IBM Mobile Tablet for Retail Systems Management Guide

Version Code: V1.5

Currency Statement This version of the document was printed from an on-line system and must only be used for reference purposes. The official copy of this document is the on-line version. Please preserve the integrity of the documentation by destroying any obsolete versions and by not removing any pages from this printed copy

Summary of Changes

Changes resulting in document revisions will be summarized in this table in reverse chronological sequence. Revision bars (|) will highlight the text changed in new document versions.

Version	Approval Date	Change Description
V1.0	05/16/05	Initial Release
V1.1		MBeans listed and described
V1.2		MBeans added and document reformatted for maintainability
V1.3		Updated formatting and title
V1.4		Adding new MBean properties and notifications
V1.5		Adding new notifications

Table of Contents

1. Introduction

1.1. Objective

This document explains what steps need to be done to install the Systems Management for the IBM Cart Mounted Consumer Services Webpad; and how to create policy files and use them within Systems Management.

1.2. Related Documentation

The following documents are referenced in this test plan or will be used during the planning and execution phases of this test:

IBM Cart Mounted Consumer Service System Functional Specification 1.1 (May 28, 2004)

Remote Management Agent and Viewer User’s Guide Second Edition (March 2005)

2. Installing Systems Management

2.1. Requirements

To install the Remote Management Agent and Viewer for the Consumer Services Webpad, the server needs to be running either Windows or Linux, running the Websphere Application Server version 5.1.1.2.

More detailed requirements are described in Chapter Three of the Remote Master Agent and Viewer User's Guide.

2.2. Installing the Remote Management Agent and Viewer on the Server

The Remote Management Agent and Viewer can be installed interactively or silently for both Windows and Linux, documented in Chapter Four of the Remote Master Agent and Viewer User's Guide. The interactive installation instructions for Windows begin on page 31, and on page 33 for Linux. The silent installation instructions for both operating systems are on page 35.

2.3. Deploying the Remote Management Viewer in the Websphere Application Server

The Remote Management Viewer needs to be deployed to the Enterprise Applications in the Websphere Application Server before it can be used. The instructions for configuring Websphere and deploying the Viewer are described in Chapter Six of the Remote Master Agent and Viewer User's Guide.

2.4. Accessing the Remote Management Viewer

With the Websphere Application Server running and the Remote Management Viewer deployed, the Viewer can be accessed at the server's web address on port 9080 and the si folder. For example, to access it on the server itself, the address would be http://127.0.0.1:9080/si.

The Remote Management Viewer supports Mozilla and Internet Explorer.

2.5. System Management MBeans for the Consumer Services Webpad

The MBeans and their properties for the Consumer Services Webpad are documented in the IBM Cart Mounted Consumer Service System Functional Specification.

3. Creating a Policy File

There are several policies that are supported to update the tablet. This section describes what updates can be done and how to create a policy file for that update.

3.1. *Update Types*

The following components can be updated. The commands that follow the components are to be used for updating the respective components.

1. Client Stack: stack_update
2. BIOS: flashBIOS
3. EC: flashEC
4. Location (IR): flashIR
5. Scanner Firmware: flashScanner
6. Scanner Bluetooth Module: flashScannerBT
7. Custom software: custom_deploy

These commands require that the file for the update is available on an FTP or HTTP server accessible by the Customer Services Webpad.

3.2. *Creating an Update Policy File*

A sample file for all the updates are in Appendix A, and require the same changes no matter which update you wish to run. For example, follow the following steps to create a bios update policy.

1. Copy the sample policy file for the update type desired from Appendix A. In this case, copy the BIOS policy and name it bios_update_policy.xml.
2. In the *SoftwarePolicy:Installation* section, find the *SoftwarePolicy: Exec* line.
3. Change the <*URL*> field to the URL of the file to use for the update. An FTP or HTTP address is required. If the FTP server has a user ID and password, use:
   ftp://<UserID>:<Password>@<ServerAddress>/<FileLocation>
   Everything in <> is a required parameter, so using the same format as the example in Appendix A, this BIOS file could be accessible through the following sample URL:
   ftp://almond:passw0rd@192.168.0.1/c/flash/bios/al2rel26.rom
4. Save the file and exit the editor.

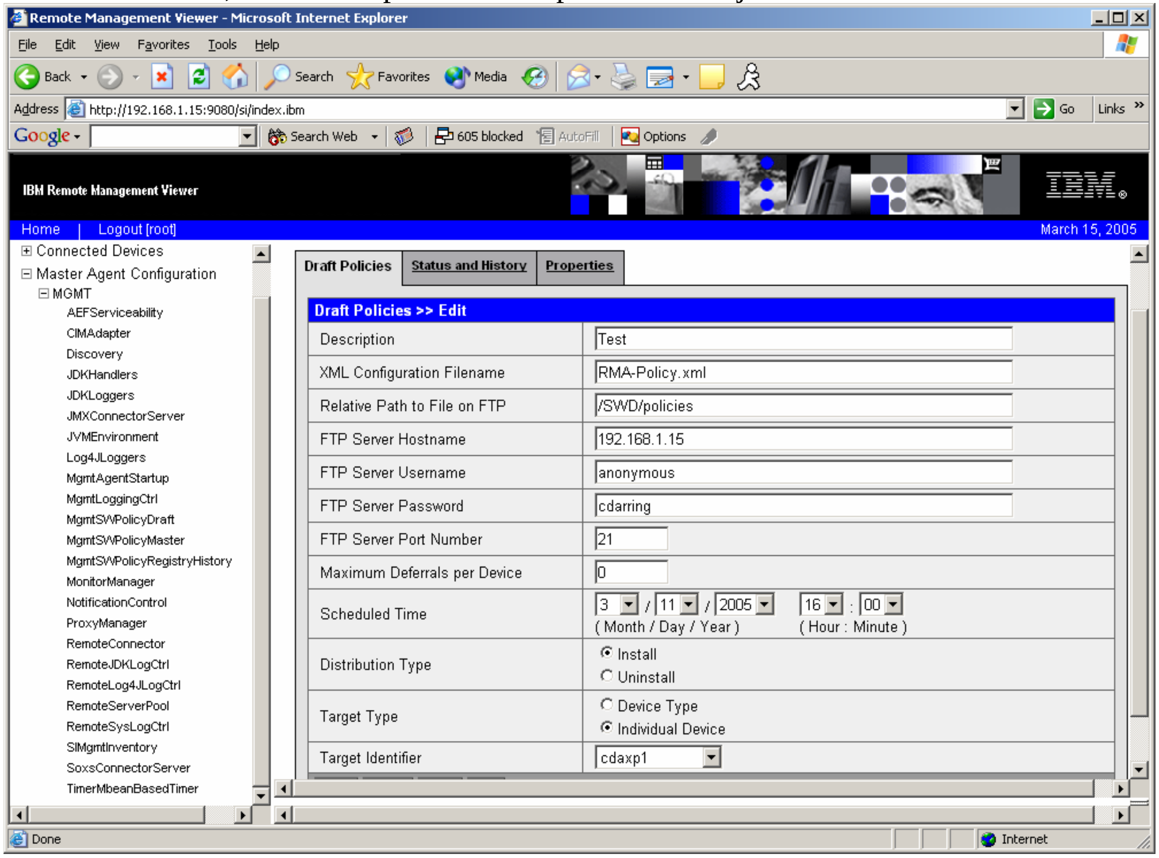
4. Using a Policy File

4.1. Add a Policy File in the Remote Management Viewer

Follow these steps to add a policy file to the Remote Management Viewer.

1. Put the policy XML file on an FTP server the Consumer Services Webpad has access to.
2. Login to the Remote Management Viewer.
3. Navigate to Master Agent Configuration->MGMT->MgmtSWPolicyMaster.
4. Under Draft policies, click Add.
5. Enter in all of the following information:
    a. The Description should be a short description of the policy.
    b. The XML Configuration Filename is just the filename of the policy file.
    c. The Relative Path to file on FTP is the directory the file is in once an FTP connection is made (what you would cd to).
    d. The FTP Server Hostname, Username, Password & Port Number are used to access and log into the server.
    e. The Maximum Deferrals per Device is the number of times the policy can be deferred.
    f. The Scheduled Time is the time after which any tablet that gets this policy will apply it. Any tablet that receives this policy after that time will attempt to apply the policy immediately.
    g. The Distribution Type for the Webpad will always be installation. To change back to a previous level will always be an installation of the previous level.
    h. The Target Type and Target Identifier are tied together. If the Target Type is Device Type, the Target Identifier will be Consumer, and the policy will be applied to all Webpads. If the Target Type is Induvidual Device, the Target Identifier will be the MAC address of a specific Webpad.

6. After the information has been entered, the information will look something like this. For the screenshot below, the tablet update will be performed on just one tablet.



Draft Policies >> Edit

Description	Test
XML Configuration Filename	RMA-Policy.xml
Relative Path to File on FTP	/SWD/policies
FTP Server Hostname	192.168.1.15
FTP Server Username	anonymous
FTP Server Password	cdarring
FTP Server Port Number	21
Maximum Deferrals per Device	0
Scheduled Time	3 / 11 / 2005 (Month / Day / Year) 16 : 00 (Hour : Minute)
Distribution Type	● Install ○ Uninstall
Target Type	○ Device Type ● Individual Device
Target Identifier	cdaxp1

7. Click Save once the information is correct.

4.2. Create a Policy from an Existing Policy

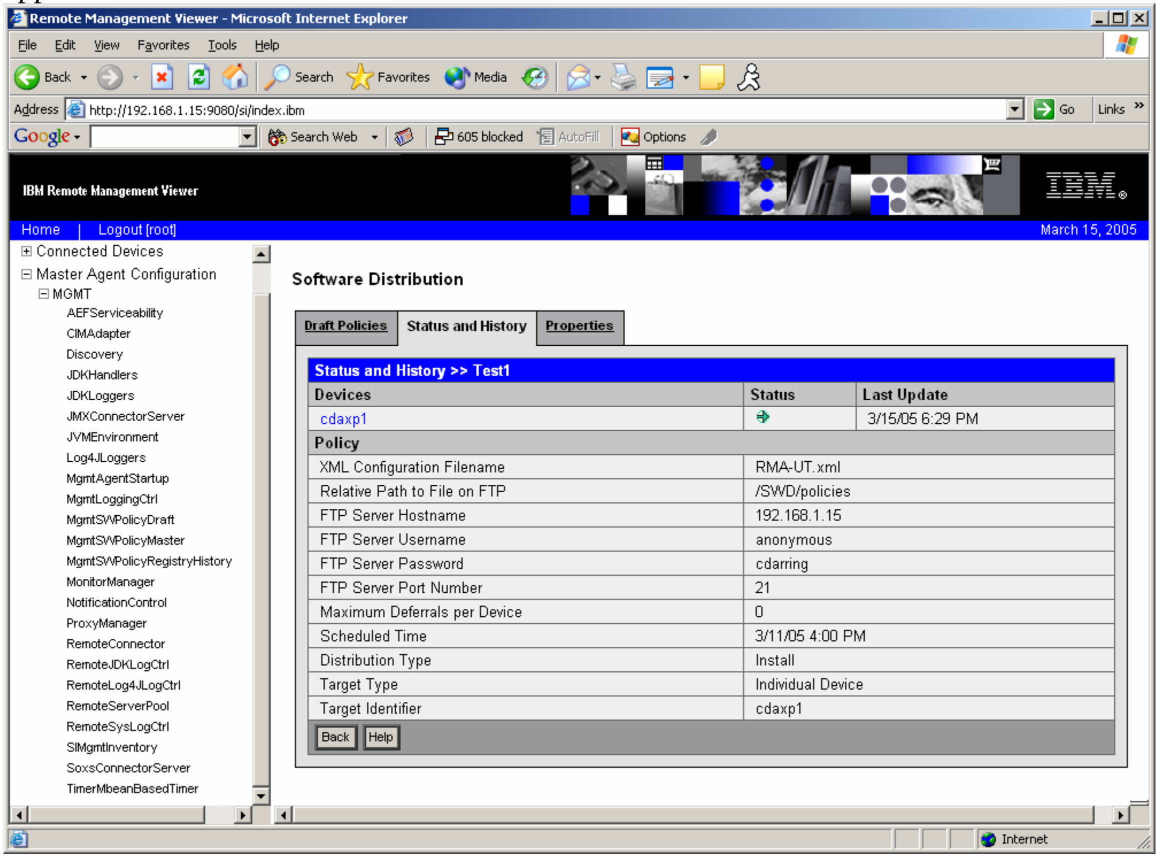
If there is an existing policy file that is either a draft or has been run that has the information needed, it can be copied into a new draft policy.

1. If there is a new policy file, put it on an FTP server the Consumer Services Webpad has access to.
2. Login to the Remote Management Viewer.
3. Navigate to Master Agent Configuration->MGMT->MgmtSWPolicyMaster.
4. If the existing policy is a running policy, click on the Status and History tab. Otherwise, if it is from another draft, leave it on the Draft Policies tab.
5. Select the check box next to the policy file and then click the Copy button to copy it.
6. In the Draft Policies tab, a new policy will be listed as (Copy) <Copied policy's name>. Click on the check box next to the policy and click Edit to make any changes required. The fields are the same as described in section 4.1 from above.
7. Once done making any changes to the policy, click the Save button.

4.3. Activating a Policy

Once a policy has been created and is ready for use, the following steps should be used to activate it.

1. From Draft policies, click on the check box next to the policy to run and click on Activate.
2. Once activated, your policy will be removed from drafts and will be displayed under Status and History. Click on that tab to view all activated policies.
3. Clicking on the activated policy will bring up details about it, including links for each affected device. The Status should indicate how the policy is affecting each device the policy applies to.

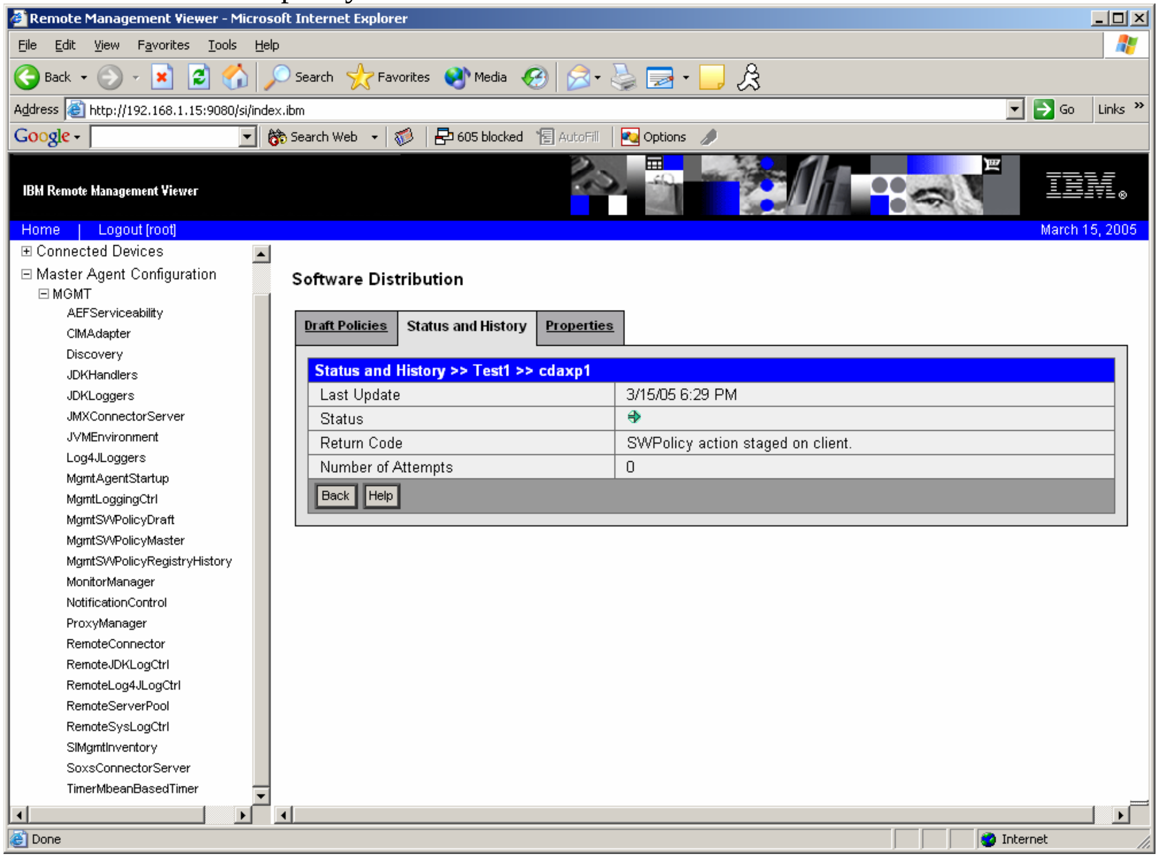


Status and History >> Test1

Devices	Status	Last Update
cdaxp1	➜	3/15/05 6:29 PM

Policy	
XML Configuration Filename	RMA-UT.xml
Relative Path to File on FTP	/SWD/policies
FTP Server Hostname	192.168.1.15
FTP Server Username	anonymous
FTP Server Password	cdarring
FTP Server Port Number	21
Maximum Deferrals per Device	0
Scheduled Time	3/11/05 4:00 PM
Distribution Type	Install
Target Type	Individual Device
Target Identifier	cdaxp1

4. Clicking on the device link will bring up details for the execution of the policy on that device, including the return code for that policy once the attempt to run the policy is complete. It should indicate if the policy succeeded or failed.


Remote Management Viewer - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.15:9080/si/index.ibm
Go Links
Google Search Web 605 blocked AutoFill Options
IBM Remote Management Viewer
IBM
Home | Logout [root]
March 15, 2005
Done
Internet

- ⊞ Connected Devices
- ⊟ Master Agent Configuration
  - ⊟ MGMT
    - AEFServiceability
    - CIMAdapter
    - Discovery
    - JDKHandlers
    - JDKLoggers
    - JMXConnectorServer
    - JVMEnvironment
    - Log4JLoggers
    - MgmtAgentStartup
    - MgmtLoggingCtrl
    - MgmtSWPolicyDraft
    - MgmtSWPolicyMaster
    - MgmtSWPolicyRegistryHistory
    - MonitorManager
    - NotificationControl
    - ProxyManager
    - RemoteConnector
    - RemoteJDKLogCtrl
    - RemoteLog4JLogCtrl
    - RemoteServerPool
    - RemoteSysLogCtrl
    - SIMgmtInventory
    - SoxsConnectorServer
    - TimerMbeanBasedTimer

Software Distribution

Draft Policies | Status and History | Properties

Status and History >> Test1 >> cdaxp1

Last Update	3/15/05 6:29 PM
Status	➔
Return Code	SWPolicy action staged on client.
Number of Attempts	0

Back Help

5. Appendix A Update Policy Files

5.1. Client Stack Update Policy

```
<SoftwarePolicy:SoftwarePolicy
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="http://www.pc.ibm.com/ibm/si/mgmt/com/ibm/retail/si/mgmt/swdist/SWPolicyXMLSchema.xsd"
       xmlns:SoftwarePolicy="http://www.pc.ibm.com/ibm/si/mgmt">

       <SoftwarePolicy:SWPolicyDescriptor policyID="007">
              <SoftwarePolicy:Description>Policy for updating the tablet software stack</SoftwarePolicy:Description>
       </SoftwarePolicy:SWPolicyDescriptor>

       <SoftwarePolicy:SWPolicyTarget targetOS="PSA" family="StackUpdate" precompress="false" >

              <SoftwarePolicy:Installation>

                     <!--
                     Replace the <URL> field below with an actual path before using
                     Example URLs
                     ftp://user:password@192.169.0.10/update/<filename>
                     http://192.168.0.10:8080/update/<filename>
                     http://user:password@192.168.0.10/update/<filename>
                     Example filename: RSS-RELEASE-05-24-2005-1803.bin
                     -->
                     <SoftwarePolicy:Exec executable="stack_update <URL>" expectedRC="0" />
                     <SoftwarePolicy:Reboot
                            expectedRC="ok"
                            rcFile="success"
                            failureLog="failure"/>
              </SoftwarePolicy:Installation>

              <SoftwarePolicy:DeInstallation>
                     <SoftwarePolicy:Reboot/>
              </SoftwarePolicy:DeInstallation>

       </SoftwarePolicy:SWPolicyTarget>
</SoftwarePolicy:SoftwarePolicy>
```

5.2. BIOS Update Policy

```
<SoftwarePolicy:SoftwarePolicy
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="http://www.pc.ibm.com/ibm/si/mgmt/com/ibm/retail/si/mgmt/swdist/SWPolicyXMLSchema.xsd"
       xmlns:SoftwarePolicy="http://www.pc.ibm.com/ibm/si/mgmt">

       <SoftwarePolicy:SWPolicyDescriptor policyID="007">
              <SoftwarePolicy:Description>Policy for updating the tablet BIOS firmware</SoftwarePolicy:Description>
       </SoftwarePolicy:SWPolicyDescriptor>

       <SoftwarePolicy:SWPolicyTarget targetOS="PSA" family="StackUpdate" precompress="false" >

              <SoftwarePolicy:Installation>

                     <!--
                     Replace the <URL> field below with an actual path before using
                     Example URLs
                     ftp://user:password@192.169.0.10/update/<filename>
                     http://192.168.0.10:8080/update/<filename>
                     http://user:password@192.168.0.10/update/<filename>
                     Example filename: bios.rom
                     -->
                     <SoftwarePolicy:Exec executable="flashBIOS <URL>" expectedRC="0" />
                     <SoftwarePolicy:Reboot
                            expectedRC="ok"
                            rcFile="firmware.success"
                            failureLog="firmware.failure"/>
              </SoftwarePolicy:Installation>

              <SoftwarePolicy:DeInstallation>
                     <SoftwarePolicy:Reboot/>
              </SoftwarePolicy:DeInstallation>

       </SoftwarePolicy:SWPolicyTarget>
</SoftwarePolicy:SoftwarePolicy>
```

5.3. EC Update Policy

```xml
<SoftwarePolicy:SoftwarePolicy
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://www.pc.ibm.com/ibm/si/mgmt/com/ibm/retail/si/mgmt/swdist/SWPolicyXMLSchema.xsd"
        xmlns:SoftwarePolicy="http://www.pc.ibm.com/ibm/si/mgmt">

        <SoftwarePolicy:SWPolicyDescriptor policyID="007">
                <SoftwarePolicy:Description>Policy for updating the tablet EC firmware</SoftwarePolicy:Description>
        </SoftwarePolicy:SWPolicyDescriptor>

        <SoftwarePolicy:SWPolicyTarget targetOS="PSA" family="StackUpdate" precompress="false" >

                <SoftwarePolicy:Installation>

                        <!--
                        Replace the <URL> field below with an actual path before using
                        Example URLs
                        ftp://user:password@192.169.0.10/update/<filename>
                        http://192.168.0.10:8080/update/<filename>
                        http://user:password@192.168.0.10/update/<filename>
                        Example filename: ec.rom
                        -->
                        <SoftwarePolicy:Exec executable="flashEC <URL>" expectedRC="0" />
                        <SoftwarePolicy:Reboot
                                expectedRC="ok"
                                rcFile="firmware.success"
                                failureLog="firmware.failure"/>
                </SoftwarePolicy:Installation>

                <SoftwarePolicy:DeInstallation>
                        <SoftwarePolicy:Reboot/>
                </SoftwarePolicy:DeInstallation>

        </SoftwarePolicy:SWPolicyTarget>
</SoftwarePolicy:SoftwarePolicy>
```

5.4. Location (IR) Update Policy

```
<SoftwarePolicy:SoftwarePolicy
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://www.pc.ibm.com/ibm/si/mgmt/com/ibm/retail/si/mgmt/swdist/SWPolicyXMLSchema.xsd"
        xmlns:SoftwarePolicy="http://www.pc.ibm.com/ibm/si/mgmt">

        <SoftwarePolicy:SWPolicyDescriptor policyID="007">
                <SoftwarePolicy:Description>Policy for updating the tablet IR receiver firmware</SoftwarePolicy:Description>
        </SoftwarePolicy:SWPolicyDescriptor>

        <SoftwarePolicy:SWPolicyTarget targetOS="PSA" family="StackUpdate" precompress="false" >

                <SoftwarePolicy:Installation>

                        <!--
                        Replace the <URL> field below with an actual path before using
                        Example URLs
                        ftp://user:password@192.169.0.10/update/<filename>
                        http://192.168.0.10:8080/update/<filename>
                        http://user:password@192.168.0.10/update/<filename>
                        Example filename: ir.hex
                        -->
                        <SoftwarePolicy:Exec executable="flashIR <URL>" expectedRC="0" />
                        <SoftwarePolicy:Reboot
                                expectedRC="ok"
                                rcFile="firmware.success"
                                failureLog="firmware.failure"/>
                </SoftwarePolicy:Installation>

                <SoftwarePolicy:DeInstallation>
                        <SoftwarePolicy:Reboot/>
                </SoftwarePolicy:DeInstallation>

        </SoftwarePolicy:SWPolicyTarget>
</SoftwarePolicy:SoftwarePolicy>
```

5.5. Custom Software Deployment Policy

```
<SoftwarePolicy:SoftwarePolicy
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="http://www.pc.ibm.com/ibm/si/mgmt /com/ibm/retail/si/mgmt/swdist/SWPolicyXMLSchema.xsd"
       xmlns:SoftwarePolicy="http://www.pc.ibm.com/ibm/si/mgmt">

       <SoftwarePolicy:SWPolicyDescriptor policyID="007">
              <SoftwarePolicy:Description>Policy for deploying custom files into a protected storage area
              </SoftwarePolicy:Description>
       </SoftwarePolicy:SWPolicyDescriptor>

       <SoftwarePolicy:SWPolicyTarget targetOS="PSA" family="StackUpdate" precompress="false">
              <!--
              Modify the server path and the resource tarball filename below.
              The path is relative to the FTP server on which the policy file exists.
              The resource tarball can have any name, but must be a valid .tar.gz archive.
              It may contain subdirectories, HTML, media, etc. After it has been deployed,
              it will be accessible by the browser at file://localhost/custom/*
              Examples:     ftpPath=/home/sbinst
                            filename=pierce.tgz
              -->
              <SoftwarePolicy:SWPolicyResourceFiles ftpPath="<server path>">
                     <SoftwarePolicy:Component filename="<resource tarball>"/>
              </SoftwarePolicy:SWPolicyResourceFiles>

              <SoftwarePolicy:Installation>
                     <!--
                     Modify the resource tarball filename below. It must match the resource tarball
                     filename specified in the SWPolicyResourceFiles tag.
                     Example: executable="custom_deploy pierce.tgz"
                     -->
                     <SoftwarePolicy:Exec executable="custom_deploy <resource tarball>"
                            expectedRC="ok"
                            rcFile="custom.success"
                            failureLog="customer.failure" />

              </SoftwarePolicy:Installation>
              <SoftwarePolicy:DeInstallation>
                     <SoftwarePolicy:Reboot/>
              </SoftwarePolicy:DeInstallation>
       </SoftwarePolicy:SWPolicyTarget>
</SoftwarePolicy:SoftwarePolicy>
```

5.6. *Custom Software Clearing Policy*

```
<SoftwarePolicy:SoftwarePolicy
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="http://www.pc.ibm.com/ibm/si/mgmt /com/ibm/retail/si/mgmt/swdist/SWPolicyXMLSchema.xsd"
       xmlns:SoftwarePolicy="http://www.pc.ibm.com/ibm/si/mgmt">

       <SoftwarePolicy:SWPolicyDescriptor policyID="007">
              <SoftwarePolicy:Description>Policy for clearing the custom file deployment area</SoftwarePolicy:Description>
       </SoftwarePolicy:SWPolicyDescriptor>

       <SoftwarePolicy:SWPolicyTarget targetOS="PSA" family="StackUpdate" precompress="false">

              <SoftwarePolicy:Installation>
                     <SoftwarePolicy:Exec executable="custom_clear"
                            expectedRC="ok"
                            rcFile="custom.success"
                            failureLog="customer.failure" />

              </SoftwarePolicy:Installation>
              <SoftwarePolicy:DeInstallation>
                     <SoftwarePolicy:Reboot/>
              </SoftwarePolicy:DeInstallation>
       </SoftwarePolicy:SWPolicyTarget>
</SoftwarePolicy:SoftwarePolicy>
```

5.7. Scanner Firmware Update Policy

```
<SoftwarePolicy:SoftwarePolicy
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="http://www.pc.ibm.com/ibm/si/mgmt/com/ibm/retail/si/mgmt/swdist/SWPolicyXMLSchema.xsd"
       xmlns:SoftwarePolicy="http://www.pc.ibm.com/ibm/si/mgmt">

       <SoftwarePolicy:SWPolicyDescriptor policyID="007">
              <SoftwarePolicy:Description>Policy for updating the scanner firmware</SoftwarePolicy:Description>
       </SoftwarePolicy:SWPolicyDescriptor>

       <SoftwarePolicy:SWPolicyTarget targetOS="PSA" family="StackUpdate" precompress="false" >

              <SoftwarePolicy:Installation>

                     <!--
                     Replace the <URL> field below with an actual path before using.
                     Example URLs
                     ftp://user:password@192.169.0.10/update/scanner.ibm
                     http://192.168.0.10:8080/update/scanner.ibm
                     http://user:password@192.168.0.10/update/scanner.ibm
                     -->
                     <SoftwarePolicy:Exec executable="flashScanner <URL>" expectedRC="0" />
                     <SoftwarePolicy:Reboot
                            expectedRC="ok"
                            rcFile="firmware.success"
                            failureLog="firmware.failure"/>
              </SoftwarePolicy:Installation>

              <SoftwarePolicy:DeInstallation>
                     <SoftwarePolicy:Reboot/>
              </SoftwarePolicy:DeInstallation>

       </SoftwarePolicy:SWPolicyTarget>

</SoftwarePolicy:SoftwarePolicy>
```

5.8. Scanner Bluetooth Module Firmware Update Policy

```
<SoftwarePolicy:SoftwarePolicy
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="http://www.pc.ibm.com/ibm/si/mgmt/com/ibm/retail/si/mgmt/swdist/SWPolicyXMLSchema.xsd"
       xmlns:SoftwarePolicy="http://www.pc.ibm.com/ibm/si/mgmt">

       <SoftwarePolicy:SWPolicyDescriptor policyID="007">
              <SoftwarePolicy:Description>Policy for updating the scanner Bluetooth module firmware</SoftwarePolicy:Description>
       </SoftwarePolicy:SWPolicyDescriptor>

       <SoftwarePolicy:SWPolicyTarget targetOS="PSA" family="StackUpdate" precompress="false" >

              <SoftwarePolicy:Installation>

                     <!--
                     Replace the <URL> field below with an actual path before using.
                     Example URLs
                     ftp://user:password@192.169.0.10/update/scanner-bt.ibm
                     http://192.168.0.10:8080/update/scanner-bt.ibm
                     http://user:password@192.168.0.10/update/scanner-bt.ibm
                     -->
                     <SoftwarePolicy:Exec executable="flashScannerBT <URL>" expectedRC="0" />
                     <SoftwarePolicy:Reboot
                            expectedRC="ok"
                            rcFile="firmware.success"
                            failureLog="firmware.failure"/>
              </SoftwarePolicy:Installation>

              <SoftwarePolicy:DeInstallation>
                     <SoftwarePolicy:Reboot/>
              </SoftwarePolicy:DeInstallation>

       </SoftwarePolicy:SWPolicyTarget>
</SoftwarePolicy:SoftwarePolicy>
```

6. Appendix B MBean List

For Properties, **(rw)** indcates a readable and writable property and **(r)** indicates a read-only property.

Properties marked as N/A are not collected for any of the following reasons:

- The information cannot currently be extracted from the associated hardware
- The information is not applicable to the hardware

For Actions, any parameters required for the action are between parenthesis, such as **(String)**. If there are no parameters for the action, there is nothing between the parenthesis.

6.1. Browser

Property		Description
BackgroundColor	rw	The default background color. Value should be in the form: “Red=<value>,Green=<value>,Blue=<value>” where the values range from 0 to 255 in intensity.
BrowserMemoryUsedKB	r	The number of Kilobytes of memory currently in use by the browser.
FontSize	rw	The default font size.
FtpProxy	rw	If enabled, the proxy URL to use for the FTP protocol.
FtpProxyEnable	rw	Whether to use a proxy for the FTP protocol.
HighBrowserMemoryThreshold	rw	The number of Kilobytes of memory which must be used by the browser before a high memory usage notification is raised.
HomePage	rw	The browser home page URL.
HttpProxy	rw	If enabled, the proxy URL to use for the HTTP protocol.
HttpProxyEnable	rw	Whether to use a proxy for the HTTP protocol.
HttpsProxy	rw	If enabled, the proxy URL to use for the HTTPS protocol.
HttpsProxyEnable	rw	Whether to use a proxy for the HTTPS protocol.
LinkUnvisitedColor	rw	If enabled, the default color in which to display hyperlinks that have not been visited.
LinkUnvisitedHasColor	rw	Whether to enable default coloring for hyperlinks that have not been visited.
LinkVistedColor	rw	If enabled, the default color in which to display hyperlinks that have been visited.
LinkVisitedHasColor	rw	Whether to enable default coloring for hyperlinks that have been visited.
NoProxyServerCheck	rw	Whether to exclude proxy servers in the NoProxyServers list.
NoProxyServers	rw	If enabled, a comma delimited list of proxy servers to exclude.
OperaClasspath	rw	The Opera JVM classpath.

UnvistedHasStrikeThrough	rw	Whether to enable strikethrough (~~example~~) for hyperlinks that have not been visited.
UnvisitedHasUnderline	rw	Whether to enable underline (example) for hyperlinks that have not been visited.
VistitedHasStrikeThrough	rw	Whether to enable strikethrough (~~example~~) for hyperlinks that have been visited.
VisitedHadUnderline	rw	Whether to enable underline (example) for hyperlinks that have been visited.

6.2. Clock

Property		Description
Day	rw	The numeric representation of the system clock day (1-31).
Hour	rw	The numeric representation of the system clock hour (0-23).
Minute	rw	The numeric representation of the system clock minute (0-59).
Month	rw	The numeric representation of the system clock month (1-12).
Second	rw	The numeric representation of the system clock second (0-59).
Year	rw	The numeric representation of the system clock year (4 digits).

6.3. Disk

Property		Description
AvailableKB	r	The number of kilobytes of persistent storage not in use.
BuildNumber	r	N/A
CurrentState	r	N/A
Description	r	A description of the inventory item.
FixLevel	r	N/A
InstallationDate	r	N/A
MajorVersion	r	N/A
Manufacturer	r	N/A
MinorVersion	r	N/A
ProductName	r	The name of the hardware product.
SerialNumber	r	The serial number of the hardware.
TotalKB	r	The number of kilobytes of persistent storage.
UsedKB	r	The number of kilobytes of persistent storage in use.
Utilization	r	The percentage used of persistent storage.
Version	r	The version of the hardware product.

6.4. Lcd

Property		Description
BrightnessLevelPercent	rw	The brightness level (percent of maximum) of the LCD backlight.

6.5. LedGreen

Property		Description
DutyCycle	rw	The duty cycle of the LED blink period in milliseconds.
Period	rw	The period of the LED blink in milliseconds.
State	rw	Whether the LED should be on or off. 1=on; 0=off.

Examples

DutyCycle=500, Period=1000, State=1 -- On for .5 seconds per second
DutyCycle=500, Period=1000, State=0 -- Full off (State takes precedence)

Action	Description
blink()	Simple method to start the LED blinking
clear()	Simple method to turn off the LED

6.6. LedOrange

Property		Description
DutyCycle	rw	The duty cycle of the LED blink period in milliseconds.
Period	rw	The period of the LED blink in milliseconds.
State	rw	Whether the LED should be on or off. 1=on; 0=off.

Examples

DutyCycle=500, Period=1000, State=1 -- On for .5 seconds per second
DutyCycle=500, Period=1000, State=0 -- Full off (State takes precedence)

Action	Description
blink()	Simple method to start the LED blinking.
clear()	Simple method to turn off the LED.

6.7. Location

Property		Description
IRReceiverFirmwareLevel	r	The IR (location) receiver firmware level.
LastBeaconBatteryLow	r	Whether the last beacon encountered and found within the store map reported a low battery level.
LastBeaconId	r	The identification code of the last beacon encountered and found within the store map.

6.8. LogReaper

The LogReaper allows the user to capture an archive of the tablet logs at the time of the reaping operation. The archive is then uploaded to an FTP server specified in the MBean parameters.

Property		Description
FTPServerHostname	rw	The hostname of a server which should receive the tablet logs.
LastOperationStatus	r	The status of the last attempted log reaping operation.
Password	rw	A password for the FTP server user.

ServerPath	rw	The directory path at which to upload the logs.
ServerPort	rw	The FTP server port.
Username	rw	A username for the FTP server.

Action	Description
reapLogsNow()	Execute the log reaping operation.

6.9. Memory

Property		Description
AvailableKB	r	The number of kilobytes of memory not in use.
BuildNumber	r	N/A
CurrentState	r	N/A
Description	r	N/A
FixLevel	r	N/A
InstallationDate	r	N/A
LoggingMemoryUsedKB	r	The number of kilobytes being used to host logging files.
MajorVersion	r	N/A
Manufacturer	r	N/A
MinorVersion	r	N/A
ProductName	r	N/A
SerialNumber	r	N/A
TempMemoryUsedKB	r	The number of kilobytes being used to host temporary files.
TotalKB	r	The number of kilobytes of memory.
UsedKB	r	The number of kilobytes of memory in use.
Utilization	r	The percentage used of memory.
Version	r	N/A

6.10. Processor

Property		Description
BuildNumber	r	N/A
CurrentState	r	N/A
Description	r	A description of the processor.
FixLevel	r	N/A
InstallationDate	r	N/A
MHz	r	The processor speed.
MajorVersion	r	N/A
Manufacturer	r	N/A
MinorVersion	r	N/A
ProductName	r	The product name of the processor.
SerialNumber	r	N/A
UtilizedPercentage	r	The processor utilization at the time of query.
Version	r	N/A

6.11. Scanner

Property		Description
AssociatedScannerAddress	r	The MAC address of any currently connected scanner. Contains an empty string when no scanner is connected.
BatteryPercentage	r	The last recorded battery level of the connected scanner.
BatteryThreshold	rw	The battery percentage level at which the scanner will begin generating battery level notifications.
DockedScannerAddress	r	The MAC address of the currently docked scanner. Contains an empty string when no scanner is docked.
PartneredScannerAddress	r	The MAC address of the scanner to which the tablet is partnered (at boot time).
ScannerBluetoothFirmwareLevel	r	The Bluetooth module firmware level of the connected scanner.
ScannerECFirmwareLevel	r	The firmware level of the connected scanner.

6.12. Tablet

Property		Description
BIOSBuildNumber	r	The BIOS level of the tablet.
BIOSReleaseDate	r	The BIOS release date.
BIOSVendor	r	The BIOS vendor.
BuildNumber	r	N/A
ClientStackVersion	r	The client stack version identifier.
CurrentState	r	N/A
Description	r	A description of the tablet.
ECFirmwareVersion	r	The embedded controller firmware level.
FixLevel	r	N/A
InstallationDate	rw	A field for maintaining the installation date of the tablet. This field can only be written using the methods provided in the actions section.
MajorVersion	r	N/A
Manufacturer	r	The manufacturer of the tablet.
MinorVersion	r	N/A
ProductName	r	The make and model of the tablet.
SerialNumber	r	The serial number of the tablet.
TabletID	r	A unique identifier for the tablet.
UUID	r	The UUID (universally unique identifier) of the tablet
Version	r	N/A

Action	Description
populateInstallationDate(String)	Populates the tablet installation date with the specified string.
poweroff()	Powers off the tablet.

reboot()	Reboots the tablet.
touchInstallationDate()	Sets the installation date of the tablet to the content of the tablet's system clock.

6.13. TabletBattery

Property		Description
BatteryPercentage (r)	r	The current tablet battery level percentage.
BatteryThreshold (rw)	rw	The battery percentage level at which the tablet will begin generating battery level notifications.

6.14. TabletRack

Property		Description
RackLocation	r	The current rack location if the tablet is docked. "Not Docked" if the tablet is not docked or there is an error reading the information.
RackNumber	r	The current rack number if the tablet is docked. "Not Docked" if the tablet is not docked or there is an error reading the information.
SlotNumber	r	The current rack slot number if the tablet is docked. "Not Docked" if the tablet is not docked or there is an error reading the information.
StoreNumber	r	The current rack store number if the tablet is docked. "Not Docked" if the tablet is not docked or there is an error reading the information.

Action	Description
repairSlot()	Repairs or clears (if repair is not possible) the current slot information.

6.15. Volume

Property		Description
VolumePercentage	rw	The volume level percentage of the sound system.

6.16. WirelessNetwork

Property		Description
Authentication	rw	The method of authentication to use when connected to the specified access point.
Channel	rw	The channel to use when connected to the access point.
CurrentIP	r	The current IP address of the wireless network connection.
DNS1	rw	The first DNS server to use.
DNS2	rw	The second DNS server to use.
DhcpEnable	rw	Whether to enable the use of DHCP.
Domain	rw	The domain to use.

EnableWep	rw	Whether to enable the use of WEP.
Enabled	rw	Whether to enable the wireless connection.
Gateway	rw	The network gateway to use.
IsConected	r	Whether the wireless network is current connected.
MACAddress	r	The MAC address associated with this wireless network connection.
Netmask	rw	The network netmask.
QualityLevel	r	The quality level of the wireless network connection.
SSID	rw	The SSID of the access point with which to connect.
StaticIP	rw	If DHCP is not enabled, the IP address to use.
Strength	r	The strength level of the wireless network connection.
Timeout	rw	The DHCP timeout period.
WEPKey	rw	If WEP is enabled, the WEP key to use.

6.17. WirelessNetworkAdapter

Property		Description
BuildNumber	r	N/A
CurrentState	r	N/A
Description	r	Description of the wireless network adapter.
FixLevel	r	N/A
InstallationDate	r	N/A
MACAddress	r	The MAC address of the wireless network adapter.
MajorVersion	r	N/A
Manufacturer	r	The manufacturer of the wireless network adapter.
MinorVersion	r	N/A
ProductName	r	The product name of the wireless network adapter.
SerialNumber	r	N/A
Version	r	The version of the wireless network adapter.

6.18. WirelessStatistics

Property		Description
CollisionCount	r	The number of collisions that have occurred.
CurrentAccessPoint	r	The access point that is currently associated.
RXInvalidCryptCount	r	The received packet invalid encryption count.
RXInvalidFrag	r	The received packet invalid fragment count.
RXInvalidNWIDCount	r	The received packet invalid NWID count.
RXPacketCount	r	The received packet count.
RXPacketDroppedCount	r	The received packet dropped count.
RXPacketErrorCount	r	The received packet error count.
RXPacketFrameCount	r	The received packet frame error count.
RXPacketOverrunCount	r	The received packet overruns count.
TXExxcessiveRetryCount	r	The transmission packet excessive retries count.
TXInvalidMiscCount	r	The transmission packet misc. invalid count.
TXMissedBeaconCount	r	The transmission packet missed beacon count.

TXPacketCarrierCount	r	The transmission packet carrier error count.
TXPacketCount	r	The transmission packet count.
TXPacketDroppedCount	r	The transmission packet dropped count.
TXPacketErrorCount	r	The transmission packet error count.
TXPacketOverrunCount	r	The transmission packet overruns count.
TXQueueLength	r	The transmission queue length.

7. Appendix C Notifications

Below are listed the systems management notifications generated by the MTR and the conditions under which they are sent.

7.1. Information

Notification	Condition
Tablet docked	Sent when the tablet detects that it has been docked into a charging rack.
Tablet undocked	Sent when the tablet detects that it has been undocked (removed) from a charging rack.
Scanner docked	Sent when the tablet detects that a scanner has been docked with the tablet.
Scanner undocked	Sent when the tablet detects that a scanner has been undocked from the tablet.
Reboot required	Sent when a setting is altered through the systems management interface that requires a tablet reboot before the setting will become active.

7.2. Warning

Notification	Condition
Tablet docked without scanner	Sent when the tablet detects that it has been docked without a docked (holstered) scanner.
Beacon battery low	A beacon was detected emitting the battery low signal.
Scanner driver exited	The Bluetooth scanner driver exited. This is typically indicative of a Bluetooth connection loss, but may be a scanner error. This condition typically recovers automatically.
Partnering errors	This is a group of notifications that report difficulties in establishing a scanner partner.
Memory key mechanism	This is a group of notifications that report errors during log reaping and other memory key operations.

7.3. Critical

Notification	Condition
Tablet battery level critical	Sent when the tablet detects that its battery level has fallen bellow the threshold set in the TabletBattery.BatteryThreshold MBean property. Sent on each percentage point of change while below the threshold.

Scanner battery level critical	Sent when the tablet detects that its scanner's (currently connected via Bluetooth) battery level has fallen bellow the threshold set in the Scanner.BatteryThreshold MBean property. Sent on each percentage point of change while below the threshold.
Browser crash	Sent when the tablet detects that the browser has restarted (e.g. in the case of a browser crash).
Browser memory threshold exceeded	A memory threshold has been exceeded by the browser. This may indicate a memory leak.
Unable to partner with scanner	The tablet has not yet been able to partner with a scanner.
Poor Bluetooth connection	The Bluetooth connection between the scanner and the tablet has failed several times in a short period of time.
USB takeover failure	The OS failed to takeover the USB subsystem.