Device Management for *Windows Mobile*

User's Guide

Version 7.2

October 9, 2009

BigFix, Inc.
1480 64th Street, Suite 200
Emeryville, California 94608

Contents

CONTENTS

Part One

Introduction

Background

Organizations have become increasingly reliant on mobile technology such as phones, PDAs, point-of-sale devices, kiosks and mobile healthcare units. The enthusiasm for these devices is understandable: working remotely and wirelessly offers a tremendous boost to productivity and creates entirely new business opportunities. However, these tiny computers present the same privacy and security concerns as any other computer in the enterprise. Adding to the difficulty, they are only intermittently connected to corporate data centers.

Device Management for Windows Mobile addresses these concerns by applying proven Inspector technology to continuously monitor, update and report on issues as soon as they arise on the device. Employing a very small footprint, BigFix technology ensures that mobile applications are as secure and reliable as those that are wired to the corporate data center. Using the BigFix Console, you can continuously monitor potential problems and policy compliance across all your mobile clients, world-wide.

This manual assumes you have already installed the BigFix Mobile Client on your Windows Mobile devices and that you have created a custom site to serve up relevant Fixlet messages. If not, please consult the *Windows Mobile Installation Guide* and then return to this guide for more user information.

System Requirements

Device Management for Windows Mobile requires BigFix Version 7.2 or better.

Windows Mobile Device Support

Windows Mobile refers to the general family of compact operating systems used on mobile devices such as Pocket PCs, Smartphones, and Point of Sale devices. The BigFix Windows Mobile client is designed to run on most versions of the windows mobile platforms. The following devices are currently supported:

Windows CE 4.2:

- Windows Mobile 2003 for Smartphone
- Windows Mobile 2003 for Pocket PC Professional Edition
- Windows Mobile 2003 for Pocket PC Phone Edition
- Windows Mobile 2003 for Pocket PC Premium Edition
- Windows Mobile 2003 SE

Windows CE 5.0:

- Windows Mobile 5.0 Pocket PC
- Windows Mobile 5.0 Smartphone

Windows CE 6.0:

- Windows Mobile 6.0 Standard
- Windows Mobile 6.0 Classic
- Windows Mobile 6.0 Professional
- Windows Mobile 6.1 Standard
- Windows Mobile 6.1 Professional

Windows Mobile Client Limitations

Not every Windows interface is applicable to the BigFix Windows Mobile client, because the corresponding functionality doesn't exist on the mobile device. In particular, the following BigFix Client features for Windows don't have a mobile counterpart:

- UI Modes. Trays and balloon help are not supported by Windows Mobile.
- Wake on LAN.
- Actions that won't work:
  - **Dos**. Because the mobile client doesn't include CMD.exe, execution of this command will stop the Action with a fail on the line containing the command.
  - **Hidden**. WinCE can't launch an application using the **hidden** command.
- UDP won't work while using GPRS unless the IP address is static. A static IP address can be requested from the carrier.
- Dynamic bandwidth throttling is unavailable.
- No FIPS certification is possible on these platforms, although you can still put OpenSSL into FIPS mode.

Part Two

Windows Mobile Tools

Using the BigFix Mobile Client

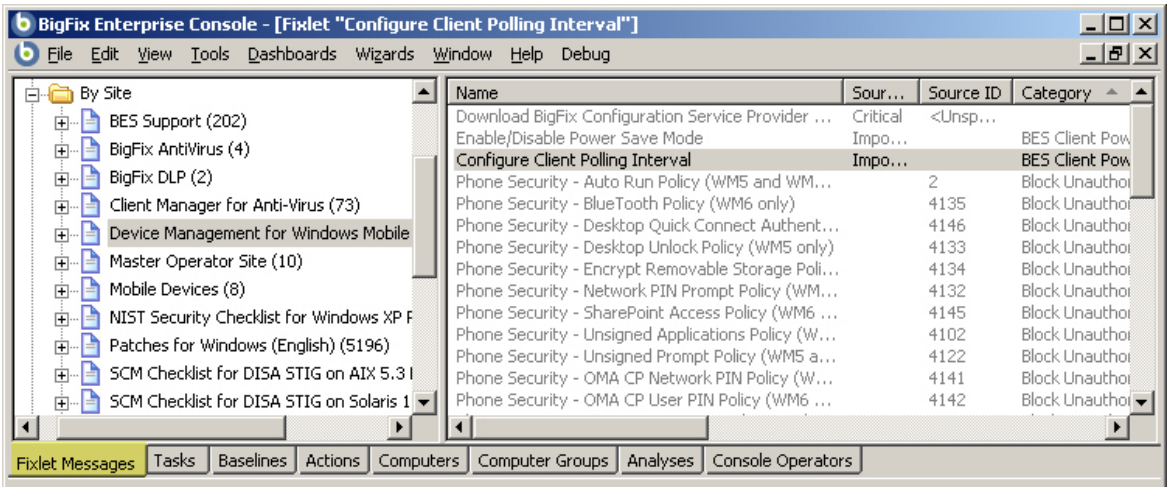
Once you have installed the software and verified it (see the *Windows Mobile Installation Guide* for more information), there are several features you can customize to enhance the management of your BigFix mobile devices. As with other offerings from BigFix, the primary workhorses of the site are Fixlets, Tasks and Analyses. Fixlets and Tasks often work together to complete a specified function. They provide the means for you to customize your site by setting specific values to align with your internal corporate policy. The group of values you create are called your "benchmark."

Analyses, on the other hand, allow you to *examine* the current settings on the mobile devices that are running the BigFix Mobile Client. Typically they display the current state of the benchmark you created through the use of Fixlets and Tasks. The following sections provide an overview of these tools, followed by a few specific examples to get you up and running.

Using Mobile Fixlet Messages

The BigFix Mobile Device site includes several Fixlet messages that you can use to adjust your policy settings or benchmark. To see the entire list of available Fixlet messages, follow these steps:

1. Click the **Fixlet Messages** tab.
2. From the navigation pane on the left, click **All Fixlet Messages**, open the **By Site** folder and select **Device Management for Windows Mobile**.



Note that there are Fixlet messages marked Critical and Important that you should address first. One of them downloads the CSP tool that is needed to properly customize your configuration. Another one enables the power save mode to keep your freshly installed devices from running down their batteries. The rest are security settings that you can configure to implement your corporate policy for mobile devices. These are grouped into categories (as seen in the last column). For more information on each of these settings, please consult the Microsoft MSDN site at http://msdn.microsoft.com/en-us/library/bb416355.aspx.

Here is a list of each of the available security settings, broken down by category.

Block Unauthorized Penetration

- Auto Run Policy
- Unsigned CABS Policy
- Unsigned Applications Policy
- Unsigned Themes Policy
- Service Loading (SL) Message Policy
- Service Indication (SI) Message Policy
- Unauthenticated Message Policy
- OTA Provisioning Policy
- WSP Push Policy
- Unsigned Prompt Policy
- Network PIN Prompt Policy
- WAP Signed Message Policy
- OMA CP Network PIN Policy
- OMA CP User PIN Policy
- OMA CP User Network PIN Policy
- Desktop Unlock
- Desktop Quick Connect Authentication Policy
- Encrypt Removable Storage Policy
- Bluetooth Policy
- SharePoint Access Policy

Protect Against Application Corruption

- RAPI Policy

Protect Sensitive Data During Transmission

- Signed Mail Policy
- Encrypted Message Policy
- SMIME Signing Policy
- SMIME Signing Algorithm Policy
- SMIME Encryption Policy
- SMIME Encryption Algorithm Policy
- Software Certificates Policy
- Message Encryption Negotiation Policy
- HTML Message Policy

Protect Sensitive Data in Case of Device Theft

- Message Authentication Retry Number Policy
- Password Required Policy

Specify Security Level

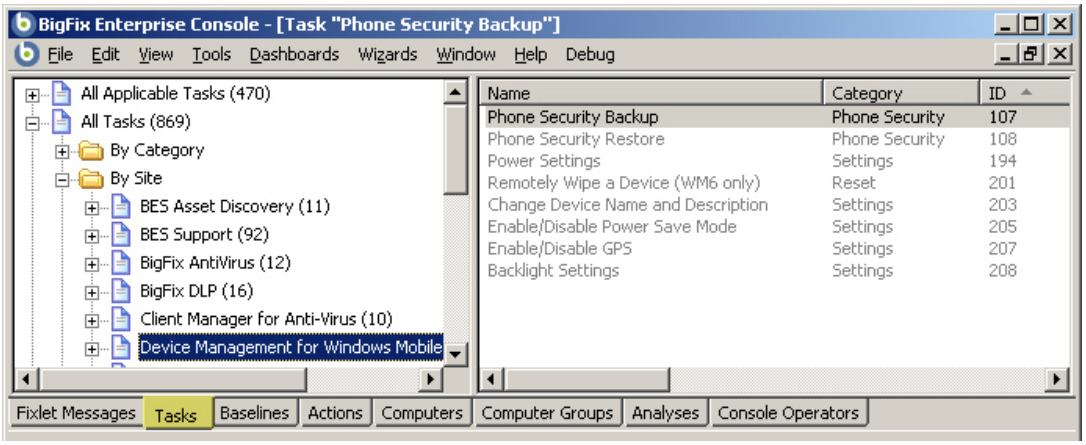
- Grant User Authenticated Policy
- Grant Manager Policy
- DRM Security Policy
- Trusted WAP Proxy Policy
- Trusted Provisioning Server (TPS) Policy
- SL Security Policy

It is a good idea to click on the corresponding Fixlet messages and look at their descriptions to get a feel for what the Windows Mobile site can do for you. The section on examples (later in this guide) will show you how to use the Fixlet messages and to customize their values.

Using Mobile Tasks

The BigFix Mobile Device site includes a set of Tasks that allows you to change several aspects of a given device. These are viewable by following these steps:

1. Click the **Tasks** tab.
2. From the navigation pane on the left, click **All Tasks**, open the **By Site** folder and select **Device Management for Windows Mobile**.

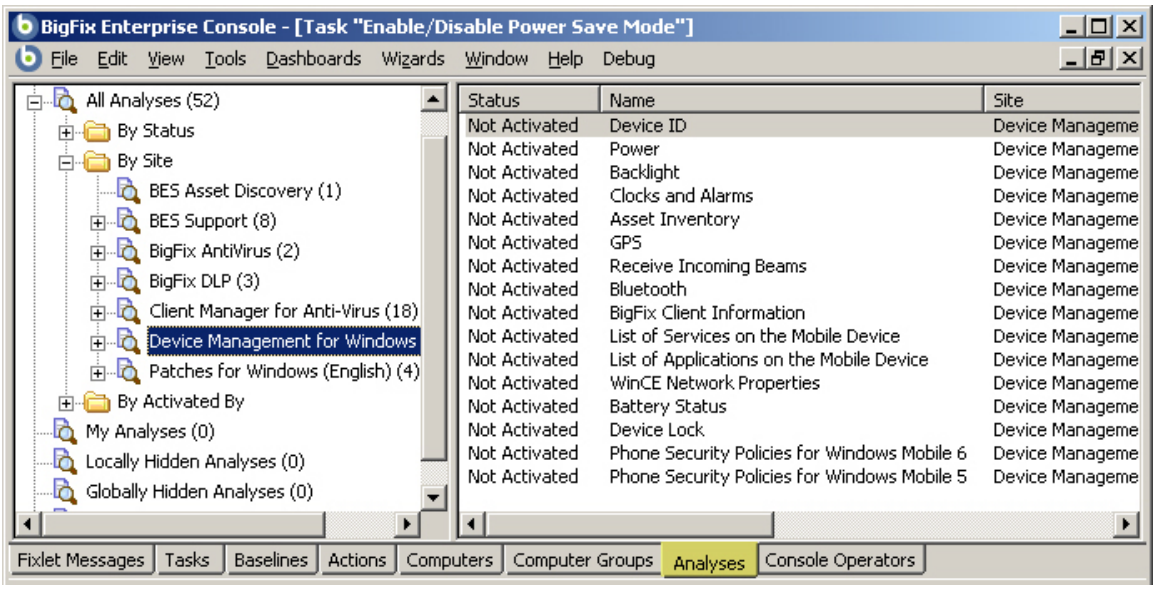


Note: Some of these Tasks, like Enable/Disable Power Save Mode, are tied in to Fixlet messages. In this particular case, the Fixlet warns you about Power Save mode, and then automatically refers you to the Task, which actually implements the setting.

Using Mobile Fixlet Analyses

The BigFix Mobile Device site includes a set of Analyses that can help you to monitor all the mobile devices with the BigFix Client installed. Among the Analyses you can perform, you will find the following:

1. Click the **Analyses** tab.
2. From the navigation pane on the left, click **All Fixlet Messages**, open the **By Site** folder and select **Device Management for Windows Mobile**.



As with the Fixlet messages and Tasks, it is a good idea to look through the list and open up some Analyses to check them out. In the next section, you will find some examples of how to evaluate what an Analysis will do and how to target it to just the set of mobile devices that you desire.

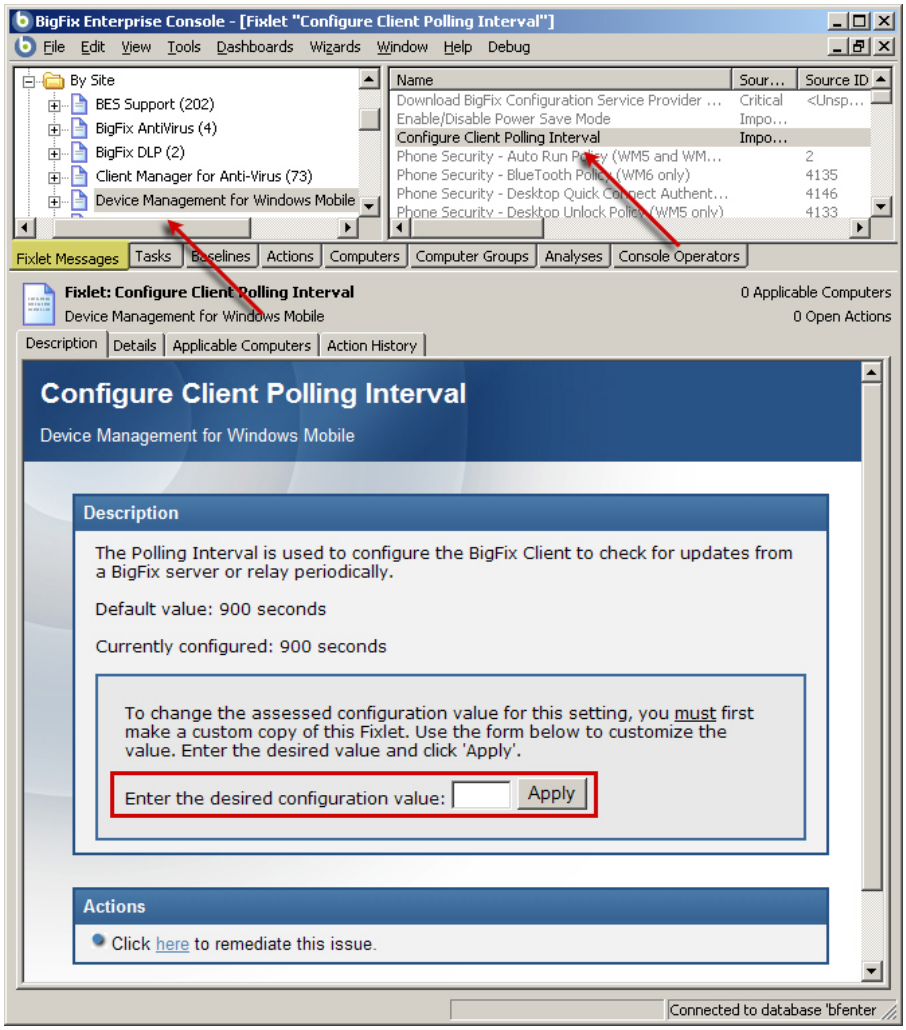
A Few Examples

This section provides you with a few select examples of using some of the built-in Fixlets, Tasks and Analyses. You will learn how to set values to customize Fixlets and Tasks and how to use Analyses to examine various aspects of your mobile devices.

Configuring the Client Polling Interval

When you first installed the Client software, you were encouraged to set a short polling interval (typically 60 seconds) to ensure a swift registration. Once the mobile device has registered, however, it is wise to lengthen the interval in order to conserve battery life. There is a Fixlet to adjust this value:

1. From the BigFix Console, click the **Fixlet Messages** tab.
2. From the left navigation panel, select **All Relevant Fixlet Messages**, then select the **By Site** folder and the **Device Management for Windows Mobile** site.
3. Select the Fixlet labeled **Configure Client Polling Interval**.

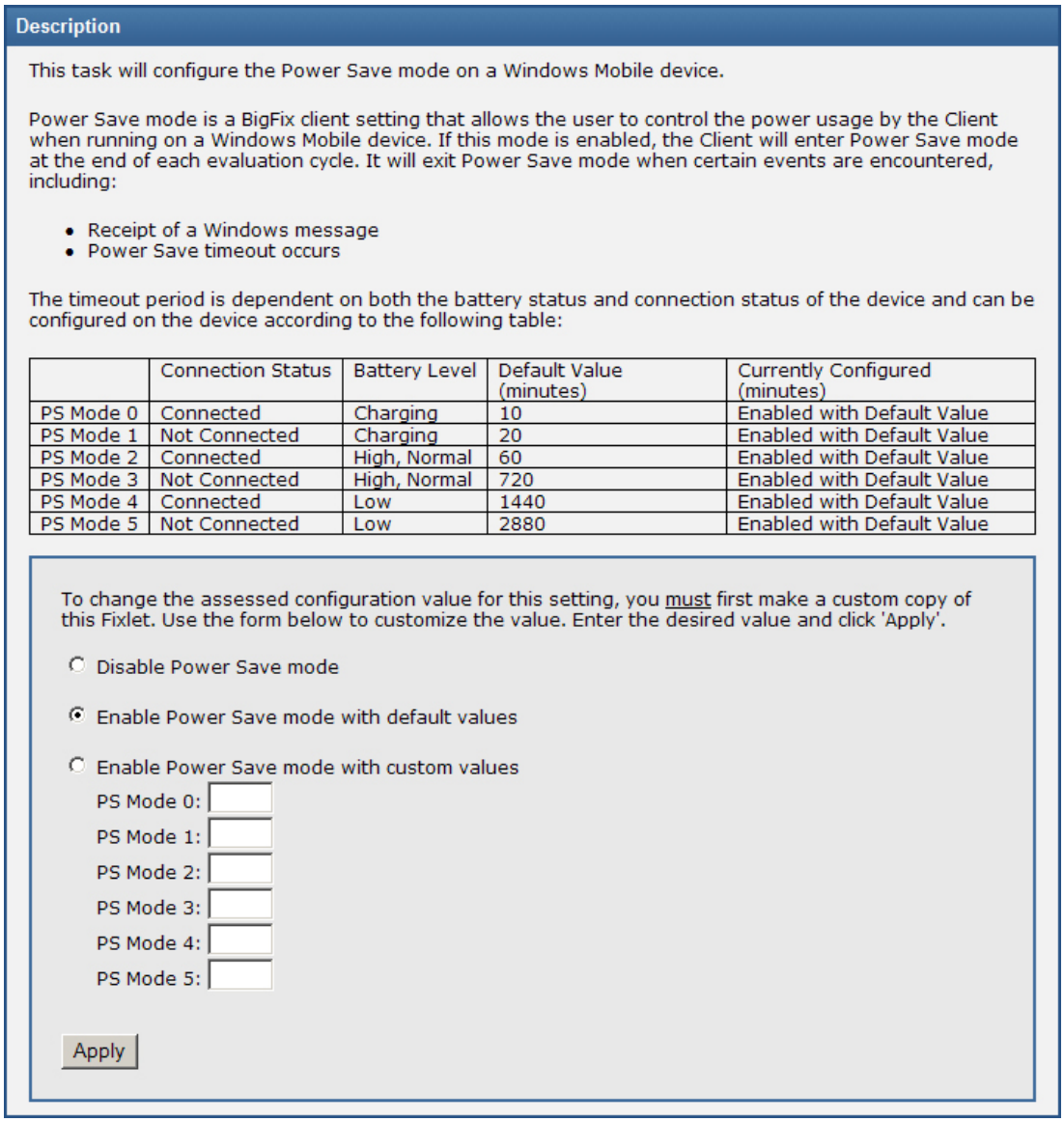


4. Note that the current value is 900 seconds, which is probably sufficient. However, if you want to set a different value, enter it into the text box and click the **Apply** button.

Enabling the Power Save Mode

There are actually six different power modes, and you can set each of them independently. Here's how:

1. As before, from the BigFix Console, click the **Fixlet Messages** tab.
2. From the left navigation panel, select **All Relevant Fixlet Messages**, then select the **By Site** folder and the **Device Management for Windows Mobile** site.
3. Select the Fixlet labeled **Enable/Disable Power Save Mode**. The Fixlet message is displayed in the work area below.



Description

This task will configure the Power Save mode on a Windows Mobile device.

Power Save mode is a BigFix client setting that allows the user to control the power usage by the Client when running on a Windows Mobile device. If this mode is enabled, the Client will enter Power Save mode at the end of each evaluation cycle. It will exit Power Save mode when certain events are encountered, including:

- Receipt of a Windows message
- Power Save timeout occurs

The timeout period is dependent on both the battery status and connection status of the device and can be configured on the device according to the following table:

	Connection Status	Battery Level	Default Value (minutes)	Currently Configured (minutes)
PS Mode 0	Connected	Charging	10	Enabled with Default Value
PS Mode 1	Not Connected	Charging	20	Enabled with Default Value
PS Mode 2	Connected	High, Normal	60	Enabled with Default Value
PS Mode 3	Not Connected	High, Normal	720	Enabled with Default Value
PS Mode 4	Connected	Low	1440	Enabled with Default Value
PS Mode 5	Not Connected	Low	2880	Enabled with Default Value

To change the assessed configuration value for this setting, you must first make a custom copy of this Fixlet. Use the form below to customize the value. Enter the desired value and click 'Apply'.

- ○ Disable Power Save mode
- ◉ Enable Power Save mode with default values
- ○ Enable Power Save mode with custom values

PS Mode 0:
PS Mode 1:
PS Mode 2:
PS Mode 3:
PS Mode 4:
PS Mode 5:

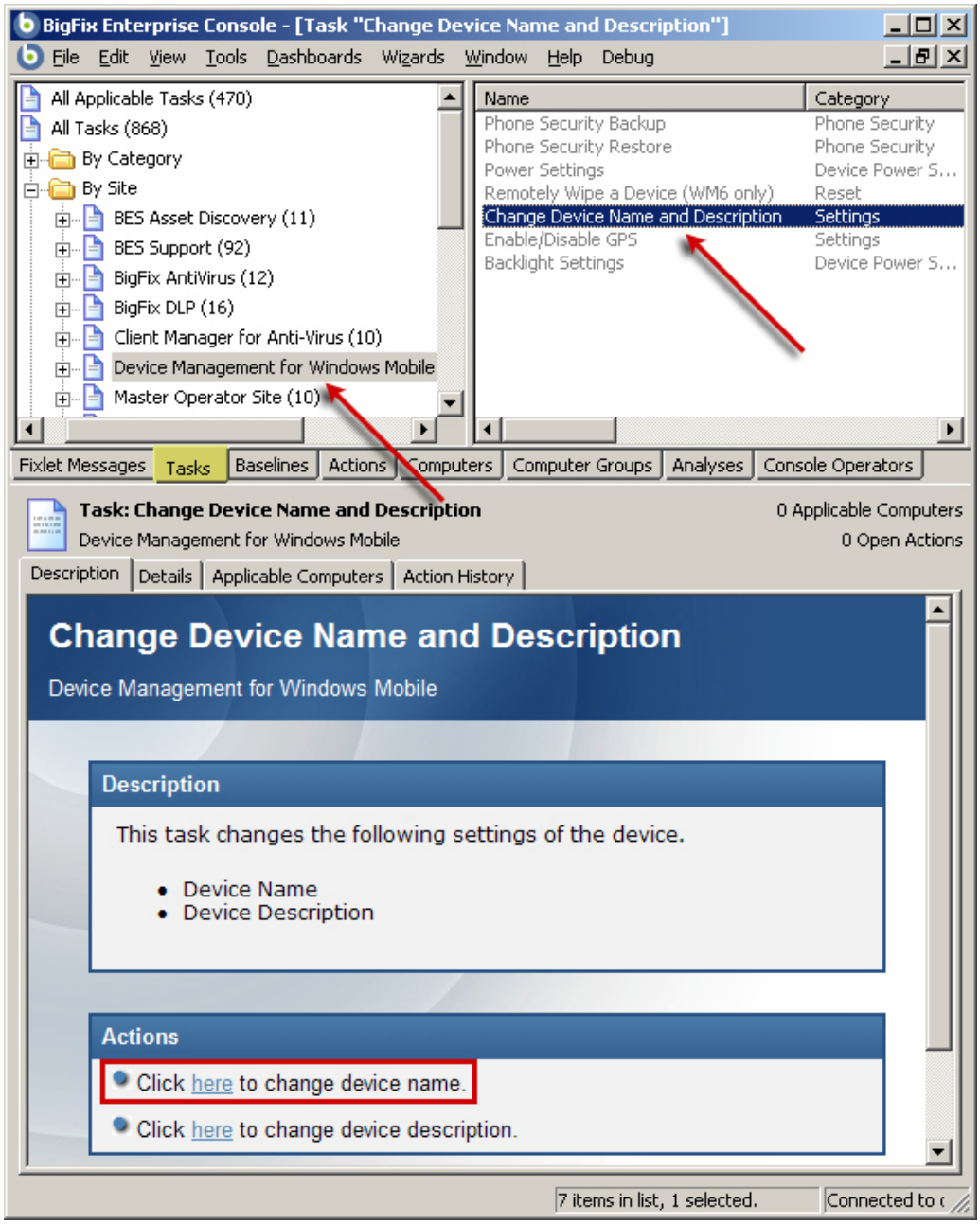
Apply

4. You have several choices here, including the ability to customize each power saving mode separately. Once you've settled on your values, click the **Apply** button.

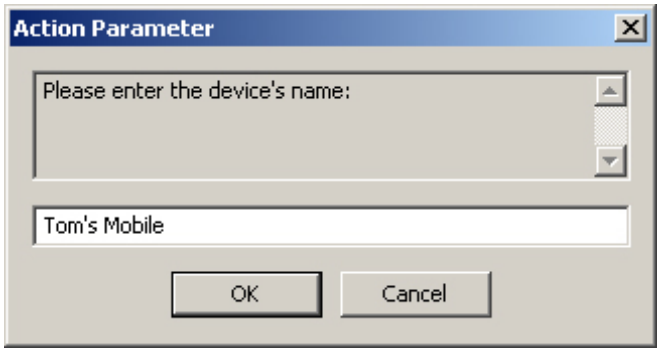
Changing the Name of a Device

Tasks act similarly to set values in your devices. An example Task is to change the name of the device. This can be accomplished as follows:

1. As before, from the BigFix Console, click the **Tasks** tab.
2. From the left navigation panel, select **All Tasks**, then select the **By Site** folder and the **Device Management for Windows Mobile** site.
3. Select the Task labeled **Change Device Name and Description**. The Task is displayed in the work area below.



4. Click the Action link to **change the device name**. A dialog pops up, prompting you for a new name.



5. The **Take Action** dialog opens, allowing you to target the particular phone. From the **Target** tab, click the first button to select a **specific computer**.
6. From the list of **applicable computers**, select the desired one. Click **OK**.
7. Enter your password to propagate the Action to the specified mobile device.

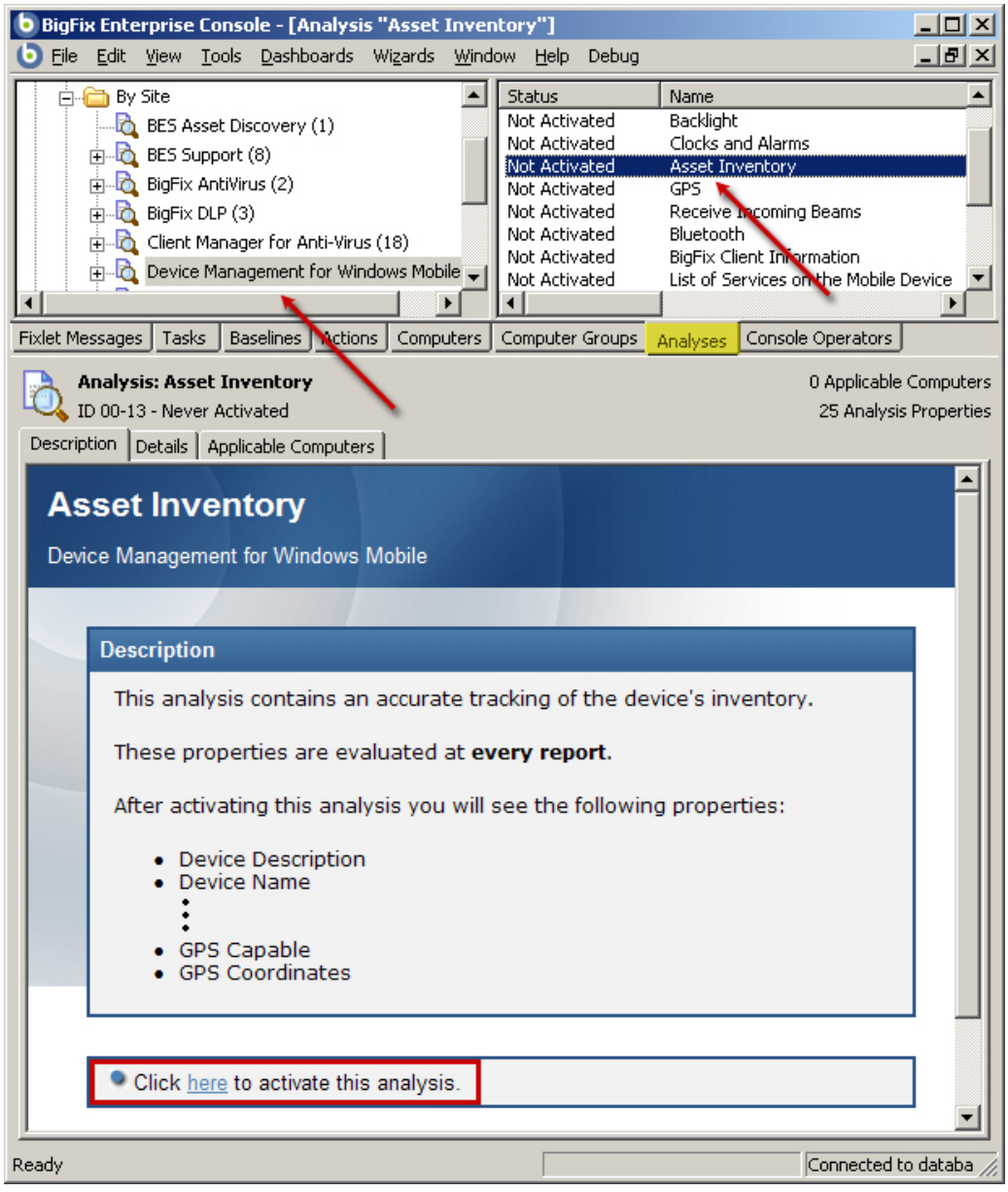
Note that this Task also allows you to change the description of the device as well. This is the general three-stage technique you will use with all tasks:

1. Select the Task.
2. Click an Action link to supply a value.
3. Target the device(s).

Monitoring Your Assets

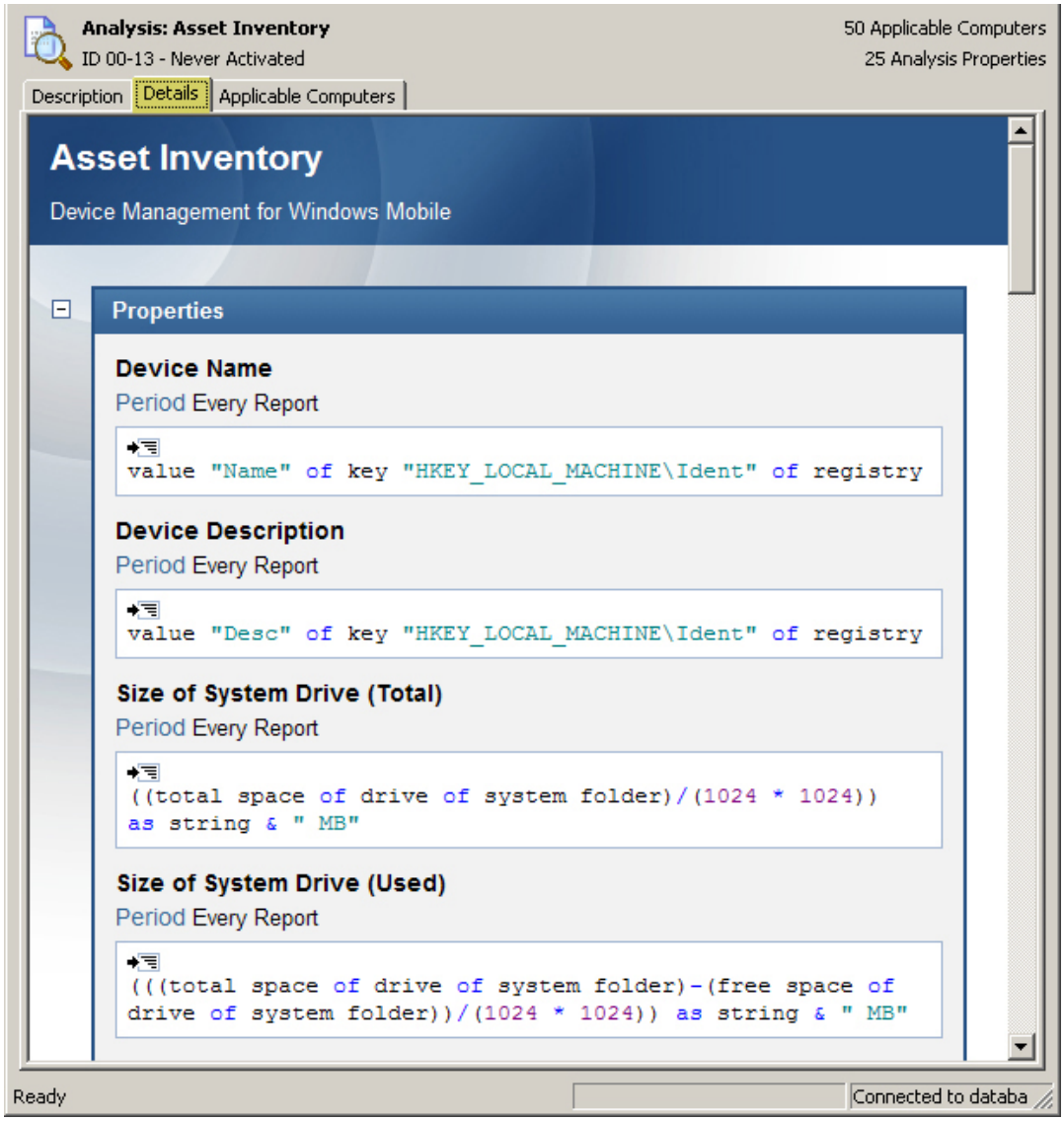
You can keep track of several aspects of your BigFix mobile devices by using Analyses. With a few mouse-clicks, you can easily ensure that a common operating environment is being adhered to across your enterprise. The content included with the BigFix Windows Mobile Fixlet site can provide you with a sample inventory analysis.

1. From the BigFix Console, click the **Analyses** tab.
2. From the left navigation panel, select **All Analyses**, then select the **By Site** folder and the **Device Management for Windows Mobile** site.
3. Select **Asset Inventory** from the list on the right.



This screen shot shows a truncated list of the properties that are analyzed.

4. Click the **Details** tab to see how the Analysis is implemented. Note which properties of the mobile device are captured and reported on, including drive size, processor, RAM size, OS version, serial number, GPS coordinates, battery life and more.

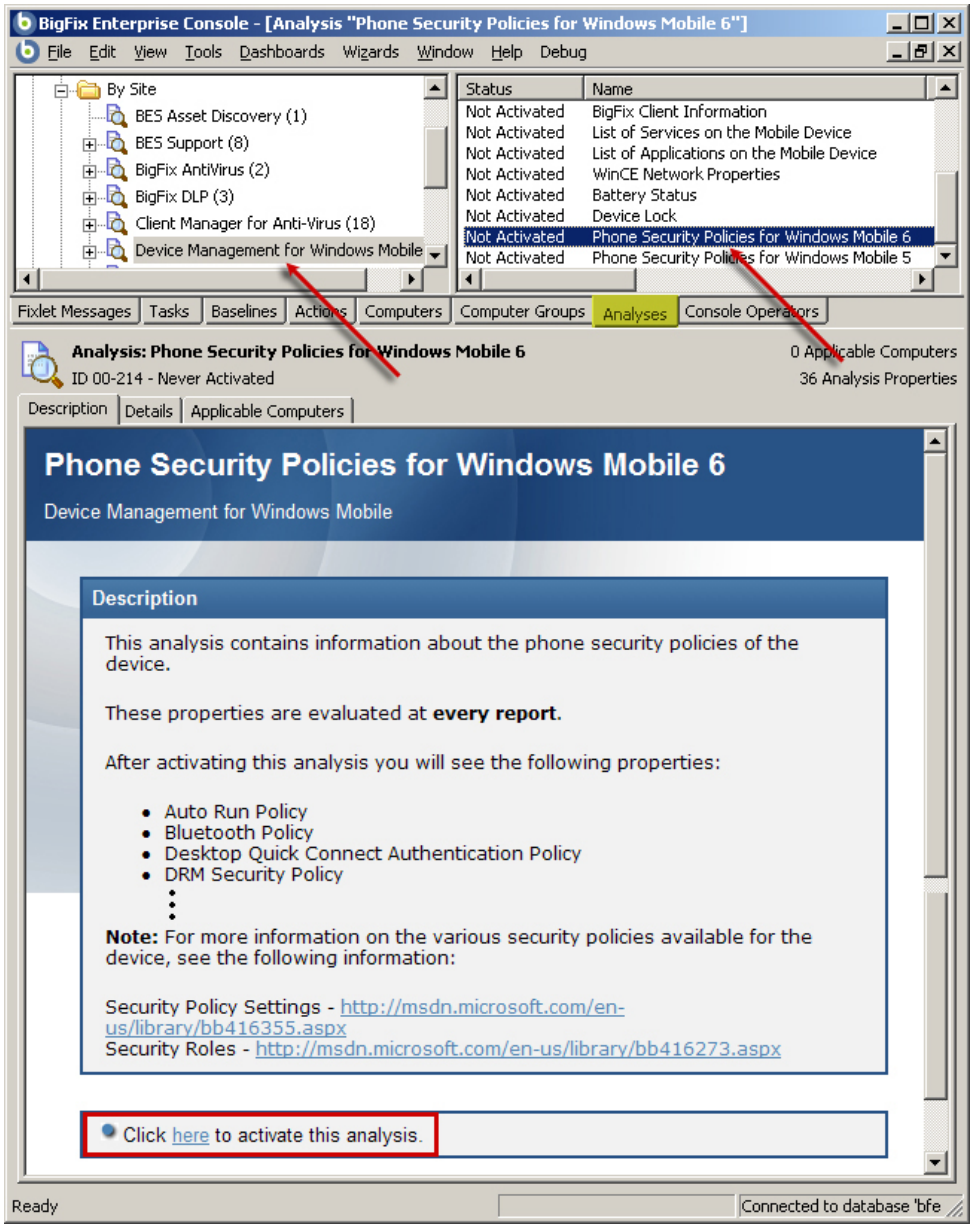


5. Click the **Applicable Computers** tab to select which devices you wish to analyze
6. Once you are satisfied with your selections, click the **Description** tab and click the link at the bottom of the page to activate the analysis.

Setting Phone Security Policies

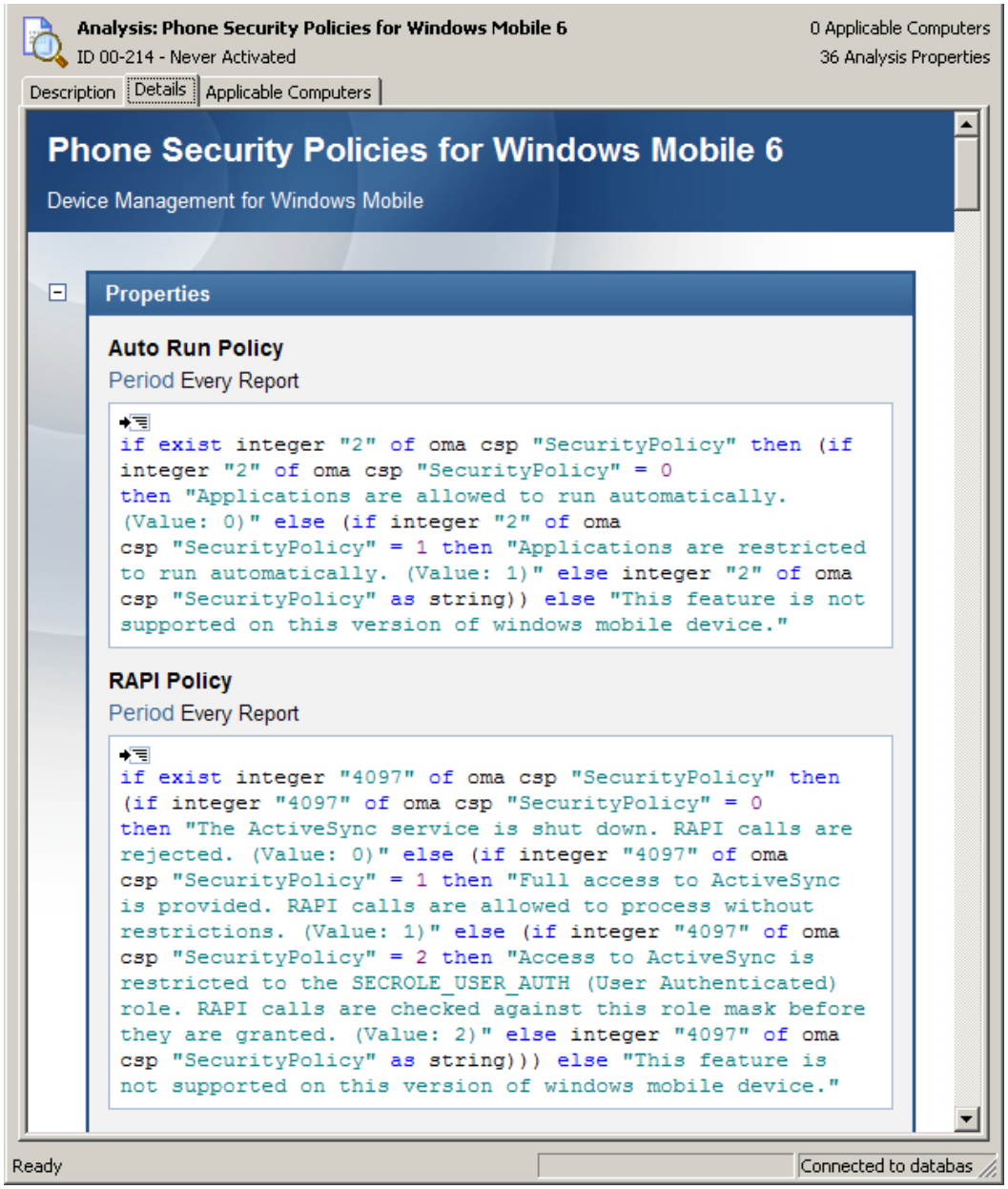
To monitor the security policy settings and roles on BigFix mobile devices, you can run an Analysis. This will present you with several values derived from the OMA CSP of the device to ensure adherence to your corporate security policies.

1. From the BigFix Console, click the **Analyses** tab.
2. From the left navigation panel, select **All Analyses**, then select the **By Site** folder and the **Device Management for Windows Mobile** site.
3. Select **Asset Inventory** from the list on the right.
4. Select **Phone Security Policies for Windows Mobile 6** from the list.



This screen shot shows a truncated list of the security properties that are analyzed.

5. Click the **Details** tab to see how the Analysis is implemented. Note which properties of the mobile device are captured and reported on, including AutoRun, DRM, OTA provisioning, RAPI, SL security, Trusted WAP Proxy, WSP Push and much more.



6. Click the **Applicable Computers** tab to select which devices you wish to analyze
7. Once you are satisfied with your selections, click the **Description** tab and click the link to activate the analysis.

Advanced Topics

Reading the Log Files as Text

Through the registry, you can associate the log file extensions so that you can open them as text files in Windows Explorer.

```
regset "[HKEY_CLASSES_ROOT\.log]" "Content Type"="text/plain"
regset "[HKEY_CLASSES_ROOT\.log]" "Default"="txtfile"
```

Setting Low Priority Connection Communication

This setting allows you to configure whether the client will initiate a network connection (0) or merely piggyback on existing network connections (1).

```
_BESClient_Comm_UseLowPriorityConnection=1 or 0
```

NOTE: For more reliable reporting, turn off **low priority connection** and set **command polling** to a small interval.

This setting controls whether the client will go into 'power save' mode after the gather/evaluation cycle is completed. During power save mode the client will primarily stay in sleep mode, saving battery life.

```
_BESClient_Resource_PowerSaveEnable=1 or 0
```

This setting controls the connection preferences for windows mobile clients. This setting is basically a semicolon-delimited list of connection types. For example:

```
 _BESClient_Comm_PhoneConnectionPreference="Wifi;*"
```

The client will attempt to connect to the server starting with the connection type listed first. If that fails the client moves on to the next connection type. An asterisk (*) can be used to allow the ConnectionManager to decide the best connection type to use. The supported values for this setting are:

- Wifi
- ActiveSync
- Ethernet
- Cellular
- Bluetooth
- VPN
- Unimodem
- *

Running the Windows Application Emulator

Launch the desired emulator and cradle it. Then you can launch WMAppLauncher as described below:

WMAppLauncher.exe <qna> <questions> <destination> <answers>
<qna> Path to QnAFile.exe (on the PC).
<questions> Questions file to use (on the PC).
<destination> Destination folder (on the device).
<answers> Path to the folder to which the resulting answers file will be copied (on the PC).

For example:

```
WMAppLauncher "C:\depot\working\Main\BES\ProjectFiles\Windows\Windows Mobile 5.0 Pocket PC SDK (ARMV4I)\PhoneQnAFile\Release\QnAFile.exe" "C:\depot\q.qna" "\QnA" "C:\depot"
```

Using the Configuration Service Provider

Starting with Windows Mobile 5.0, you can use XML files to provision devices with multiple settings at one time using the Configuration Service Provider (CSP). BigFix allows you to set up these XML files and then quickly launch them as Actions.

For instance, here is an example of an XML file to set the second parameter of the Security Policy to zero:

```
<wap-provisioningdoc>
   <characteristic type="SecurityPolicy">
      <parm name="2" value="0" />
   </characteristic>
</wap-provisioningdoc>
```

To implement this CSP provisioning command, follow these steps:

1. Create and test the XML file.
2. Delete any existing default XML file on the client.
3. Move the temporary file you created in step 1 to the target location
4. Run the CSPTool to execute the xml file at the target location.

These steps can be incorporated into an Action script, which would look like this:

```
createfile until endfile
<wap-provisioningdoc>
   <characteristic type="SecurityPolicy">
      <parm name="2" value="0" />
   </characteristic>
</wap-provisioningdoc>
endfile
```



```
delete "{location of client}\default.xml"

copy __createfile "{location of client}\default.xml"

wait "{location of client}\CSPTool.exe" "{location of client}\default.xml" "{location of client}\output.xml"
```

NOTE: the CSPTool accepts your XML file for provisioning and also creates an output file that you can specify.

Part Three

Windows Mobile Inspectors

Configuring a mobile device allows you to control the usage and behavior of the device in accordance with your policy and usage requirements. BigFix provides you with the ability to customize the settings as needed. The BigFix Mobile Device site provides you with three ways to manage these settings:

- **Fixlet messages**: These allow you to interrogate devices whenever they are connected and then to use Action scripts to change the settings based on relevance.
- **Tasks**: Similar to Fixlet messages, these also allow you to make setting changes based on relevance criteria.
- **Analyses**: These allow you to monitor the existing settings of any specified mobile device(s).

Using an extensive set of Inspectors (see the ***Windows Mobile Inspector Guide***) BigFix Clients can query the device and report back to the BigFix Console. These Inspectors provide you with access to the major settings available for Windows Mobile devices. Following is a list of those Inspectors (for more details, see the ***Inspector Library for Windows Mobile Devices***):

Type	Inspector Name	Description
<base_battery>	full life of <base_battery>	For the specified Windows Mobile battery, this Inspector returns a time interval corresponding to the number of seconds of battery life when at full charge. Base battery is an abstract type that can refer to either the main "battery" or the "backup battery".
<base_battery>	life of <base_battery>	For the specified Windows Mobile battery, this Inspector returns a time interval corresponding to the number of seconds of battery life remaining. Base battery is an abstract type that can refer to either the main "battery" or the "backup battery".
<base_battery>	life percent of <base_battery>	For the specified Windows Mobile battery, this Inspector returns an integer corresponding to the percentage of full battery charge remaining. This is a value in the range 0 to 100. Base battery is an abstract type that can refer to either the main "battery" or the "backup battery".
<base_battery>	millivolts of <base_battery>	For the specified Windows Mobile battery, this Inspector returns an integer corresponding to the amount of battery voltage in millivolts (mV). This is a value in the range of 0 to 65,535. Base battery is an abstract type that can refer to either the main "battery" or the "backup battery".
<base_battery>	status of <base_battery>	Returns a string corresponding to the current status of the battery. This is one of the following: Charging, High, Low, Critical, No battery or Unknown. Base battery is an abstract type that can refer to either the main "battery" or the "backup battery".
<battery>	ac of <battery>	Returns a string detailing the AC power status of the specified Windows Mobile device battery. This can include offline, online or backup. For more information, see the MSDN article on SYSTEM_POWER_STATUS_EX.

Type	Inspector Name	Description
<battery>	average interval of <battery>	Returns an integer corresponding to the time constant in milliseconds (ms) used for integrating the average battery current in milliamps.
<battery>	average milliamps of <battery>	Returns an integer corresponding to the short-term average current drain of the Windows Mobile device (in milliamps). This number is in the range of 0 to 32,767 when charging and 0 to –32,768 when discharging.
<battery>	chemistry of <battery>	This Inspector returns a string describing the type of chemistry used by the specified Windows Mobile battery. It can include alkaline, nicad, lithium and more. For details, see the MSDN article on SYSTEM_POWER_STATUS_EX2.
<battery>	milliamps of <battery>	Returns an integer corresponding to the instantaneous current drain of the Windows Mobile device (in milliamps). This number is in the range of 0 to 32,767 when charging and 0 to –32,768 when discharging.
<battery>	milliamps per hour of <battery>	Returns an integer corresponding to the long-term cumulative average discharge in milliamperes per hour (mA/H). This number can have a value in the range of 0 to –32,768. This value can be reset by charging or changing the batteries.
<battery>	temperature of <battery>	For this specified Windows Mobile device battery, this Inspector returns a floating point number corresponding to the battery temperature in degrees Celsius. It can be in the range of –3,276.8 to 3,276.7 in increments of 0.1 degrees Celsius.
<gps>	altitude of <gps>	Returns a string containing the altitude (in meters) of the Windows Mobile device, as determined by the onboard GPS.
<gps>	enabled of <gps>	Returns TRUE if the Global Positioning Service (GPS) on the Windows Mobile device is enabled.
<gps>	full status of <gps>	Returns a string containing the full status of the Windows Mobile device, as determined by the onboard GPS. It is a concatenation of all the inspectable items, with the general form 'feature: {value} units', each separated by a space. The full string looks like 'Name: {name} Status: {ON/OFF} Last sample time: {sample time} Latitude: {latitude} degrees Longitude: {longitude} degrees Heading: {heading} degrees Speed: {speed} knots Altitude: {altitude} m.'.
<gps>	heading of <gps>	Returns a string containing the heading in degrees (a heading of zero is true north) of the Windows Mobile device, as determined by the onboard GPS.
<gps>	latitude of <gps>	Returns a string containing the latitude (in degrees) of the Windows Mobile device, as determined by the onboard GPS. Positive numbers indicate the northern latitudes.
<gps>	longitude of <gps>	Returns a string containing the longitude (in degrees) of the Windows Mobile device, as determined by the onboard GPS. Positive numbers indicate east longitudes.

Type	Inspector Name	Description
<gps>	name of <gps>	Returns a string containing the human-readable name of the embedded GPS of the Windows Mobile device. It might, for example, be something like 'Acme GPS Card, version 3.4.'.
<gps>	sample time of <gps>	Returns a time value containing the current sample time used by the onboard GPS of the Windows Mobile device.
<gps>	speed of <gps>	Returns a string containing the speed (in knots) of the Windows Mobile device, as determined by the onboard GPS.
<oma csp>	autorun policy of <oma csp>	Returns an integer corresponding to the current autorun policy from the SecurityPolicy Configuration Service Provider. 0 indicates that applications are allowed to run automatically from the Multimedia Card when inserted. 1 indicates that applications are restricted from autorunning.
<oma csp>	block incoming calls of <oma csp>	Returns an integer corresponding to the current 'block incoming calls' status from the SecurityPolicy Configuration Service Provider.
<oma csp>	block outgoing calls of <oma csp>	Returns an integer corresponding to the current 'block outgoing calls' status from the SecurityPolicy Configuration Service Provider.
<oma csp>	bluetooth mode of <oma csp>	Returns an integer corresponding to the current bluetooth mode from the SecurityPolicy Configuration Service Provider.
<oma csp>	bluetooth policy of <oma csp>	Returns an integer corresponding to the current bluetooth policy from the SecurityPolicy Configuration Service Provider. This setting indicates whether a Bluetooth-enabled device will allow other devices to perform a search on the device. Possible values are: 0 blocks other devices from searching. 1 allows other devices to search.
<oma csp>	boolean <string> of <oma csp>	Returns the result of the specified OMA CSP query as a boolean value.
<oma csp>	call waiting enabled of <oma csp>	Returns the current 'call waiting enabled' status (TRUE or FALSE) from the SecurityPolicy Configuration Service Provider.
<oma csp>	construct xml <string> of <oma csp>	Returns an XML snippet to query an OMA CSP based on the parameters passed in <string>.
<oma csp>	desktop quick connect authentication policy of <oma csp>	Returns the current 'desktop quick connect authentication' policy from the SecurityPolicy Configuration Service Provider. This setting indicates how device authentication will be handled when connecting to the desktop. Possible values are: 0 User must authenticate the device upon connection, if the device lock is active. 1 If user chooses quick connect, the desktop will uniquely identify the device and allow it to connect without requiring the user to manually unlock it.

Type	Inspector Name	Description
<oma csp>	drm security policy of <oma csp>	Returns a bit-map integer corresponding to the current Digital Rights Management (DRM) security policy from the SecurityPolicy Configuration Service Provider. The given role bit-map indicates which DRM rights messages will be accepted by the DRM engine.
<oma csp>	encrypt removable storage policy of <oma csp>	Returns an integer corresponding to the current 'encrypt removable storage' policy from the SecurityPolicy Configuration Service Provider. This setting indicates if the user is allowed to change mobile encryption settings for the removable storage media. Possible values are: 0 indicates that the user is not allowed to change the encryption settings. 1 indicates that the user can change the encryption settings. This is the default.
<oma csp>	fixed dialing enabled of <oma csp>	Returns the current 'fixed dialing enabled' setting (TRUE or FALSE) from the SecurityPolicy Configuration Service Provider.
<oma csp>	forward all calls enabled of <oma csp>	Returns the current 'forward all calls enabled' setting (TRUE or FALSE) from the SecurityPolicy Configuration Service Provider.
<oma csp>	forward all calls of <oma csp>	Returns a string corresponding to the current 'forward all calls' setting from the SecurityPolicy Configuration Service Provider.
<oma csp>	forward all calls timeout of <oma csp>	Returns an integer corresponding to the current 'forward all calls timeout' setting from the SecurityPolicy Configuration Service Provider.
<oma csp>	forward all calls to of <oma csp>	Returns a string corresponding to the current 'forward all calls to' string from the SecurityPolicy Configuration Service Provider.
<oma csp>	forward calls enabled when busy of <oma csp>	Returns the current 'forward calls enabled when busy' setting (TRUE or FALSE) from the SecurityPolicy Configuration Service Provider.
<oma csp>	forward calls enabled when no answer of <oma csp>	Returns the current 'forward calls enabled when no answer' setting (TRUE or FALSE) from the SecurityPolicy Configuration Service Provider.
<oma csp>	forward calls enabled when unavailable of <oma csp>	Returns the current 'forward calls enabled when unavailable' setting (TRUE or FALSE) from the SecurityPolicy Configuration Service Provider.
<oma csp>	forward calls timeout when busy of <oma csp>	Returns an integer corresponding to the current 'forward calls timeout when busy' setting from the SecurityPolicy Configuration Service Provider.
<oma csp>	forward calls timeout when no answer of <oma csp>	Returns an integer corresponding to the current 'forward calls timeout when no answer' setting from the SecurityPolicy Configuration Service Provider.
<oma csp>	forward calls timeout when unavailable of <oma csp>	Returns an integer corresponding to the current 'forward calls timeout when unavailable' setting from the SecurityPolicy Configuration Service Provider.
<oma csp>	forward calls to when busy of <oma csp>	Returns a string corresponding to the current 'forward calls to when busy' setting from the SecurityPolicy Configuration Service Provider.

Type	Inspector Name	Description
<oma csp>	forward calls to when no answer of <oma csp>	Returns a string corresponding to the current 'forward calls to when no answer' setting from the SecurityPolicy Configuration Service Provider.
<oma csp>	forward calls to when unavailable of <oma csp>	Returns a string corresponding to the current 'forward calls to when unavailable' setting from the SecurityPolicy Configuration Service Provider.
<oma csp>	forward calls when busy of <oma csp>	Returns a string corresponding to the current 'forward calls when busy' setting from the SecurityPolicy Configuration Service Provider.
<oma csp>	forward calls when no answer of <oma csp>	Returns a string corresponding to the current 'forward calls when no answer' setting from the SecurityPolicy Configuration Service Provider.
<oma csp>	forward calls when unavailable of <oma csp>	Returns a string corresponding to the current 'forward calls when unavailable' setting from the SecurityPolicy Configuration Service Provider.
<oma csp>	grant manager policy of <oma csp>	Returns an integer bit-mask corresponding to the current 'grant manager' policy from the SecurityPolicy Configuration Service Provider. This setting grants the system administrative privileges held by the role manager to other security roles, without modifying metabase role assignments. The bit-mask describes which roles are granted system administrative privileges.
<oma csp>	grant user authenticated policy of <oma csp>	Returns an integer bit-mask corresponding to the current 'grant user authenticated' policy from the SecurityPolicy Configuration Service Provider. This setting grants privileges held by the User Authenticated role to other security roles without modifying metabase role assignments. The bit-mask describes which roles are granted system administrative privileges.
<oma csp>	html message policy of <oma csp>	Returns an integer corresponding to the current 'html message' policy from the SecurityPolicy Configuration Service Provider. This setting specifies whether message transports will allow HTML messages. 0 indicates that HTML messages are not allowed. 1 indicates that HTML messages are allowed.
<oma csp>	integer <string> of <oma csp>	Returns the result of the specified OMA CSP query as an integer value.
<oma csp>	message authentication retry number policy of <oma csp>	Returns a one-byte integer corresponding to the current 'message authentication retry number' policy from the SecurityPolicy Configuration Service Provider. This indicates the maximum number of times the user is allowed to try authenticating a Wireless Application Protocol (WAP) PIN-signed message. The default value is 3 for WM. Possible values are 1 through 256.

Type	Inspector Name	Description
<oma csp>	message encryption negotiation policy of <oma csp>	Returns an integer corresponding to the current 'message encryption negotiation' policy from the SecurityPolicy Configuration Service Provider. This setting indicates whether the Inbox application can negotiate the encryption algorithm in the case that a recipient's certificate doesn't support the specified encryption algorithm. Possible values are: 0 doesn't allow negotiation. 1 allows negotiation to a strong algorithm. 2 allows negotiation to any algorithm.
<oma csp>	network pin prompt policy of <oma csp>	Returns an integer corresponding to the current 'network personal identification number (PIN) prompt' policy from the SecurityPolicy Configuration Service Provider. This setting is used when an over-the-air (OTA) OMA Client Provisioning message is only signed with a network PIN. This setting indicates whether or not the user will be prompted to accept the device setting changes. Possible values are: 0 indicates that the device will prompt the user. 1 indicates that the user is not prompted. This is the default.
<oma csp>	network type of <oma csp>	Returns the current 'network type' policy from the SecurityPolicy Configuration Service Provider.
<oma csp>	obex enabled of <oma csp>	Returns the current 'obex enabled' policy from the SecurityPolicy Configuration Service Provider. This indicates whether or not the phone can exchange binary objects, either by infrared or bluetooth.
<oma csp>	oma cp network pin policy of <oma csp>	Returns the current 'oma cp network personal identification number (PIN)' policy from the SecurityPolicy Configuration Service Provider. This setting indicates whether the OMA network PIN-signed message will be accepted. The message's role bit-mask and the policy's role mask are ANDed together. If the result is non-zero, then the message will be accepted.
<oma csp>	oma cp user network pin policy of <oma csp>	Returns the current 'oma cp user network personal identification number (PIN)' policy from the SecurityPolicy Configuration Service Provider. This setting indicates whether the OMA user network PIN-signed message will be accepted. The message's role bit-mask and the policy's role mask are ANDed together. If the result is non-zero, then the message will be accepted.
<oma csp>	oma cp user pin policy of <oma csp>	Returns the current 'oma cp user personal identification number (PIN)' policy from the SecurityPolicy Configuration Service Provider. This setting indicates whether the OMA-user PIN or user MAC-signed message will be accepted. The message's role bit-mask and the policy's role mask are ANDed together. If the result is non-zero, then the message will be accepted.

Type	Inspector Name	Description
<oma csp>	ota provisioning policy of <oma csp>	Returns an integer bit-mask corresponding to the current 'ota provisioning' policy from the SecurityPolicy Configuration Service Provider. This setting indicates which provisioning messages are accepted by the configuration host based on the role bit-maps assigned to the messages. This policy restricts the provisioning messages that come from the Push Router. A specified role bit-mask indicates system administrative privileges are provided to the given mask.
<oma csp>	password required policy of <oma csp>	Returns an integer corresponding to the current 'password required' policy from the SecurityPolicy Configuration Service Provider. Possible values are: 0 indicates that a password is required. This is the default. A value other than 0 indicates that a password is not required.
<oma csp>	privileged applications policy of <oma csp>	Returns the current 'privileged applications' policy from the SecurityPolicy Configuration Service Provider. This setting indicates which security model has been implemented on the WM device. Possible values are: 0 indicates that a two-tier security model is enabled. 1 indicates that a one-tier security model is enabled. Any value other than 1 is treated as 0.
<oma csp>	process xml query <string> of <oma csp>	This Inspector will take the value passed in <string> and then ask the system to process it. In order to use it, the value provided must be a valid OMA CSP XML query that is not trying to set a value (only queries are allowed). A typical use is to take the results of the 'construct xml query' Inspector and pass it in as the query string.
<oma csp>	rapi policy of <oma csp>	Returns an integer corresponding to the current RAPI (Remote API) policy from the SecurityPolicy Configuration Service Provider. 0 indicates that the ActiveSync service is shut down and RAPI calls are rejected. 1 indicates that full access to ActiveSync is provided and RAPI calls are allowed without restrictions. 2 indicates that access to ActiveSync is restricted to the User-Authenticated role. RAPI calls are then checked against this role mask before being granted.
<oma csp>	security policy of <oma csp>	Returns an integer corresponding to the current 'security policy' policy from the SecurityPolicy Configuration Service Provider.
<oma csp>	send caller id of <oma csp>	Returns an integer corresponding to the current 'send caller id' policy from the SecurityPolicy Configuration Service Provider.
<oma csp>	service indication message policy of <oma csp>	Returns an integer bit-mask corresponding to the current 'service indication message' policy from the SecurityPolicy Configuration Service Provider. An SI message is sent to WM 6 Standard to notify users of new services and service updates. This setting indicates whether SI messages are accepted in the form of a role bit-mask.

Type	Inspector Name	Description
<oma csp>	service loading message policy of <oma csp>	Returns an integer bit-mask corresponding to the current 'service loading message' policy from the SecurityPolicy Configuration Service Provider. An SL message downloads new services to the WM device. This setting indicates whether SL messages are accepted in the form of a role bit-mask.
<oma csp>	sharepoint access policy of <oma csp>	Returns an integer corresponding to the current 'sharepoint access' policy from the SecurityPolicy Configuration Service Provider. This setting indicates whether OMA SharePoint or UNC access is enabled through ActiveSync protocol to fetch documents. Possible values are: 0 doesn't allow SharePoint or UNC file access. 1 allows OMA to fetch documents on a corporate SharePoint site or UNC.
<oma csp>	sl security policy of <oma csp>	Returns an integer corresponding to the current 'sl security' policy from the SecurityPolicy Configuration Service Provider. This setting indicates that the operator can override https to use http, or wsps to use wsp. Possible values are: 0 use https or wsps. 1 use http or wsp. This is the default value.
<oma csp>	smime encryption algorithm policy of <oma csp>	Returns an integer corresponding to the current 'smime encryption algorithm' policy from the SecurityPolicy Configuration Service Provider. This setting indicates which algorithm is used to encrypt a message. Possible values are: 0 specifies the default algorithm. 1 is an invalid value. 2 specifies the triple DES algorithm. 3 specifies the DES algorithm. 4 specifies the RC2 128-bit algorithm. 5 specifies the RC2 64-bit algorithm. 6 specifies the RC2 40-bit algorithm.
<oma csp>	smime encryption policy of <oma csp>	Returns an integer corresponding to the current 'smime encryption' policy from the SecurityPolicy Configuration Service Provider. This setting indicates whether the Inbox application will send all messages encrypted. 0 all messages must be encrypted. 1 encrypting messages is optional.
<oma csp>	smime signing algorithm policy of <oma csp>	Returns an integer corresponding to the current 'smime signing algorithm' policy from the SecurityPolicy Configuration Service Provider. This setting indicates which algorithm is used to sign a message. Possible values are: 0 specifies the default algorithm. 1 is an invalid value. 2 specifies the SHA algorithm. 3 specifies the MD5 algorithm.

Type	Inspector Name	Description
<oma csp>	smime signing policy of <oma csp>	Returns an integer corresponding to the current 'smime signing' policy from the SecurityPolicy Configuration Service Provider. This setting indicates whether the Inbox application will send all messaged signed. 0 all messages must be signed. 1 signing messages is optional.
<oma csp>	software certificates policy of <oma csp>	Returns an integer corresponding to the current 'software certificates' policy from the SecurityPolicy Configuration Service Provider. This setting indicates whether software certificates can be used to sign outgoing messages. Possible values are: 0 indicates that software certificates cannot be used to sign messages. 1 indicates that software certificates can be used to sign messages. This is the default.
<oma csp>	storage card encryption of <oma csp>	Returns the current 'storage card encryption' policy from the SecurityPolicy Configuration Service Provider.
<oma csp>	string <string> of <oma csp>	Returns the result of the specified OMA CSP query as a string value.
<oma csp>	timezone of <oma csp>	Returns an integer corresponding to the current timezone policy from the SecurityPolicy Configuration Service Provider.
<oma csp>	trusted provisioning server policy of <oma csp>	Returns an integer corresponding to the current 'trusted provisioning server' policy from the SecurityPolicy Configuration Service Provider. Possible values are: 0 indicates that assigning TPS role assignment is disabled. 1 indicates TPS role assignment is enabled and the TPS role can be assigned to mobile operators. This is the WM default.
<oma csp>	trusted wap proxy policy of <oma csp>	Returns an integer bit-map corresponding to the current 'trusted wap proxy' policy from the SecurityPolicy Configuration Service Provider. This setting indicates the level of permissions required to create, modify or delete a trusted proxy. The security roles that can have Trusted WAP Proxy level permissions are returned as a bit-mask.
<oma csp>	unauthenticated message policy of <oma csp>	Returns an integer bit-mask corresponding to the current 'unauthenticated message' policy from the SecurityPolicy Configuration Service Provider. This setting indicates whether to accept unsigned WAP messages processed by the default security provider in the Push Router, based on their origin. The message source must match one of the security roles specified by this policy. This setting indicates whether unauthenticated messages are accepted in the form of a role bit-mask.

Type	Inspector Name	Description
<oma csp>	unsigned applications policy of <oma csp>	Returns an integer corresponding to the current 'unsigned applications' policy from the SecurityPolicy Configuration Service Provider. The possible values are: 0 indicates that unsigned apps are not allowed to run on the device. 1 indicates that unsigned apps are allowed to run on the device. This is the default for WM. Any value other than 1 is treated as 0.
<oma csp>	unsigned cabs policy of <oma csp>	Returns an integer corresponding to the current 'unsigned CABS' policy from the SecurityPolicy Configuration Service Provider. This indicates whether unsigned .cab files can be installed on the device. Possible values are: 0 is equivalent to having none of the role mask bits set and indicates that no unsigned .cab files can be installed. A specified role bit-mask indicates accepted unsigned .cab files are installed with the given role mask.
<oma csp>	unsigned prompt policy of <oma csp>	Returns an integer corresponding to the current 'unsigned prompt' policy from the SecurityPolicy Configuration Service Provider. This setting indicates whether a user must be prompted to accept or reject unsigned .exe, theme, .dll or .cab files. Possible values are: 0 indicates that the user will be prompted. This is the WM default. 1 indicates that the user will not be prompted. Any value other than 1 is treated as 0.
<oma csp>	unsigned themes policy of <oma csp>	Returns an integer corresponding to the current 'unsigned themes' policy from the SecurityPolicy Configuration Service Provider. Possible values are: 0 is equivalent to having none of the role-mask bits set, and indicates that no unsigned Theme files can be installed. A specified role bit-mask indicates accepted unsigned Theme files are installed with the given role mask.
<oma csp>	value <string> of <oma csp>	Returns the result of the specified OMA CSP query as a string value.
<oma csp>	wsp push policy of <oma csp>	Returns an integer corresponding to the current 'Wireless Session Protocol (WSP) push' policy from the SecurityPolicy Configuration Service Provider. This setting indicates whether WSP notifications from the WAP stack are routed. Possible values are: 0 indicates that routing of WSP notifications is not allowed. 1 indicates that Routing is allowed. This is the WM default.
<phone>	identifier of <phone>	Returns a string corresponding to the identifier of the specified phone.
<phone>	manufacturer of <phone>	Returns a string corresponding to the manufacturer of the specified phone.
<phone>	model of <phone>	Returns a string corresponding to the model of the specified phone.

Type	Inspector Name	Description
<phone>	operator name of <phone>	Returns a string corresponding to the operator name of the specified phone.
<phone>	owner address of <phone>	Returns a string corresponding to the address of the owner of the specified phone.
<phone>	owner company of <phone>	Returns a string corresponding to the company name of the owner of the specified phone.
<phone>	owner email of <phone>	Returns a string corresponding to the email address of the owner of the specified phone.
<phone>	owner name of <phone>	Returns a string corresponding to the name of the owner of the specified phone.
<phone>	owner notes of <phone>	Returns a string containing the owner notes of the specified phone.
<phone>	phone number of <phone>	Returns a string containing the phone number of the specified phone.
<phone>	rated speed of <phone>	Returns a string corresponding to the rated speed of the specified phone.
<phone>	revision of <phone>	Returns a string identifying the revision of the specified phone.
<phone>	roaming status of <phone>	Returns a string identifying the roaming status of the specified phone.
<phone>	serial number of <phone>	Returns a string corresponding to the serial number of the specified phone.
<phone>	signal strength of <phone>	Returns a string corresponding to the signal strength of the specified phone as a percentage.
<phone>	subscriber number of <phone>	Returns a string corresponding to the subscriber number of the specified phone.
<phone>	type of <phone>	Returns a string identifying the type of the specified phone.
<ram>	available of <ram>	Returns the total amount of RAM (in bytes) currently available on the Windows Mobile device. This is the same as for the Windows client.
<ram>	load of <ram>	Returns the amount of memory being used on the Windows Mobile device as a percentage. 0 = no memory used, 100 = all memory used. This is the same as for the Windows client.
<wince network connection detail>	<wince network connection detail> as string	Returns the WinCE network connection detail as a string of the following form: "<description>" "<adapter name>" "<type>" "<status>" "<flags>" "<source network>" "<destination network>" "<last connected>" "<signal quality>" "<ip addresses>".
<wince network connection detail>	adapter name of <wince network connection detail>	Returns a string corresponding to the null-terminated name of the adapter for the given WinCE network connection. If no adapter name is available, the Inspector returns NULL.

Type	Inspector Name	Description
<wince network connection detail>	description of <wince network connection detail>	Returns a string corresponding to the null-terminated description of the given WinCE network connection. If no adapter name is available, the Inspector returns NULL.
<wince network connection detail>	destination network of <wince network connection detail>	Returns a string containing the GUID of the destination network for the specified WinCE connection.
<wince network connection detail>	flags of <wince network connection detail>	Returns a string containing one or more connection options for the specified WinCE network connection. These flags include: billed by time, always on, or suspend and resume. The constants for these flags are explained in greater detail in the MSDN article on the Connection Manager Connection Options Constants.
<wince network connection detail>	ip addresses of <wince network connection detail>	Returns a string containing the available IP addresses for the specified WinCE network connection. If no addresses are available, this Inspector returns NULL.
<wince network connection detail>	last connected of <wince network connection detail>	Returns a string containing the last time that the connection was established for the specified WinCE network connection.
<wince network connection detail>	secure of <wince network connection detail>	Returns a boolean describing the security level of the current connection for the specified WinCE network. If TRUE, the connection is secure.
<wince network connection detail>	signal quality of <wince network connection detail>	Returns the signal quality of the specified WinCE network connection. This is an integer between 0 and 255, with 255 indicating the best signal quality.
<wince network connection detail>	source network of <wince network connection detail>	Returns a string containing the GUID of the source network for the specified WinCE connection.
<wince network connection detail>	status of <wince network connection detail>	Returns the status of the specified WinCE network connection. This is a string indicating whether the connection is established, suspended, disconnected, waiting, failed or more. These are explained in greater detail in the MSDN article on the Connection Manager Status Constants.
<wince network connection detail>	type of <wince network connection detail>	Returns the type of the specified WinCE network connection. This is a string indicating a cellular, NIC, Bluetooth, Unimodem, VPN, Proxy or PC connection. These are explained in greater detail in the MSDN article on the Connection Manager Connection Type Constants.
<wince_web_browser>	version of <wince_web_browser>	Returns the version of the current web browser on the Windows CE device.
<world>	backup battery	Returns an inspectable object corresponding to the backup battery of the Windows Mobile device. The backup battery takes over should the main battery run out of charge.
<world>	battery	Returns a global object corresponding to the main battery of the Client Windows Mobile device.

Type	Inspector Name	Description
<world>	default web browser	Returns a global object corresponding to the WinCE web browser installed on the Client Windows Mobile device. Windows Embedded CE uses IE, which has been optimized for WinCE devices.
<world>	gps	Returns a global object corresponding to the gps device in the Client Windows Mobile phone.
<world>	network connection	Returns a global object corresponding to the network connection of the Client Windows Mobile device.
<world>	oma csp	Returns a global object corresponding to the OMA CSP of the Client Windows Mobile device.
<world>	oma csp <(string, string)>	Returns a global object corresponding to the OMA CSP of the Client Windows Mobile device. This version of the Inspector takes two string arguments.
<world>	oma csp <(string, string, string)>	Returns a global object corresponding to the OMA CSP of the Client Windows Mobile device. This version of the Inspector takes three string arguments.
<world>	oma csp <(string, string, string, string)>	Returns a global object corresponding to the OMA CSP of the Client Windows Mobile device. This version of the Inspector takes four string arguments.
<world>	oma csp <string>	Returns a global object corresponding to the OMA CSP of the Client Windows Mobile device. This version of the Inspector takes a single argument that concatenates the desired parameters.
<world>	phone	Returns a global object corresponding to the Client Windows Mobile phone.

Part Four

Windows Mobile Settings

Changing Settings with Actions

You can use settings to change the value of the Mobile Client variables listed above. This is typically done in an Action Script using the general format:

```
setting "<name>"="value" on "<date>" for client
```

For the Mobile Client settings, this will look like:

```
setting "_BESClient_Resource_GPSEnable"="1" on "{now}" for client
```

In this formulation, "{now}" represents a substitution, and the current time will be inserted at run-time. For multiple values, use semicolons to separate them:

```
setting "_BESClient_Comm_PhoneConnectionPreference"="Wifi;*;Cellular;ActiveSync" on
"{now}" for client
```

Changing Settings from the Console

You can also change settings manually in the BigFix Console by following these steps:

1. Click the **Computers** tab in the Console.
2. From the list, right-click the desired Mobile Client(s).
3. From the pull-down menu, select **Edit Computer Settings**.
4. In the dialog box, click **Add**.
5. From the **Add Custom Setting** dialog, enter the **Name** and the **Value**(s) you want.
6. Click **OK** and supply your password to propagate the setting to the Client(s).

New Client Settings

The following new settings have been added for mobile devices.

Phone Connection Preference

Setting:

Name: _BESClient_Comm_PhoneConnectionPreference
Values: Wifi, ActiveSync, Ethernet, Cellular, Bluetooth, VPN, Unimodem, *
Default: Wifi;*

Effect:

This setting controls the connection preferences for windows mobile clients. This setting is basically a semicolon-delimited list of connection types in order of preference, e.g. “Wifi;*”. The client will attempt to connect to the server using the connection type listed first. If that fails the client moves on to the next connection type. The asterisk can be used to allow the ConnectionManager to automatically decide the best connection type to use.

Use Low Priority Connection

Setting:

Name: _BESClient_Comm_UseLowPriorityConnection
Values: 0 or 1 (False or True)
Default: 0

Effect:

If true, the client will use a low priority data connection. This means that the client will not connect unless a connection already exists. If false, a connection will be attempted even if one doesn’t already exist.

Power Save Enable

Setting:

Name: _BESClient_Resource_PowerSaveEnable
Values: 0 or 1 (False or True)
Default: 0

Effect:

If true, the client will enter power-save mode as soon as each evaluation cycle is completed. The client will exit power-save mode upon receiving any Windows message or when the power-save timeout occurs. The timeout length depends on battery status and connection status and can be configured via the Lvl_X_PowerSaveTimeout settings. Power-save mode will be entered when EvaluationComplete becomes true and no current or pending commands are found. In power-save mode, the client sleeps (using the ControlManager::Sleep() function) for 1 minute intervals, during which it will still react to any Windows message that may be received. At the end of each interval, the current connection and battery statuses are used to evaluate whether the client will exit power-save mode. At the end of the power-save mode the client will set the TriggerConnectionEvent and continue until it is time to enter power-save mode again.

Run Full Speed When Client Idle

Setting:

Name: _BESClient_Resource_RunFullSpeedWhenUserIdle
Values: 0 or 1 (False or True)
Default: 1 for WinCE

Effect:

If true, the client will not limit the CPU usage when the user is idle.

Power Save Timeout 0

Setting:

Name: _BESClient_Resource_PowerSaveTimeout0
Values: 0 – MaxUint32 minutes
Default: 10

Effect:

This is the timeout value (in minutes) that will be used in power-save mode when the device is connected and charging.

Power Save Timeout 1

Setting:

Name: _BESClient_Resource_PowerSaveTimeout1
Values: 0 – MaxUint32 minutes
Default: 20

Effect:

This is the timeout value (in minutes) that will be used in power-save mode when the device is not connected and charging.

Power Save Timeout 2

Setting:

Name: _BESClient_Resource_PowerSaveTimeout2
Values: 0 – MaxUint32 minutes
Default: 60

Effect:

This is the timeout value (in minutes) that will be used in power-save mode when the device is connected and the battery level is high or normal.

Power Save Timeout 3

Setting:

Name: _BESClient_Resource_PowerSaveTimeout3
Values: 0 – MaxUint32 minutes
Default: 12 hours

Effect:

This is the timeout value (in minutes) that will be used in power-save mode when the device is not connected and the battery level is high or normal.

Power Save Timeout 4

Setting:

Name: _BESClient_Resource_PowerSaveTimeout4
Values: 0 – MaxUint32 minutes
Default: 24 hours

Effect:

This is the timeout value (in minutes) that will be used in power-save mode when the device is connected and the battery level is low.

Power Save Timeout 5

Setting:

Name: _BESClient_Resource_PowerSaveTimeout5
Values: 0 – MaxUint32 minutes
Default: 2 days

Effect:

This is the timeout value (in minutes) that will be used in power-save mode when the device is not connected and the battery level is low.

Enable Gps

Setting:

Name: _BESClient_Resource_GPSEnable
Values: 0 or 1 (False or True)
Default: 0

Effect:

If true, the client will turn on the GPS device if any. When set to false (or deleted) the GPS device is turned off.

Settings with different default values

Name: _BESClient_Comm_CommandPollEnable
Default: 1 (True)

Part Five

Resources

Troubleshooting

My Mobile Device won't Connect to the BES Server on a WiFi Network

In some environments, the phone may not correctly connect to the BES Server. The issue can be easily resolved by adding an entry into the 'Hosts' section of the Windows Mobile 6 registry. Editing the registry is straightforward, but comes with the usual warnings. Follow these steps:

7. Download a Registry Editor for the mobile device.
8. Open the registry using the editor and navigate to the following location: HKLM\Comm\Tcpip\Hosts\.
9. Create a KEY under the server's hostname and create a binary value under the hostname called **ipaddr**.
10. Add the binary value for the IP Address. Note that the value is the HEX conversion of the IP address (e.g. "c0 a8 01 02" which stands for 192.168.1.2).

Alternatively, you can download a utility to set the hostname. A utility called Pocket Hosts by Zimmerman can be found in the following location:
http://handheld.softpedia.com/progDownload/Pocket-Hosts-Download-8804.html

You can also set the host resolution for BigFix relays once the phone registers by modifying the *_BESClient_Relay_NameOverride* setting.

After the phone registers with the BigFix server, the setting _BESClient_Relay_NameOverride can be set on a BigFix relay. Use the IP address of that relay to avoid having to set the host resolution for future relays.

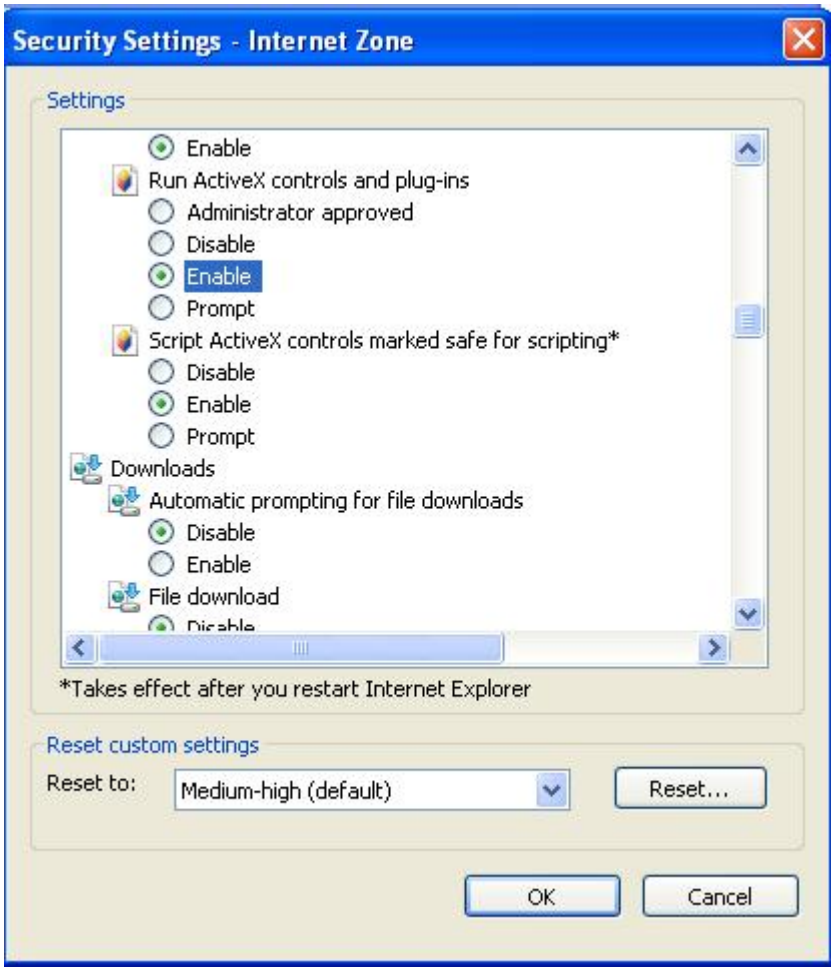
I Accidentally Removed the CSP Tool

If you accidentally remove the CSP tool, you will not be able to use any of the related Fixlet messages or Tasks. You can recover the tool with a Fixlet:

1. In the Console, click the Fixlet Messages tab.
2. Find Fixlet #99, "Download BigFix Configuration Service Provider Tool".
3. Click the Action link to download the specified utility.

I received an "Automation server can't create object" Error

If you receive this error after attempting to apply an Action , you need to enable two Internet Explorer security settings. Specifically, you need to enable both “Run ActiveX control and plug-ins” and “Script ActiveX controls marked safe for scripting”.



I have a Proxy Issue

BigFix attempts to collect proxy information from the connection manager and configure it properly. However, when there is a username and password set in the connection manager and automatic proxy detection is enabled, the client may misconfigure the proxy settings. To fix it, set the proxy information manually.

Global Support

BigFix offers a suite of support options to help optimize your user-experience and success with this product. Here's how it works:

- First, check the BigFix website Documentation page:
- Next, search the BigFix Knowledge Base for applicable articles on your topic:
- Then check the User Forum for discussion threads and community-based support:

If you still can't find the answer you need, contact BigFix's support team for technical assistance:

- Phone/US: 866 752-6208 (United States)
- Phone/International: 661 367-2202 (International)
- Email: enterprisesupport@bigfix.com

Index

