected" and nothing happens after clicking the **Connect** button, then the mobile device is not being able to connect with the Deployment Server. Click the **Servers** tab to verify that the server information is correct. If it is correct, select that entry and click **Test**. The test should complete successfully. If it does, go back to the **General** tab and click **Connect**. If the Deployment Server test fails, verify the Deployment Server information and make sure that the Deployment Server is running. If the Deployment Server information is not correct, please correct it.

A2. How can I make sure that the clocks on my mobile devices have the proper time?

MobiControl supports two forms of time synchronization: **Sync Time with MobiControl Deployment Server** and **Sync with SNTP/NTP Time Server.**

Sync Time with MobiControl Deployment Server: When you enable this option, the MobiControl Device Agent will synchronize the device clock with the Deployment Server clock each time it connects to a Deployment Server. To use this option, you must enable the device time synchronization settings for a device (or group of devices). In the device tree, select the device or group, then select **Configure Device (s)** from the **Device** menu, and then select **Time Synchronization.**



Device Time Synchronization Settings

Sync with SNTP/NTP Time Server: This option uses the SNTP/NTP time synchronization protocol to synchronize the clock on your mobile devices with a public or private SNTP/NTP time server. You can configure this option using the MobiControl Manager. The most common problem with this form of time synchronization occurs when there is a personal or corporate firewall between your mobile device(s) and the time server. To correct this problem, please make sure that connections from your mobile device(s) through UDP port 123 are not being blocked by a firewall. Please see the "Device Time Synchronization" topic on page 173 for more information on this topic.

A3. Why is the MobiControl Device Agent changing the server host name/IP address information that I am configuring on the device?

The Device Agent is not changing the host name/IP address information on its own. It is the MobiControl Deployment Server that is sending what it believes is the correct address information to the device and asking the Device Agent to update its address information.

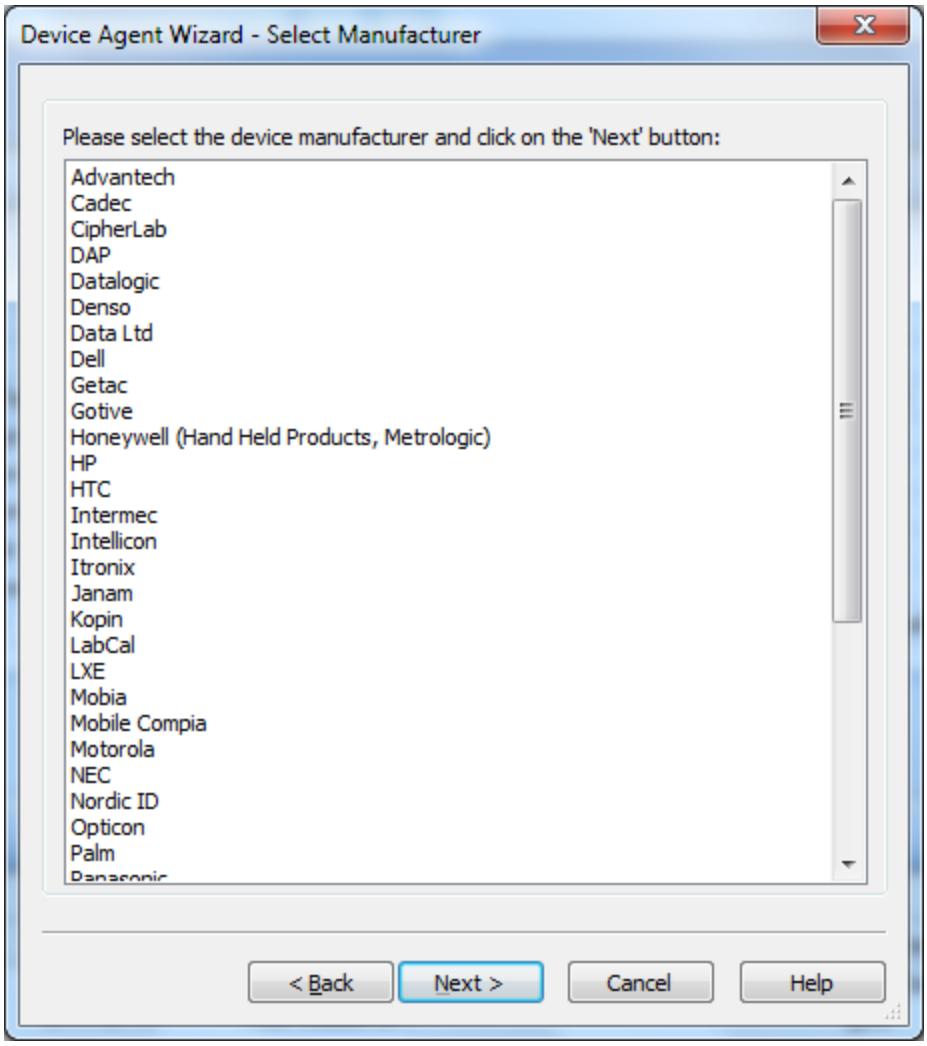
When a device connects to a server, the server sends the device what it believes to be the addresses of MobiControl Deployment Servers. The MobiControl Device Agent then stores the server address information it receives and overwrites the previously configured address information. In order for changes to the host name/IP information to stay, you need to configure this with MobiControl Manager:

1. In MobiControl Manager, go to the Deployment Servers view (tab).
2. Right-click the icon of the Deployment Server whose address information you want to change, and select the **Server Properties** menu item.
3. On the Server Properties dialog box, set the host name/IP address information as needed in the **Primary** or **Secondary External IP Address** fields.
4. Click **OK** to save the changes. MobiControl Deployment Servers will now send the updated information to devices when they connect.

A4. Can I use MobiControl to manage my Windows-based computers, laptops, tablet PCs? If so, how can I create the agent?

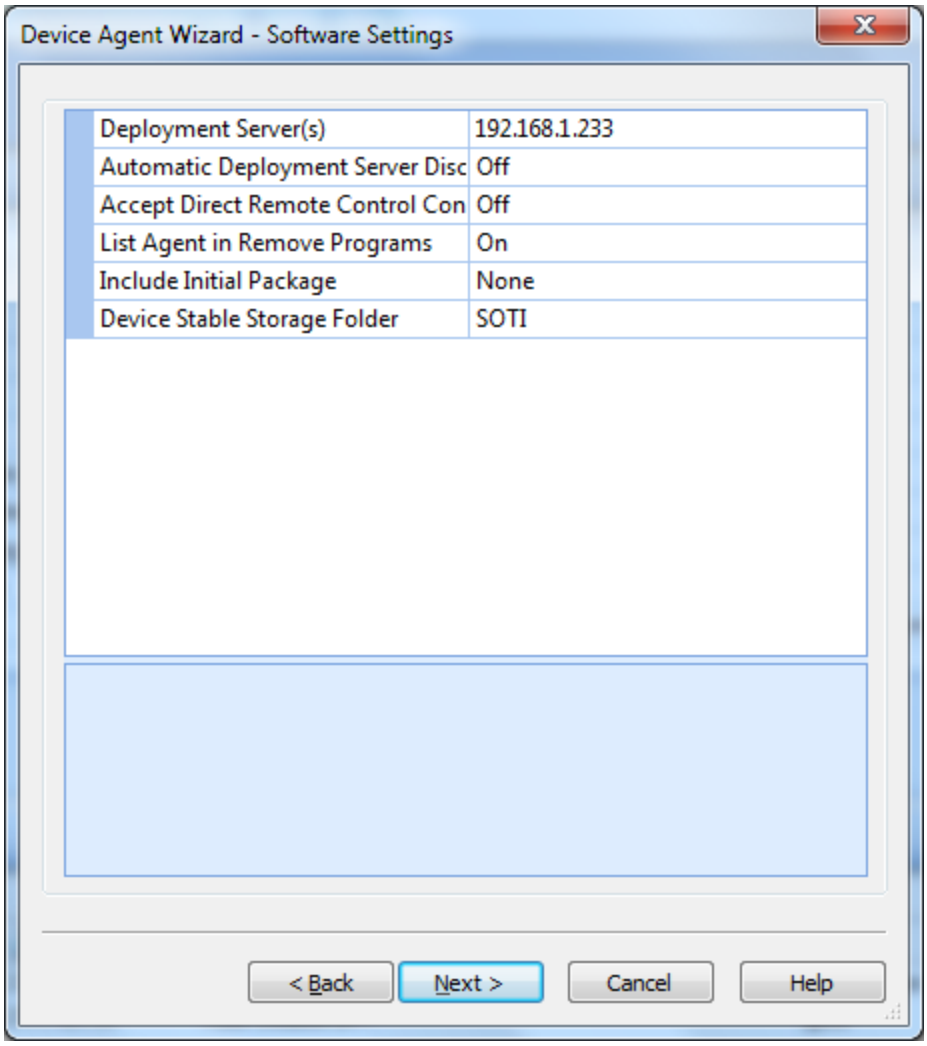
You can use MobiControl to manage your laptops, tablet PCs, and even your workstations. You can have the Device Agent installed on these devices and manage them as you would manage your other mobile devices with MobiControl Manager.

You can create the Device Agent using the Device Agent Manager as you would for any other mobile device. When you are creating the Device Agent, select Microsoft Windows 2000/XP/ Embedded (computers/laptops/thin clients)as the device manufacturer.



Microsoft Windows-based Device Agent

Once this is selected, you will notice that you have now skipped some steps in the Device Agent Manager. The next screen will ask you for various software settings.



Microsoft Windows-based Device Agent

Follow the remaining steps and once the Device Agent has been created, you are now ready to have it pushed out to your computer, laptop, or tablet PC.

IMPORTANT:

The MobiControl Device Agent for Microsoft Windows PC's cannot be installed on the same machine as the MobiControl Deployment Server.

The Device Agent and Deployment Server processes (McAgent and McDeplSvr) both listen on port 5494 for activity. This will cause a constant conflict as each process attempts to use the port.

Remote Control

R1. What settings should I use to remotely manage and establish remote control sessions to devices over cellular (e.g. GPRS) or dial-up connections?

Cellular and dial-up connections are typically low bandwidth (slow) connections. The information in this section applies to low bandwidth connections but also to other forms of connections such as Wi-Fi.

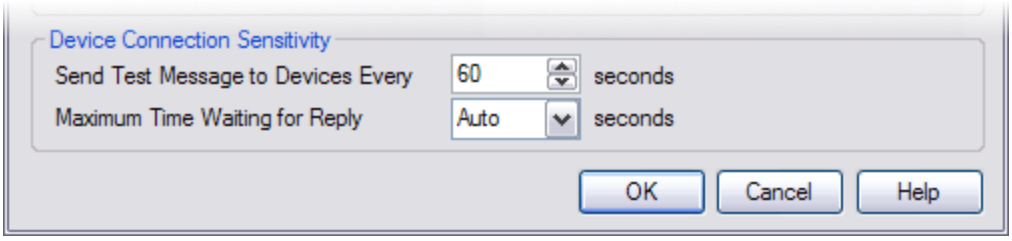
Two of the main factors that affect **battery consumption** on mobile devices are the device screen and the device radio. Most devices include a control panel applet to adjust screen power consumption. We recommend that you adjust the screen settings to minimize power consumption based on your usage patterns. To limit the amount of power consumed by Wi-Fi and/or cellular radios, you need to minimize the amount of data sent and received by radio(s). The information in this section describes how to minimize the amount of data sent and received by MobiControl Device Agents.

Carrier charges can also be an issue. If you are using a cellular connection (e.g. GPRS/EDGE), your carrier may be billing you based on the amount of data that you send or receive through their network. The information provided below describes various MobiControl settings that can be tuned to minimize the data transmitted on cellular networks.

Device to Server Connectivity Settings

- Device Connection Sensitivity

  MobiControl Deployment Servers send test messages (32 bytes) to devices periodically and then wait for the device to send the message back. If a Deployment Server does not receive a test message back within a specified time, it concludes that the connection is not functioning properly, and closes the connection to the device. For slow connections or when you are being charged based on your amount of data you send through the network (e.g. some cellular plans) we recommend that you set the Deployment Server **Send Test Message to Devices Every** option to 300 seconds in the Deployment Server **Properties** dialog box.



- Device Connection Mode

  MobiControl provides three connection mode settings that allow you to control the time period during which MobiControl Device Agents are connected to servers. In order to conserve battery power or to reduce cellular data charges, you can reduce the time period that devices are connected to server(s). The three connection modes provided are Persistent, Scheduled, and Manual. By default, the MobiControl Device Agents use the Persistent connection mode and try to maintain a connection to a Deployment Server whenever network connectivity exists. The Scheduled connection mode allows a connection to a server to be maintained only within a specified time window (e.g. 09:00 to 17:00). Scheduled mode can also be used to take advantage of a cheaper or higher bandwidth network that is only available during specific hours. The Manual connection mode does not maintain a connection to the server. In this case the device user needs to explicitly initiate a connection from the mobile device when required. This mode can be used in situations where connectivity is only required to support users. In this case, when an end user needs support and wants the help desk to remote control the device, the connection can be initiated from the device at that time.

- Device Update Schedule

  The update schedule determines how often server(s) check devices to ensure that they have the required software packages and configuration settings installed. The update schedule is also used to refresh the information shown in the Info panel in the MobiControl Manager Devices view (tab) (e.g. battery or memory indicators, custom data). By setting the schedule to be less frequent network traffic and device battery consumption can be reduced. Typically the update schedule should be set for once a day at an off peak hour, or once every two or three days.

- File Sync Schedule

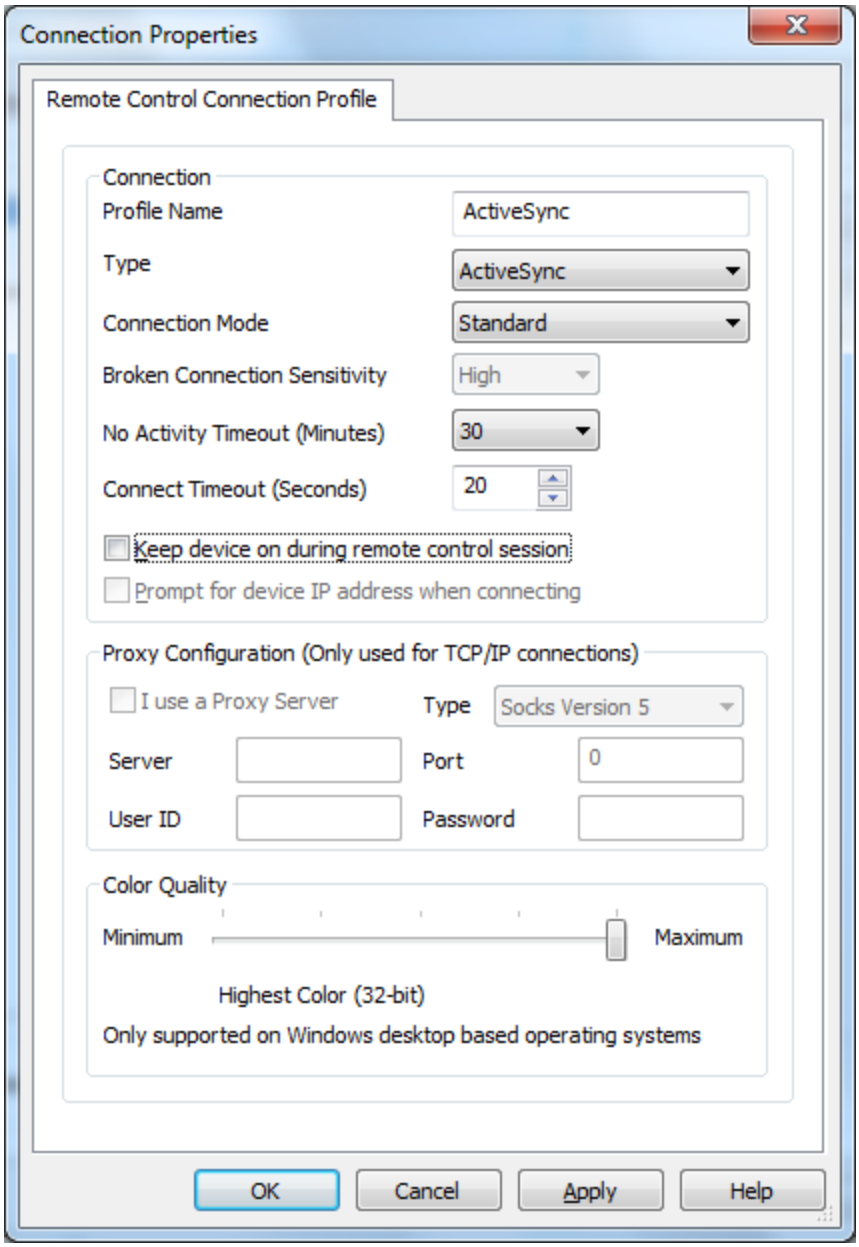
  A file sync schedule is used when a file sync rule has been configured for synchronizing data files between devices and the server. A file sync schedule determines how often data files are to be synchronized with mobile devices. The file sync schedule can be used to control when large files are transferred. File sync schedule can be configured to take advantage of high-bandwidth Wi-Fi connections and avoiding GPRS data usage during peak hours. It is important to note that even when all files are synchronized, the activity involved in checking to see if files need to be synchronized generates some data traffic. Typically, a file sync schedule should be set to synchronize once a day at an off peak hour, or once every two or three days.

For remotely controlling devices over slow networks, MobiControl provides options to reduce the amount of data that is sent over these networks. A second characteristic of these sorts of connections is that the IP address of the device is often private, meaning that MobiControl remote control desktop software will not be able to initiate a TCP/IP connection to the device. To deal with the private device IP address issue MobiControl has a TCP/IP(SERVER) setting which allows MobiControl to use a connection initiated by the mobile device for remote control purposes.

The following table summarizes the various options available for establishing remote control sessions to mobile devices over slow connections and also devices that have private IP addresses:

Field Name	**Recommended Setting**	**Description**
Type	TCP/IP (SERVER)	GPRS or dial-up connections often have private addresses for mobile devices connected over these networks. When the addresses for devices are private you need to set the **Connection Type** field to "TCP/IP (SERVER)" in the remote control profile you are using.
Broken Connection Sensitivity	Low	This field reflects the responsiveness of the connection. Setting the field to "Low" indicates to the software that the connection is generally slow and to expect lags in waiting for responses. Since GPRS and dial-up connections are generally slow, setting the value of this field to "Low" is usually appropriate. The software will in this case wait extra long periods of time waiting for responses.
Connect Timeout	45	Since GPRS and dial-up connections are generally slow, setting the value of this field to 45 seconds allows extra time for a connection attempt to complete.
Color Reduction	2 bit (4-shade grayscale)	Reducing the colors sent in images further reduces the size of the data that needs to be sent on slow networks. You can change the remote control connection settings to view the device display in 16-color grayscale or 4-color grayscale instead of the default full-color display. Although the amount of data transferred will be reduced, CPU usage on the device will increase.

You can edit one of the existing remote control profiles and make the changes listed above or create a new profile. The MobiControl installation software creates a remote control profile called TCP/IP (SERVER) by default. It can be edited.



Once the changes have been made, right-click on the device or device group (if you want to use the profile for a group of devices) in MobiControl Manager and make sure that the remote control profile you just edited is configured for use.

NOTE:

When attempting remote control sessions to devices from outside a firewall (i.e. device located on the inside) or to devices on cellular networks that assign devices with private IP addresses, the MobiControl TCP/IP (SERVER) connection type must be used. The TCP/IP (SERVER) connection type allows devices with private IP addresses to be remote controlled by using connections initiated by mobile devices for remote control purposes. If the devices and the MobiControl Manager console are both on the same network the TCP/IP (DIRECT) remote control profile can be used.

R2. How can I use MobiControl to manage and/or remote control devices whose IP address is not reachable or not public (i.e. external or private addresses) as is often the case for GPRS connections?

The MobiControl desktop software does not need to initiate connections to devices, instead the MobiControl device software connects to servers. If the MobiControl Device Agent software is installed on a mobile device, it will attempt to connect to a Deployment Server and maintain that connection. In this way the desktop software does not need to connect to the device, it just uses the connection that the device software maintains to the server. Since the desktop software does not need to initiate connections to devices, dynamic device addresses are also not a problem.

MobiControl also allows external IP addresses and ports to be assigned to Deployment Servers. In this way devices can connect to external addresses that then get mapped to internal addresses and ports by firewall or proxy software. When initiating remote control sessions to devices with private addresses you need to use the TCP/IP (SERVER) connection profile. TCP/IP (SERVER) remote control sessions use device-initiated connections to provide remote control, in this way remote control sessions go through an intermediate MobiControl Deployment Server. In situations where devices do not have private addresses, using regular TCP/IP remote control profiles allows direct connections to devices with no intermediate servers. If a regular TCP/IP remote control profile is used, the connection is initiated from the desktop software.

R3. I need to remote control a device that is in the sleep or standby mode and is currently offline. How can I wake up the device and force it to connect to MobiControl?

If your mobile device is not showing up as online in MobiControl Manager and you want to establish a connection, you can do so with MobiControl's **Send SMS (to initiate connection to MobiControl)** feature. (Please see the "Sending Messages / Scripts" topic on page 136.) It may be that your mobile device is in a suspended state (sleeping), or the data connection is not active. With the **Send SMS (to initiate connection to MobiControl)** feature, you can wake up the mobile device, activate the data connection, and have the mobile device connect to MobiControl.

R4. Why do I get a Rapi initialization timeout error when I try to remote control my mobile device?

Rapi Connection Error

When you receive the connection error "Rapi initialization timeout error" while trying to connect to your mobile device, it means MobiControl cannot communicate with Microsoft ActiveSync or WMDC and your mobile device. To resolve this error make sure you have your mobile device properly connected to your computer and to ActiveSync or WMDC.

Security

S1. How do I put pictures into my lockdown menu?

Lockdown menus are based on HTML template files. When you install MobiControl several sample template files are installed into the system. To create a lockdown menu screen with your own custom look and feel, open up one of the existing template files, and save it to a different file name. You can then edit the saved HTML template file and give it your own style. If you want to display images in the menu, then you need to make sure that the image files are located in stable storage on your mobile device. MobiControl does not automatically copy images referenced in template files to mobile devices. You can copy the images to your mobile devices either manually via a File Explorer tool, or you can get the images to your devices by using deployment rules or file sync rules. The destination location for images needs to be in stable storage. The image files can be referenced by their absolute path on the mobile devices that they reside on. Once you have finished creating your HTML template file, add the new template to MobiControl and then use it to configure lockdown rules. Please see the "Device Lockdown" topic on page 201 and the "Customizing Lockdown Program Menu Templates" topic on page 217 for more information about creating and customizing template files.

S2. How can I restrict what a user of the MobiControl Manager console can do?

MobiControl includes a security system that integrates with your existing Windows Domain security system (Microsoft Active Directory). You can configure permissions for your domain users, and MobiControl will allow or disallow access to specific functionality based on the permissions configured for the currently logged in user. Please see the "Manager Console User Security" topic on page 409 for more information.

Package Creation and Deployment

PD1. How do I deploy registry settings?

To deploy software, data or settings to your mobile devices, you need to create a package and then create a MobiControl deployment rule to send the package to your devices. To create a package, to use the MobiControl Package Studio tool, accessible from the **Tools** menu in MobiControl Manager. (Please see the "MobiControl Package Studio" topic on page 413.) To initially generate the registry file that you want to deploy, open a MobiControl Remote Control session to a device that has the proper registry settings, then, using the remote control Registry tool, export the registry settings to a `.reg` file. Once the `.reg` file has been created, create a package using Package Studio, browse to your registry file and add it to your package, and then build the package using the Package Studio **Build** menu open. Package Studio recognizes certain file types such as registry files and sets these files to auto-execute by default when they are installed onto mobile devices. Once the package is built, in MobiControl Manager create a deployment rule to deploy the package to your mobile devices.

PD2. Do I need a second Deployment Server?

There are three reasons why you may want to add an additional MobiControl Deployment Server:

1. Scalability

   When you are running multiple Deployment Servers, MobiControl will distribute the load among functioning servers. This means that if your existing server(s) are getting too loaded down, you can add additional servers to distribute the load amongst the servers. When connecting to servers, devices will distribute themselves amongst servers in order to balance the load across the servers.

2. Fault Tolerance

   When you are running multiple Deployment Servers, if a particular server fails, or a server is down for maintenance, MobiControl will automatically move devices that were connected to the disabled server onto other functioning servers. When the server is available again, the system will start balancing the load to move load off other servers onto the available server. This feature means that all devices can be fully manageable even while one or more servers are not operating.

3. Bandwidth Management

   In situations where an organization has remote sites, each of which has several mobile devices, placing Deployment Servers at each site can mean less bandwidth consumption between the head office and the remote sites and an overall increase in performance of the system. If there is only one centrally-located Deployment Server, each package delivery must be sent from the central server over the slow connection to each remote mobile device.

   Imagine a company with ten remote sites, each with one hundred devices, and the connections between the central office and the sites being very slow or having limited bandwidth availability. To deliver a package, there would be 1000 deliveries from the central location to the remote devices over the slow connection. This would be very slow and would consume available bandwidth between the sites and the central location. However, if there is a server at each site, the package will be sent once to each site (i.e. 10 deliveries over the slow connection instead of 1000). Then, the Deployment Server at each site will cache the package and transmit it to each of its local devices over the fast local network.

Our general recommendation is that you do not need to run more than one Deployment Server if you are managing less than 1500 devices, but you need to consider the information provided above, as well as any other network, infrastructure or other requirements your organization may have.

PD3. I am running my application on all my devices. From time to time I have to update some settings in my applications .ini file. I don't want to send the entire .ini file each time, is there a better way?

When you deploy packages with MobiControl, you can insert scripts into your packages. The MobiControl scripting language contains commands that allow you edit `.ini` files. So instead of sending an entire `.ini` file, you can just put in script commands to edit an existing `.ini` file and add or remove entries as needed.

EXAMPLE:

The following command will edit the `mov.ini` file and set the Color value to "Red" in the "Video" section of the file:

```
writeprofstring \Movie\mov.ini Video Color Red
```

Please see the "Script Command Set" topic on page 72 for more information about MobiControl script commands.

PD4. I need to create a script that I will use in the package I deploy to my devices. Is there a way to test the script before I deploy it to my devices?

To test your scripts before putting them into a package, open a remote control session to your mobile device, and then click on the **DOS Screen** tab on the right edge of the remote control session window. If you copy your script to the mobile device file system you can run it by typing in the name of the script file at the prompt. When the script is executed you will see each line of the script execute in the DOS window. You can also test out individual script commands by typing them at the prompt.

PD5. Does MobiControl support a fault tolerance Deployment Server?

For added fault tolerance, MobiControl provides the capability to add multiple Deployment Servers to ensure high availability and minimize downtime. With multiple Deployment Servers, you can set different Deployment Server priorities for your devices. If the priority 1 server is down, the devices would automatically connect to the priority 2 server. The multiple Deployment Servers can run in an Active/Active or Active/Standby mode, configurable from within MobiControl. You can even specify multiple external IP addresses for the devices to connect to. If the devices are not able to connect to the first IP, they would try to connect to another IP where a backup Deployment Server can service the requests. An additional server license is required for Deployment Server fault tolerance.

Scripts

SC1. Are there any APIs (Application Programming Interfaces) available so that I can call and execute a MobiControl scripts from a custom application?

Yes, you can call a MobiControl script from a custom application; you need to use `Commloader.exe` with a switch to execute scripts. Please see the "Tips and Tricks" topic on page 1511 for more information.

Database

D1. What are recommendations for doing backups?

We recommend that you do a backup as often as possible. If you are running MobiControl v2.06 or earlier, you need to back up your file store and your database. If you are using MobiControl v3 or later, you only need to back up your database. To back up your file store, use the Microsoft File Explorer to

copy the contents of the file store to a backup folder. To back up your database, if you are using the lightweight Microsoft SQL Server Desktop Engine (MSDE), you may need to purchase a third-party tool. If you are running the full Microsoft SQL Server, you can back up your database using the back up tool provided with Microsoft SQL Server Enterprise Manager. Most database back up tools provide an automated backup system so that your database will be automatically backed up at regular intervals.

D2. Can I use a third-party reporting tool to generate my own custom reports?

Yes, we can make the schema available. Please contact us for additional information.

MobiControl Tips & Tricks

Q1. Can I execute scripts on the mobile device to accomplish various tasks? If so, what kind of tasks can I accomplish?

There are various options available to you that allow for execution of tasks on your mobile device. The following tasks can be accomplished using `commloader.exe` with any of the following switches.

Switch	Purpose
`-app`	Run `CommLoader.exe` as an application instead of a service. (This is only applicable to an agent running on a Windows desktop platform such as Windows XP.)
`-n <device name>`	Rename a device
`-m <script file>`	Run a script file
`-mm <script command>`	Run an inline script command
`-g`	Reset advanced settings
`-s`	Manual time synchronization
`-connect`	Connect to the Deployment Server
`-connect -connmgr`	Establish data connection (usually GPRS) if no data connection is available, and then connects to the MobiControl server. **NOTE:** This is the same as clicking the Connect button within the MobiControl Agent Applet.
`-connmgr`	Establish data connection only (usually GPRS). It will do nothing if any data connection (e.g. WiFi, GPRS, or ActiveSync) is available. **NOTE:**

Switch	Purpose
	Depending on how the device is configured, it may not open a GPRS connection even if it has the capability to.
`-connect -connmgr -inet`	Establish Internet data connection (usually GPRS) and connect to the MobiControl server. A connection is attempted regardless of any available data connections (ActiveSync, Wi-Fi,etc.)
`-connmgr -inet`	Establish Internet data connection (usually GPRS). It attempts to open a connection regardless of any available data connections (ActiveSync, Wi-Fi, etc.)
`-connmgr -inet -hangup`	Disconnects the GPRS connection. **NOTE:** Does not apply to CDMA devices.
`-disconnect`	Disconnect from the MobiControl Deployment Server
`-install`	Install Windows agent (only applicable to an agent running on a Windows desktop platform)
`-uninstall`	Uninstall Windows agent (only applicable to an agent running on a Windows desktop platform)
`-pfx <pfxfile> -pwd <password>`	Import `.pfx` private key file. Some device may require a soft reset after importing.
`-exit`	Exit the program
`-syncfile`	Checks the Deployment Server to see if there are any files to sync. This switch performs the same operation as though a user were to right-click on a device in the Manager and select 'Sync Files Now'. **NOTE:** Device must be online for this command to complete successfully. It will not attempt to establish a connection if one is not present.
`-syncpkg`	Checks the Deployment Server to see if new packages are available. If packages are available they will be downloaded and installed. This is similar to right-clicking on the device and selecting "Push Pending Packages to Device" **NOTE:** Device must be online for this command to complete successfully. It will not attempt to establish a connection if one is not present.
`-installpkgs`	Immediately proceeds with the installation of ANY packages that it has

Switch	Purpose
	downloaded but not yet installed because they are scheduled to be installed at a later time. **NOTE:** The Package will not show successfully installed in the MobiControl Manager until the device has connected to Deployment Server.

EXAMPLES:

- To force a mobile device to establish a MobiControl connection with the MobiControl Deployment Server: `\windows\startup\commloader.exe -connect`
- To run a custom script (`*.cmd` file) on a mobile device: `\windows\startup\commloader.exe -m 1:\MyScript.cmd`
- To run a custom script (`*.cmd` file) from a lockdown menu, browse for the `.cmd` file in the Add New Menu Item dialog box when configuring the Lockdown Policy. Enter the file's location as the Program Path: `"\windows\startup\commloader.exe, -m %22\MyScript.cmd%22"` **

  ** The purpose of `%22` is to emulate double quotes in the Lockdown menu. This is required when the file name or path has spaces in it.

Q2. How can I force my mobile device to wake up from standby mode and establish a connection with MobiControl?

In MobiControl v5.00, we added a function that allows you to send a message (SMS) to your mobile device which contains instructions that will wake the mobile device from its suspended state and force a connection with MobiControl Deployment Server. In MobiControlManager, right-click on a device and select **Send message to a device** and click **Send message via SMS.** Select **Initiate Connection to MobiControl** as the message type and check the box next to **Activate data connection if not present** if you want to activate the data connection. Please see the "Sending Messages / Scripts" topic on page 136 for more information on sending messages to mobile devices.

Q3. How do I use "custom" information to name my mobile devices (e.g. the device owner's name)?

In MobiControl, a mobile device can have its name based on a custom data value. This naming convention can be enforced once the mobile device has connected to MobiControl or when creating the Device Agent.

EXAMPLE:

At the time of the Device Agent creation, let the agent device name be `%REG://HKEY_CURRENT_USER\ControlPanel\Owner?VN=Name%`

Once the mobile device is online on MobiControl, a script needs to be written, inserted into a MobiControl package and then pushed down to the mobile device(s). The name of the mobile device will change automatically and you will see the new name in MobiControl Manager.

SCRIPT EXAMPLE:

```
Set Temp=REG://HKEY_CURRENT_USER\ControlPanel\Owner?VN=Name
 \Windows\Startup\Commloader.exe -n "%Temp%"
```

For more information about Commloader switches, please see Q1. Can I execute scripts on the mobile device to accomplish various tasks? If so, what kind of tasks can I accomplish? in this section.

Q4. How do I run a MobiControl script on my mobile device every time on startup?

In order to run a script on your mobile device every time on startup, you need to create a `*.lnk` shortcut on your mobile device and place this shortcut in its `\windows\startup\` folder. This `*.lnk` shortcut will contain the instructions for the script to execute upon startup of the mobile device.

A shortcut is a plain text file saved with a `.lnk` extension and contains instructions to perform a task. This task could be launching a process, an application or a file.

To create a `*.lnk` shortcut, follow these steps:

1. Open Notepad.
2. Enter the instructions or commands that you want executed when the shortcut is run. (Please see below for information on these commands.)
3. Save this text file with a `*.lnk` extension, e.g. `MyShortcut.lnk`.
4. Place this shortcut in the `\windows\startup\` folder on the mobile device.

EXAMPLE:

```
NN#\windows\startup\commloader.exe -m "\Temp\MyScript.CMD"<CR>
```

If you wish to have the shortcut point to Windows settings and features, this shortcut is one line of text.

Command	Description
`nn#`	The "`nn`" variable represents the total size, in characters (including spaces) in the line of text following the # (pound) sign.
`Commloader.exe`	This is the program to be executed. It will always be the same for feature settings.
`i`	This is the index number of the feature setting you wish to run. Refer to the table below for the index numbers of the settings.
`0`	This represents the optional tab number to select.
`<CR>`	This represents a carriage return. Instead of a true carriage return, today we press the ENTER key. (In other words, don't include the literal in your file.)

SAMPLE CONTROL PANEL .LNK FILE:

```
nn#\windows\ctlpnl.exe cplmain.cpl,i,0<CR>
```

For a full list of the Control Panel options, please see Q5. How do I create shortcuts to Windows settings or features on my mobile device, with a lockdown menu? in this section.

EXAMPLE:

If you are trying to enter the memory settings, you will notice there are three tabs at the bottom. When entering
`ctlpnl.exe cplmain.cpl,4`
this will open the Memory main tab in the memory settings, but if you enter
`ctlpnl.exe cplmain.cpl,4,1<CR>`
this will open the next tab in the Memory settings, which is storage card. If there are more tabs, use the next corresponding number. Tab numbering starts with zero.

Q5. How do I create shortcuts to Windows settings or features on my mobile device, with a lockdown menu?

To create a shortcut to a Windows setting, you can create a `*.lnk` as noted above, or you can create a shortcut within a lockdown menu.

To create a shortcut in the MobiControl lockdown menu (Please see the "Device Lockdown" topic on page 201.) the format is `windows\ctlpnl.exe, cplmain.cpl i 0`.

Index Number	Opens	Example
1	Password settings	`ctlpnl.exe, cplmain.cpl 1`
2	Owner Information settings	`ctlpnl.exe, cplmain.cpl 2`
3 *	Power menu from settings\system	`ctlpnl.exe, cplmain.cpl 3`
4	Memory menu from the units settings	`ctlpnl.exe, cplmain.cpl 4`
5	About menu from the units settings\system	`ctlpnl.exe, cplmain.cpl 5`
6 *	Backlight settings (for only certain devices)	`ctlpnl.exe, cplmain.cpl 6`
7	Screen Calibration settings	`ctlpnl.exe, cplmain.cpl 7`
8	Input settings	`ctlpnl.exe, cplmain.cpl 8`
9	Sounds and Notifications settings	`ctlpnl.exe, cplmain.cpl 9`
10	Remove Programs menu from the units \settings\system	`ctlpnl.exe, cplmain.cpl 10`
11	Menus settings	`ctlpnl.exe, cplmain.cpl 11`
12	Buttons settings	`ctlpnl.exe, cplmain.cpl 12`
13	Today settings	`ctlpnl.exe, cplmain.cpl 13`
14 *	PC Connections settings (works only for certain devices)	`ctlpnl.exe, cplmain.cpl 14`
15	Beam settings	`ctlpnl.exe, cplmain.cpl 15`
16	Clock and Alarms settings	`ctlpnl.exe, cplmain.cpl 16`
17	Configure Network Adapters settings	`ctlpnl.exe, cplmain.cpl 17`
18	Regional Settings settings	`ctlpnl.exe, cplmain.cpl 18`
19	Connections settings	`ctlpnl.exe, cplmain.cpl 19`
20	Phone settings (for only certain devices)	`ctlpnl.exe, cplmain.cpl 20`
22	Manage Certificates settings	`ctlpnl.exe, cplmain.cpl 22`
23	Settings and Bluetooth tabs settings Tabs are numbered: 0, 1, 2, 3,…	`ctlpnl.exe, cplmain.cpl 23`

NOTES:

- Do not forget the comma. It is necessary to separate the command from its parameters. The examples described here are to be used in scripts only. If you wish to use these examples in the lockdown menu, or a `.lnk` file please refer to the syntax mentioned above.
- If the particular program you wish to set up with a shortcut has several tabs for its settings, adding "`1`" or "`2`" after the defined number would enter the next tab.
- The options mentioned above are general options and may not work on some devices.
- The options marked * are not supported on Pocket PC 2003 O.S.

Q6. How can I send custom message to the MobiControl Deployment Server?

In MobiControl, you can have custom messages send back to the MobiControl Deployment Serverfrom the mobile device. This message will show up in the Log panel of the mobile device in the Devices view (tab) in MobiControl Manager.

Command	Description
`log <type> <message>`	**`<type>`** is the type of message that should get associated. The options are error (`-e`), warning (`-w`), and information (`-i`). `<message>` is the message that will be displayed in the device log in MobiControl Manager.

Command Execution

The only way to run this `log` command is to insert it into a script (`*.cmd`) file. Inside the script, you can specify the `log` command to send messages to the MobiControl Deployment Server during certain activity or at certain actions.

EXAMPLE:

During an software push from MobiControl to your mobile device, you can use this command to send notification to the MobiControl at certain intervals during the software push.

```
log -i "Starting software push"
```

MobiControl Troubleshooting Guide

Q1. I created an add devices rule, generated a Device Agent, and installed it onto my mobile device. Why does it seem not to get connected to MobiControl?

The most common reason why a MobiControl Device Agent cannot connect to a MobiControl Deployment Server is because there is a firewall between the device and the Deployment Server that is blocking the connection attempt from the device. By default, MobiControl Device Agents open TCP/IP connections to Deployment Servers on port 5494. If there is an intermediate firewall (i.e. personal firewall or corporate firewall) between the device and the Deployment Server that is blocking the connection, the connection attempt will fail.

A **personal firewall** is one that is running on the computer that is running the Deployment Server. For example, the Windows XP firewall (typically running by default) blocks several TCP/IP ports including port 5494. If you are running a Windows XP or another firewall on a computer that is running a MobiControl Deployment Server, make sure that TCP/IP port 5494 is not being blocked.

If your devices are external from your corporate network and need to go through a **corporate firewall** to get to MobiControl Deployment Server(s), you will probably need to configure external IP address(es) for Deployment Server(s) and then setup firewall rules to map the connections to the external addresses to the internal Deployment Server IP addresses. To configure external IP addresses and ports for your Deployment Servers:

1. In MobiControl Manager, go to the Deployment Servers view (tab), right-click on the Deployment Server icon for a particular server, and select **Properties.**
2. In the **Deployment Server Properties** dialog box, you can enter external IP addresses and ports. Once you have configured alternate addresses, all MobiControl Device Agents that you create after that point will use the external IP addresses and ports to connect.

If you have multiple Deployment Servers, you need to configure a different external address for each server. Once you have configured external addresses, you need to generate new MobiControl Device Agents and install them on your mobile devices. The Device Agents will now use the external addresses to connect to Deployment Servers. To be able to establish remote control sessions to external mobile devices and/or devices whose IP addresses are not public you need to set the MobiControl remote control profile for your devices to "TCP/IP(SERVER)." The default remote control connection profile setting is "TCP(IP)." You can set the default remote control connection profile when creating add devices rules or by right-clicking on a device group or device in the MobiControl Manager device tree and selecting the **Configure Device(s)** menu option.

NOTE:

MobiControl Deployment Servers always listens for connections on TCP/IP port 5494, this "internal" port is currently fixed. The **Deployment Server Properties** dialog box in MobiControl Manager allows you to change both the external IP address and the external port for Deployment Servers. If you do assign external IP addresses and ports for your servers, you must create a firewall/proxy server rule to map the external address to the internal IP address and port (5494) of your Deployment Server computers.

EXAMPLE:

If you have configured a Deployment Server as follows:

Deployment Server Primary External IP = 209.151.100.111, Port = 2000
Deployment Server Internal IP = 192.168.1.11, Port = 5494

You will need to configure a firewall rule to map the external TCP/IP address 209.151.100.111:2000 to the internal TCP/IP address 192.168.1.11:5494 of the Deployment Server computer.

Please also see the answer to Q5. What are the files associated with MobiControl at the desktop level and at the mobile device level? below.

Q2. Is there a way to troubleshoot or test to see if my devices can successfully connect to Deployment Servers?

To test if the MobiControl Device Agentthat is installed on a device can connect to a MobiControl Deployment Server:

1. Click on the **MobiControl** icon in the system tray of the device.
2. From the displayed menu, select **Configure.**
3. In the **Configuration tool**, select the **Servers** tab.
4. In the **Deployment Server(s)** section of the **Servers** tab, select the address of a server (i.e. tap on the address) and then click on the **Test** button. A dialog box will be displayed that shows the status of the connection test as it proceeds.

NOTE:

If you have multiple Deployment Servers configured you can repeat the above test for each Deployment Server in the list.

Q3. Why do I receive a "No matching add devices rule" message from MobiControl when my device tries to connect to a Deployment Server?

If you created an add devices rule, generated a Device Agent, installed the agent onto a device, then deleted or disabled the add devices rule that you previously created, you will get this message.

When you generate a MobiControl Device Agent from an add devices rule, the rule ID of that add devices rule is embedded into the generated Device Agent. When you install the agent onto a device, it will send that rule ID to the server, and the server will use the rule ID to look up the particular add devices rule to configure the device accordingly.

If you delete or disable the add devices rule, when the agent on the device sends the rule ID up to the server, the server will not find the rule, and will notify the Device Agent of the problem. In this case the Device Agent will display the "No matching add devices rule" message. Once you create an agent from a rule, you need to keep the rule till all of your devices have been configured.

If the add devices rule is disabled, just enable it. If you have deleted the add devices rule, you can create a new rule and then generate a new agent and use the new agent on all of your devices. It is also possible to create a new "open" add devices rule. An open add devices ruleis configured to allow configuration of any agent; it skips the rule ID check). To configure an open add devices rule, you need to use the **Advanced Settings** button when configuring the rule. If you configure an open add devices rule it will work with any existing Device Agent. If you create an open add devices rule you should disable any other add devices rules that you may have.

Q4. I'm trying to deploy an executable to the device, but the deployment fails because the application is running. What can I do?

When you deploy packages with MobiControl, you can insert scripts into your packages. There are two types of scripts: pre-install scripts and post-install scripts. Pre-install scripts are executed before the package files are installed onto the device, post-install scripts are executed after the package files are installed. In this case you can add a pre-install script with specific commands to terminate the executable file (application) that is running on the device before installing the new executable file. You can also use the "`kill`" script command to terminate a running executable.

Q5. What are the files associated with MobiControl at the desktop level and at the mobile device level?

If any file from the list above is missing in the device, then the MobiControl Device Agentinstallation did not complete successfully. Please re-install the agent on the mobile device.

Files Where a Management Consol or Deployment Server are installed

File name	Information	File Name	Location
Deployment Server Log File	This log file contains the activity report of the Deployment Server. If the Deployment Server is not running efficiently, this log file can be very useful for diagnostics and troubleshooting.	`MCDeplSvr.log`	`\Documents and Settings \LocalService \Application Data \SOTI\`
MobiControl Manager Log File	This log file contains the activity report of the MobiControl Manager. If the MobiControl Manager is not running efficiently, this log file can be very useful for diagnostics and troubleshooting.	`MCManager.log`	`\Documents and Settings \%username% \Local Settings \Application Data \SOTI \MobiControl\`

File name	Information	File Name	Location
MobiControl Remote Log File	This log file contains the activity report of the MobiControl Remote. If the MobiControl Remote is not running efficiently, this log file can be very useful for diagnostics and troubleshooting.	MCRemote.log	\Documents and Settings\ %username%\ Local Settings \Application Data \SOTI \MobiControl\
MobiControl Security Audit Log File	This log file contains the activity report of the MobiControl Security Audit. If the MobiControl Security Audit feature is reporting alerts, this log file can be very useful for diagnostics and troubleshooting.	MCSecAudit.log	\Documents and Settings\ *%username%*\ Local Settings\ Application Data\ SOTI\ MobiControl\
MobiControl Agent Install Log File	This log file contains the activity report of the MobiControl Agent Install. If the MobiControl Agent did not get installed successfully, this log file can be very useful for diagnostics and troubleshooting.	MCAgtInst.log	\Documents and Settings\ *%username%*\ Local Settings\ Application Data\ SOTI\ MobiControl\
MobiControl Package Studio Log File	This log file contains the activity report of the MobiControl Package Studio. If the MobiControl Package Studio is not running efficiently, this log file can be very useful for diagnostics and troubleshooting.	MCPkgStudio.log	\Documents and Settings\ *%username%*\ Local Settings\ Application Data\ SOTI\ MobiControl\
Installation Log File	This log file contains the activity report of the MobiControl Installer.	DBInstall.log	C:\ (root of your computer)

Files where a Windows Mobile or Windows CE Device Agent is installed

File name	Information	Location
commloader.exe	This file manages communication between the MobiControl Deployment Server and the mobile device. This file is the primary executable for the MobiControl Device Agent. Please see the "Tips and Tricks" topic on page 1511 for more information and options available with Commloader.exe.	\windows \startup\
mckiosk.exe	Device lockdown functionality is implemented in this	\windows\

File name	Information	Location
	file.	
pdb.ini	This file contains configuration information for the mobile Device Agent to use for a successful setup and communication. It also contains the variables that control the Deployment Server information, device naming parameters, communication, logs and packages information. If this file is deleted or becomes corrupted, then the Device Agent will be unable to run and connect with MobiControl Deployment Serverproperly. You would need to re-install the agent on the mobile device.	Installation directory of the MobiControlDevice Agent For example, for rugged devices, the location would the "persistent file store" of the mobile device; for non-rugged devices, the location would be "\SOTI\."
pkctrlsv.dll	This .dll file implements the remote control functionality.	\windows\
pdbpkg	This folder contains the compressed packages that are pushed down to devices via MobiControl. As the package is now stored locally on the mobile device, if the need comes to re-install the package, MobiControl will not re-send the package. It will send the command to install the package and the package will be re-installed from the "PDBPKG" folder.	Installation directory of the MobiControl Device Agent For example, for rugged devices, the location would the "persistent file store" of the mobile device. For non-rugged devices, the location would be "\SOTI\."
pdbinfo	This folder contains the results of the package executions. If a MobiControl package has been executed successfully, the resulting files will be in this folder.	Root drive of the mobile device
pkfsh.dll	This file implements file encryption on the mobile device.	\windows\
devinit.pcg	device initial package	\Temp\
mcreseng.dll	Keeps all MobiControl program resources	\windows\
autorun.log	Contains the MobiControl autorun log. **NOTE:** This log is only available when MobiControl Device Agent is using MobiControl Autorun system.	
pkctrlsv.log	Contains general activity and information on MobiControl.	Root drive of the mobile device
pkfsh.log	Contains activity of MobiControl file encryption.	Root drive of the mobile device

File name	Information	Location
pkInst.log	Contains information on the MobiControl device agent installation.	Root drive of the mobile device

Files where a Windows Desktop Device Agent is installed

File name	Information	Location
commloader.exe	This file manages communication between the MobiControlDeployment Serverand the mobile device. This file is the primary executable for the MobiControlDevice Agent. Please see the "Tips and Tricks" topic on page 1511 for more information and options available with Commloader.exe.	Installation directory of the MobiControl Device Agent. Default location: %PROGRAM FILES%\SOTI\MobiControl\
pdb.ini	This file contains configuration information for the mobile Device Agentto use for a successful setup and communication. It also contains the variables that control the Deployment Serverinformation, device naming parameters, communication, logs and packages information. If this file is deleted or becomes corrupted, then the Device Agentwill be unable to run and connect with MobiControlDeployment Serverproperly. You would need to re-install the agent on the mobile device.	Installation directory of the MobiControl Device Agent %PROGRAM FILES%\SOTI\MobiControl\

File name	Information	Location
pdbpkg	This folder contains the compressed packages that are pushed down to devices via MobiControl. As the package is now stored locally on the mobile device, if the need comes to re-install the package, MobiControl will not re-send the package. It will send the command to install the package and the package will be re-installed from the "PDBPKG" folder.	Installation directory of the MobiControl Device Agent %PROGRAM FILES%\SOTI\MobiControl\
pdbinfo	This folder contains the results of the package executions. If a MobiControl package has been executed successfully, the resulting files will be in this folder.	Installation directory of the MobiControl Device Agent %PROGRAM FILES%\SOTI\MobiControl\
MCHook.dll	This file allow the MobiControl Desktop Agent to capture keyboard, mouse, and screen input for 32-bit and 64-bit machines.	Installation directory of the MobiControl Device Agent %PROGRAM FILES%\SOTI\MobiControl\
MCHook64.dll	This file allow the MobiControl Desktop Agent to capture keyboard, mouse, and screen input for 32-bit and 64-bit machines.	Installation directory of the MobiControl Device Agent %PROGRAM FILES%\SOTI\MobiControl\
Commloader.dll	Contains resources for Commloader.exe	Installation directory of the MobiControl Device Agent %PROGRAM FILES%\SOTI\MobiControl\
MCHookHelper.exe	This file allow the MobiControl Desktop Agent to capture keyboard, mouse, and screen input for 32-bit and 64-bit machines.	Installation directory of the MobiControl Device Agent %PROGRAM FILES%\SOTI\MobiControl\

File name	Information	Location
`Uninstall.bat`	Run this batch file to manually uninstall the MobiControl Desktop Agent	Installation directory of the MobiControl Device Agent `%PROGRAM FILES%\SOTI\MobiControl\`
`Install.Bat`	Run this batch file to manually install the MobiControl Desktop Agent	Installation directory of the MobiControl Device Agent `%PROGRAM FILES%\SOTI\MobiControl\`
`WinAgent.log`	Contains general activity and information on MobiControl.	`%USERPROFILE%\AppData\Local\MobiControl\`