RMA Cookbook

Using Remote Management Agent (RMA) 2.6

About this book:

This document includes tutorials and examples for using RMA in a real-world IBM POS environment. It includes information on installing, configuring, and using the systems management solution for IBM retail POS products.

The aim of this book is as follows:

- To make your life a little easier. It is sometimes difficult to navigate all the documentation that is available – and even more difficult to figure out how it all fits together. This guide should educate you on the end-to-end systems management solution, which always consists of many different components (e.g. the POS hardware, peripherals, firmware, system drivers, UPOS drivers, sensor drivers, RMA, IBM Director, various operating systems, etc.).

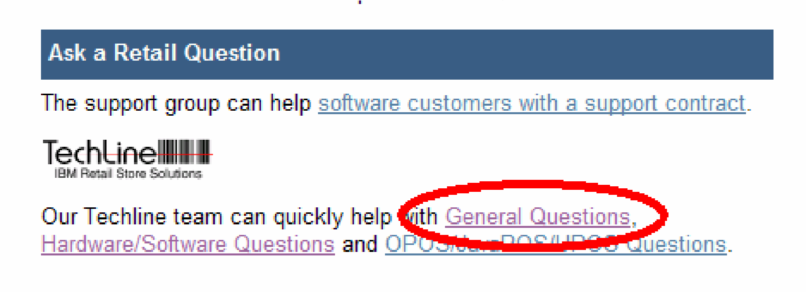
- To help you plan your RMA implementation. This book helps you understand what you can accomplish using RMA on Windows, Linux, and 4690. It also discusses the additional software and drivers that are required to monitor your POS hardware and to manage peripheral-attached devices via RMA.

- To give you step-by-step examples. Most chapters include realistic examples that illustrate the topics in that chapter. In many cases, these examples can be used to simplify your implementation, and/or to prepare demonstrations of the solution.

This document should be used as a supplement to the existing product-specific documentation for RMA, 4690, UPOS, IBM Director, etc. We have tried to avoid duplicating any significant content that is already covered in the existing publications. Links and references to other documents are included throughout the book. Overlap occurs only where necessary for the sake of clarity and/or readability.

Questions or comments?

Please contact the IBM technical sales support team using TechLine at http://www.ibm.com/retail/store/support. (Look for the section called “Ask a Retail Question”, and click on “General Questions”.)



Ask a Retail Question

The support group can help software customers with a support contract.

TechLine
IBM Retail Store Solutions

Our Techline team can quickly help with General Questions, Hardware/Software Questions and OPOS/JavaPOS/UPOS Questions.

Please note:

This document is a work in progress. Content is being added regularly, so check back for updates and/or additions.

Table of Contents:

Chapter 1 – Quick-Install Guide

These instructions describe the steps required to install the RMA general agent (GA), the RMA master agent (MA), and IBM Director Server. These instructions are for RMA version 2.6, and IBM Director 5.20.3 with service update 4.

This chapter assumes that the Windows operating system will be used for the GA, MA, and Director Server; however, it's possible to set up a mixed environment in which one or more of these components is running on a different operating system (4690 or Linux). To learn about using RMA in these other environments, you should first read and understand this chapter, then refer to one of the following: "**Chapter 2 – Setting Up RMA on 4690**", "**Chapter 3 – Setting Up RMA on Novell Linux**", or "**Chapter 4 – Setting Up RMA on IRES**".

> **Note**: This is not a comprehensive installation manual. Please refer to the RMA user's guide for more detailed information.

Installation Overview

Typically, these three components are installed on separate systems, as follows:

- The RMA general agent (GA) should be installed on all the POS systems in a particular store. These systems can have DHCP addresses (i.e. no need for static IP addresses).

- The RMA master agent (MA) should be installed on a single system within each store that will act as the RMA entry-point for the store. As of RMA V2R6, this system may have either a static IP address or a dynamic IP address provided the hostname can be resolved by DNS to the correct IP address for the MA. This system does not need to be a server-class system.

- The IBM Director Server should be installed on a system residing outside the store – typically, it will be installed at the corporate I/T headquarters or data-center. When you install the Director Server, the installation program automatically installs the Director Agent (to monitor the server on which it is installed), and the Director Console (the GUI for Director Server) along with Director Server. Typically, the Director Server should run on a dedicated server-class computer, although this is not necessary for the software to function properly.

The overall installation process is as follows:

1. Download the Director Server and required service update
2. Download RMA (which includes the Retail Extensions for IBM Director)

3. Install the IBM Director Server on a system (typically on a system outside the store), along with the Service Update for IBM Director on the same system
4. Install Retail Extensions for IBM Director on the same system
5. Configure IBM Director Console to display Groups and Tasks panes
6. Install the RMA MA on a system within a store
7. Install the RMA GA on a different POS system within the same store (or on all the POS systems in the store)
8. Configure IBM Director discovery preferences to discover the MA
9. Discover the MA by clicking the icon to discover all JMX systems

Network Requirements

If you are setting up a lab environment or a single-store scenario with no outside internet connectivity, you can install the RMA MA on the same system as the Director Server, although this is generally not desirable for a production environment.

Network infrastructure can sometimes be complex, but the basic rules are as follows:

- The RMA MA system must be able to communicate with the RMA GA systems's IP address, and vice-versa. (You can usually test this using the "ping" command – try pinging the IP address of the MA from the GA, and vice-versa.)
- The Director Server system must be able to communicate with the RMA MA system's IP address, and vice-versa. (Again, you can usually test using "ping" command.)

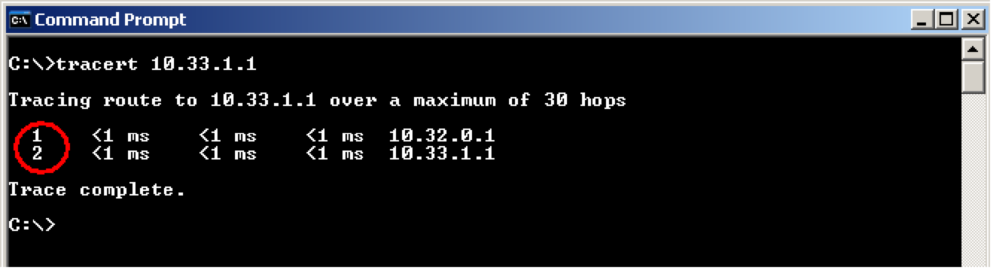
The network ports used by RMA are shown in the following table:

Network Port	Description
10149 (TCP)	Director Server to RMA MA (SOXS)
10150 (TCP)	Director Server to RMA MA (RMI)
10151 (TCP)	RMA MA to RMA GA (RMI)
10190 (TCP)	Used for RMA file transfers
31200 (UDP)	Discovery messages for MA and GA
See Director Redbook	Director Console to Server (and other Director-specific network ports)

Discovering General Agents that are on different subnets than the Master Agent

Typically, the MA and GA will be on the same subnet within the store. If they are not on the same subnet, and are connected by an in-store router, there is an additional configuration step to set the TCP/IP time-to-live parameter on the RMA agents.

First, use the "tracert" command to identify the number of hops between the Master Agent and General Agent systems. This command could be executed from either system and should use the IP address of the other system (similar to ping).



```
C:\>tracert 10.33.1.1

Tracing route to 10.33.1.1 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  10.32.0.1
  2    <1 ms    <1 ms    <1 ms  10.33.1.1

Trace complete.

C:\>
```

The number of hops returned by the tracert command is what you will need to set as the time to live for each of your general agents.

To set the time to live, add the following property to the simgmt.pro on each of your general agents:

com.ibm.retail.si.mgmt.generalagent.discovery.ttl=<hops returned by tracert>

The simgmt.pro is found in the following locations:

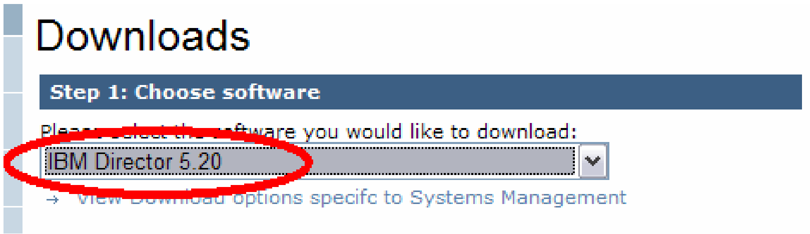
Windows: C:\Program Files\IBM\StoreIntegrator\user\rma\simgmt.pro
Linux: /opt/ibm/StoreIntegrator/user/rma/simgmt.pro
4690 Classic: m:\rma\user\rma\simgmt.pro
4690 Enhanced: f:\rma\user\rma\simgmt.pro

Note that the routers in between the systems must also pass the necessary RMA traffic between the systems in addition to just the time to live property.

Step 1 – Downloading IBM Director Server 5.20.3 and Service Update 4

1. Go to the following website: http://www-03.ibm.com/systems/management/director/about/director52/about52/downloads/index.html

2. Select IBM Director 5.20 from the drop-down list.



Downloads

Step 1: Choose software

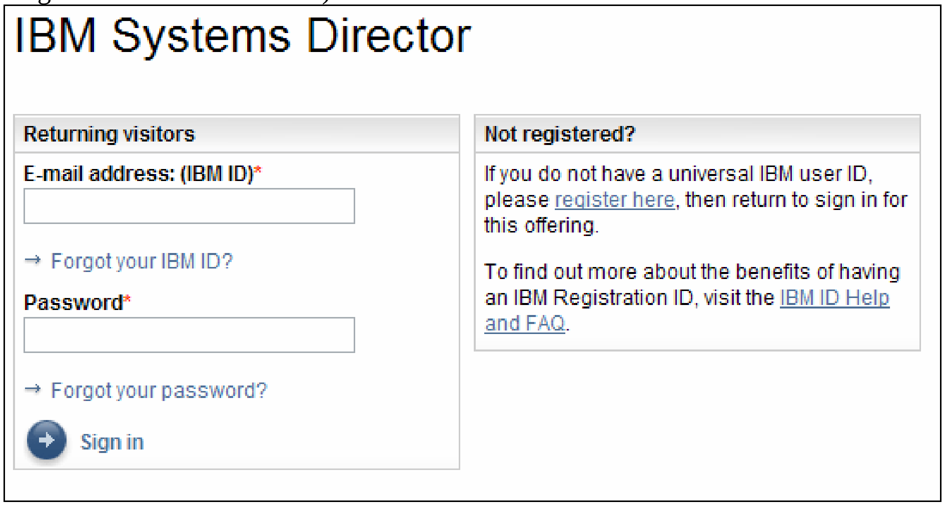
Please select the software you would like to download:

IBM Director 5.20

→ View Download options specifc to Systems Management

3. Enter your name, company, address, server serial number, and email address and the click submit button. (**Note:** If you don't have your serial number handy, you can enter in any number to proceed to the next steps.)

4. Sign in with your IBM ID. (If you do not have an IBM ID you can select "register here" to obtain one.)



IBM Systems Director

Returning visitors

E-mail address: (IBM ID)*

→ Forgot your IBM ID?

Password*

→ Forgot your password?

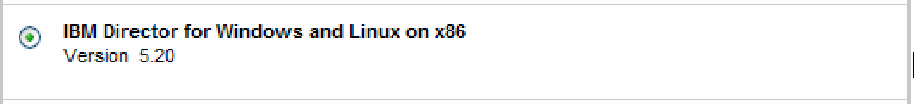
Sign in

Not registered?

If you do not have a universal IBM user ID, please register here, then return to sign in for this offering.

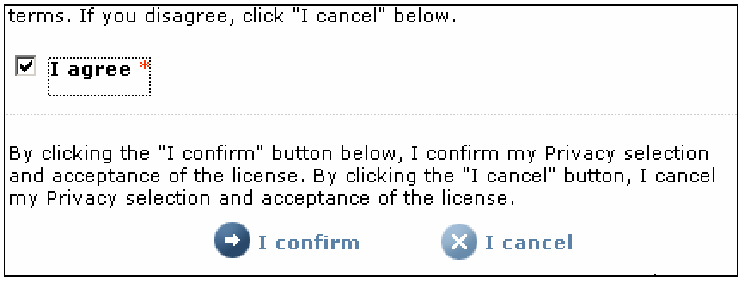
To find out more about the benefits of having an IBM Registration ID, visit the IBM ID Help and FAQ.

5. Select the operating system version to download and click continue.



● **IBM Director for Windows and Linux on x86**
Version 5.20

6. Verify your information, then select the "**I agree"** checkbox, and select the "**I confirm"** button.



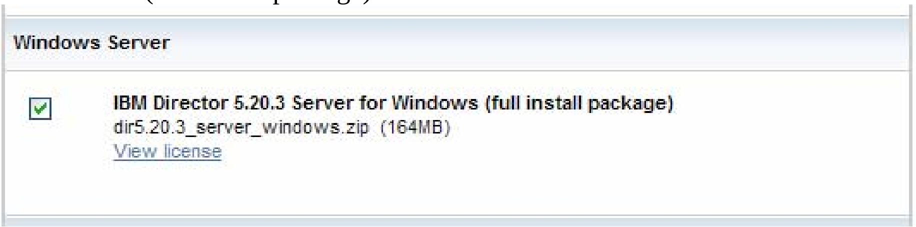
terms. If you disagree, click "I cancel" below.

☑ **I agree** *

By clicking the "I confirm" button below, I confirm my Privacy selection and acceptance of the license. By clicking the "I cancel" button, I cancel my Privacy selection and acceptance of the license.

I confirm   I cancel

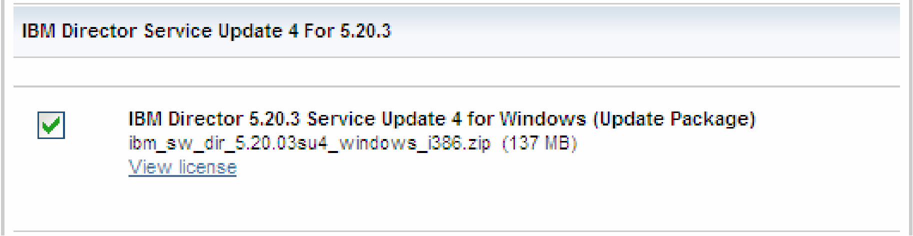
7. You will need to download 2 different files. First, select Director 5.20.3 Server for Windows (full install package):



Windows Server

☑ IBM Director 5.20.3 Server for Windows (full install package)
dir5.20.3_server_windows.zip (164MB)
View license

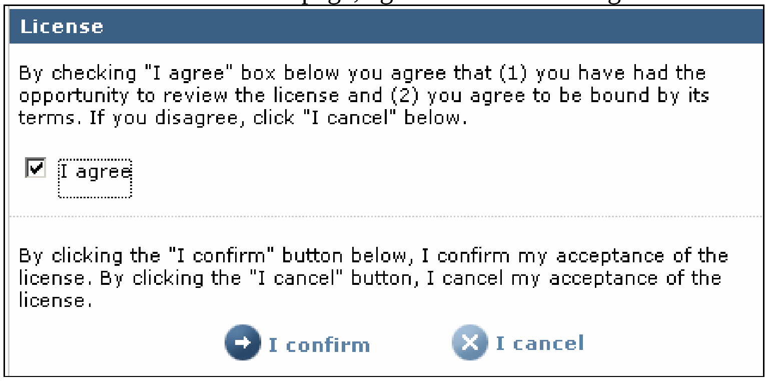
8. Next, scroll down further and select Director 5.20.3 Service Update 4 for Windows (update package).



IBM Director Service Update 4 For 5.20.3

☑ IBM Director 5.20.3 Service Update 4 for Windows (Update Package)
ibm_sw_dir_5.20.03su4_windows_i386.zip (137 MB)
View license

9. Scroll to the bottom of the page, agree to the License agreement and click confirm.



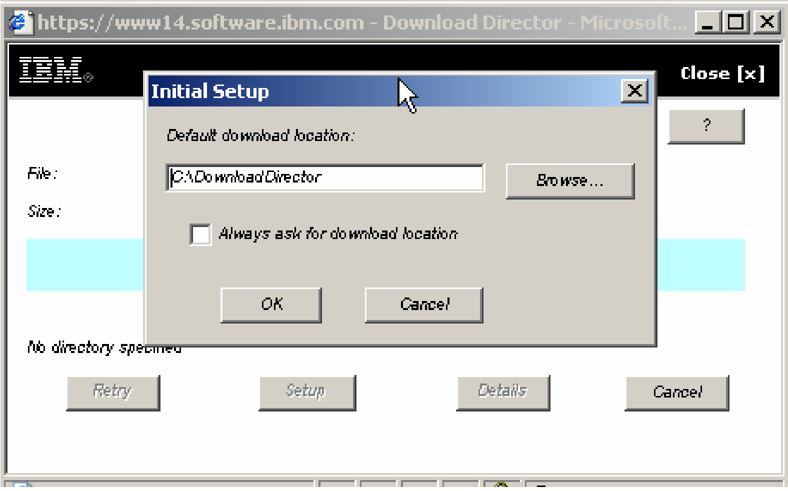
License

By checking "I agree" box below you agree that (1) you have had the opportunity to review the license and (2) you agree to be bound by its terms. If you disagree, click "I cancel" below.

☑ I agree

By clicking the "I confirm" button below, I confirm my acceptance of the license. By clicking the "I cancel" button, I cancel my acceptance of the license.

10. Select the destination to download the files and the download process begins.



Default download location: C:\DownloadDirector

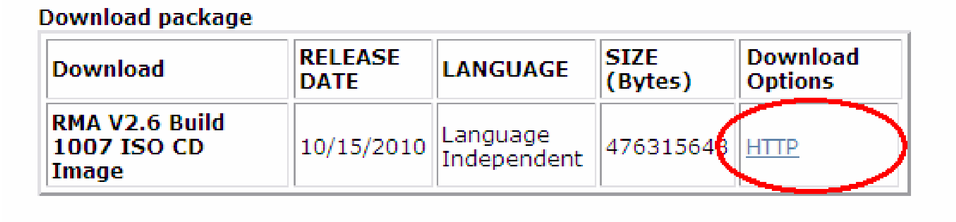
□ Always ask for download location

No directory specified

Step 2 – Downloading RMA 2.6 and the Retail Extensions for IBM Director

1. Go to the following website: http://www-1.ibm.com/support/docview.wss?rs=219&uid=pos1R4000158

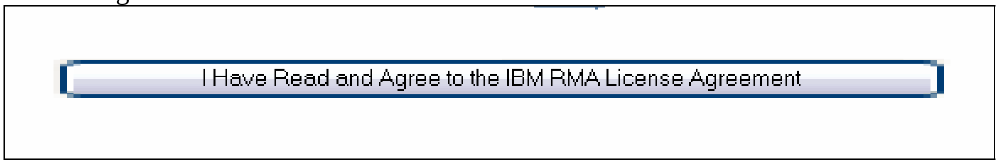
2. Scroll to the bottom of the page and select **HTTP** to begin downloading.



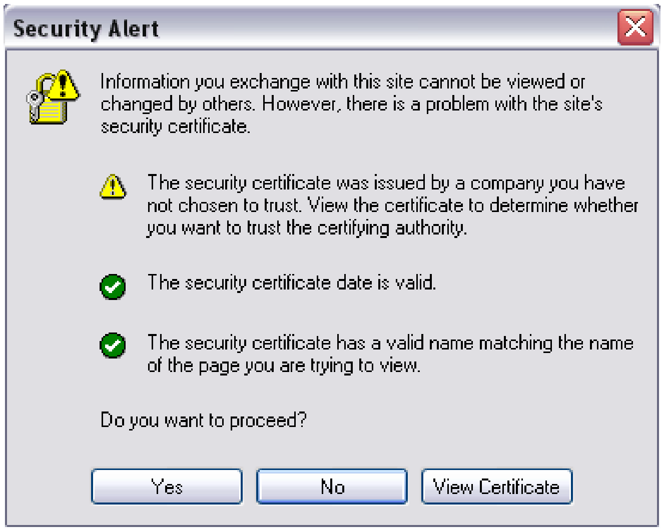
Download package

Download	RELEASE DATE	LANGUAGE	SIZE (Bytes)	Download Options
RMA V2.6 Build 1007 ISO CD Image	10/15/2010	Language Independent	476315648	HTTP

3. Enter in your name, company, email address, then select hardware platform and drivers. Select the button that says "I Have Read and Agree to the IBM RMA License Agreement".



4. Depending on your choice of web browser, you may be required to select "Yes" when prompted with a security alert.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

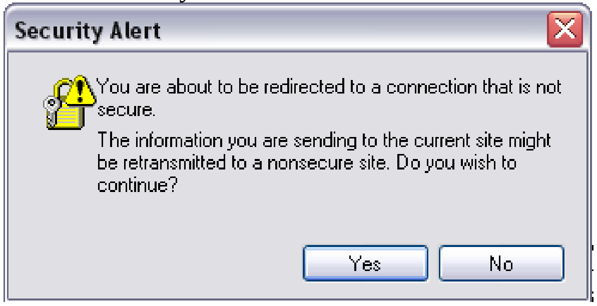
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

5. Depending on your choice of web browser, you may be required to click “Yes” on a second security alert.

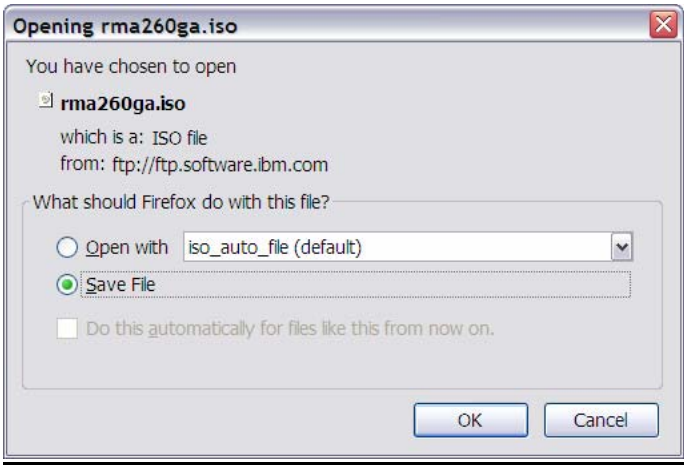


Security Alert

You are about to be redirected to a connection that is not secure.

The information you are sending to the current site might be retransmitted to a nonsecure site. Do you wish to continue?

6. Save the ISO image to the hard drive.



Opening rma260ga.iso

You have chosen to open

rma260ga.iso

which is a: ISO file

from: ftp://ftp.software.ibm.com

What should Firefox do with this file?

○ Open with iso_auto_file (default)

● Save File

□ Do this automatically for files like this from now on.

7. When the download completes, burn the ISO image to a CD using the CD-burning software of your choice.

Step 3 – Installing IBM Director Server and Service Update

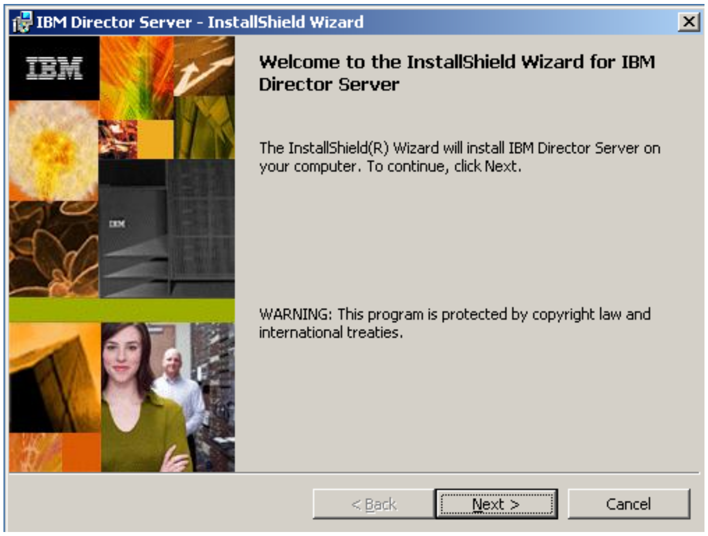
(Note: The service update should be installed on the same system as the Director Server.)

Note: This section of the manual describes a "basic" installation IBM Director Server. If you have unique installation requirements (for example, using a DB2 or Oracle database instead of the default Apache Derby database), then you should consult the IBM Director Server product documentation (especially the "Planning, Installation, and Configuration Guide"), which can be found here: http://www-03.ibm.com/systems/management/director/about/director52/about52/resources/

1. Unzip the IBM Director Server installation package ("dir5.20.3_server_windows.zip") to any location on your system.

2. To start the installation, launch the executable "dir5.20.3_server_windows.exe". **Note**: This will also automatically install the Director Console and the Director Agent.

3. On the next screen select **Next** to continue.



IBM Director Server - InstallShield Wizard

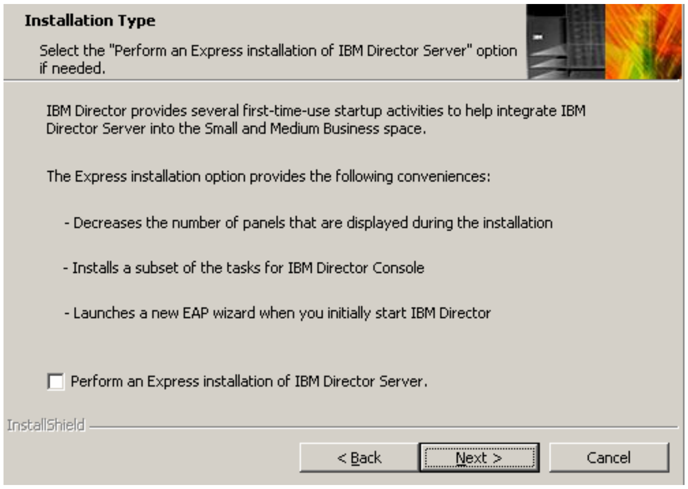
Welcome to the InstallShield Wizard for IBM Director Server

The InstallShield(R) Wizard will install IBM Director Server on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

4. Accept the License Agreement and select **Next.**

5. Do not check the option for Express installation and select **Next.**



Installation Type

Select the "Perform an Express installation of IBM Director Server" option if needed.

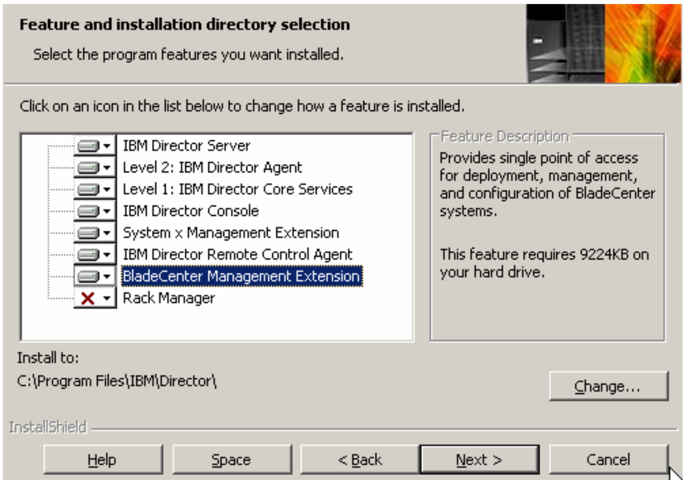
IBM Director provides several first-time-use startup activities to help integrate IBM Director Server into the Small and Medium Business space.

The Express installation option provides the following conveniences:

- Decreases the number of panels that are displayed during the installation
- Installs a subset of the tasks for IBM Director Console
- Launches a new EAP wizard when you initially start IBM Director

□ Perform an Express installation of IBM Director Server.

6. Select the features to install and select **Next.**



Feature and installation directory selection

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- IBM Director Server
- Level 2: IBM Director Agent
- Level 1: IBM Director Core Services
- IBM Director Console
- System x Management Extension
- IBM Director Remote Control Agent
- BladeCenter Management Extension
- ✗ Rack Manager

Feature Description

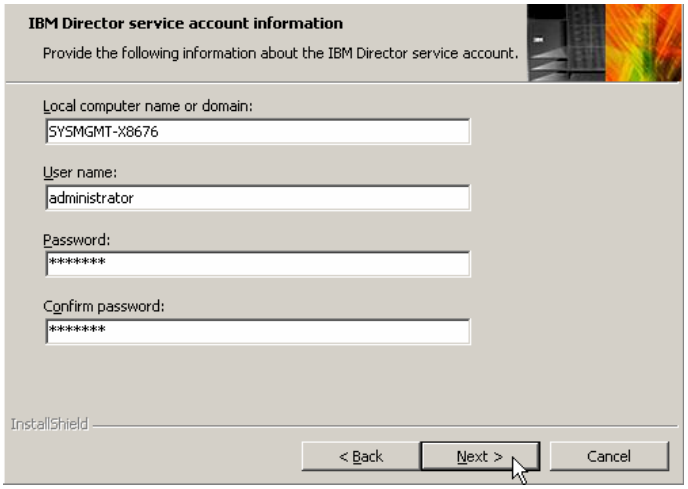
Provides single point of access for deployment, management, and configuration of BladeCenter systems.

This feature requires 9224KB on your hard drive.

Install to:
C:\Program Files\IBM\Director\

Note: Although some of these items (e.g. system x management extension, remote control agent, bladecenter management extension) are not strictly needed for RMA support, it’s a good idea to use the default settings since these have been thoroughly tested with RMA.

7. Enter an administrative user ID and PW and select **Next. Note:** It is very important that this be accurate when installing Director.



IBM Director service account information

Provide the following information about the IBM Director service account.

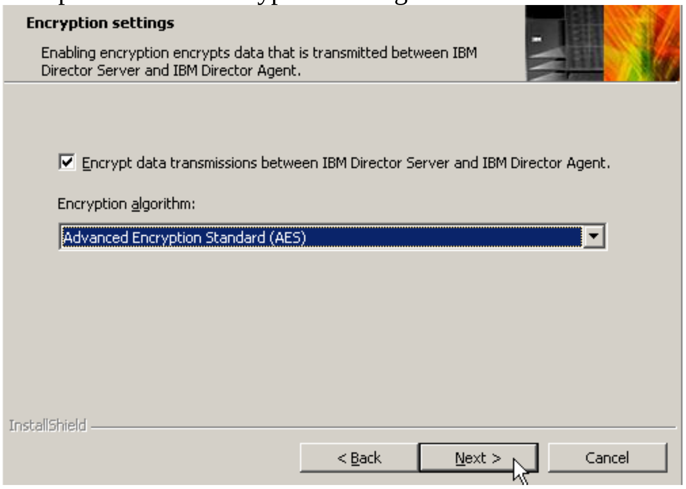
Local computer name or domain: SYSMGMT-X8676

User name: administrator

Password: *******

Confirm password: *******

8. Accept the default encryption settings and select **Next.**



Encryption settings

Enabling encryption encrypts data that is transmitted between IBM Director Server and IBM Director Agent.

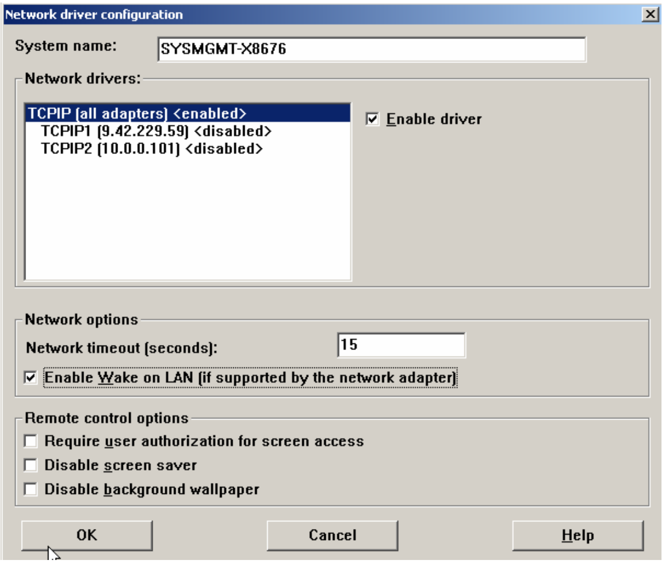
☑ Encrypt data transmissions between IBM Director Server and IBM Director Agent.

Encryption algorithm: Advanced Encryption Standard (AES)

9. Accept the default software distribution directories or edit for your environment and select **Next.**

10. Select **Install** to begin the installation.

11. Later (midway through installation), select the default adapter, TCPIP (all adapters), check Enable Wake on LAN and select **OK.**



Network driver configuration

System name: SYSMGMT-X8676

Network drivers:

TCPIP (all adapters) <enabled>
TCPIP1 (9.42.229.59) <disabled>
TCPIP2 (10.0.0.101) <disabled>

☑ Enable driver

Network options

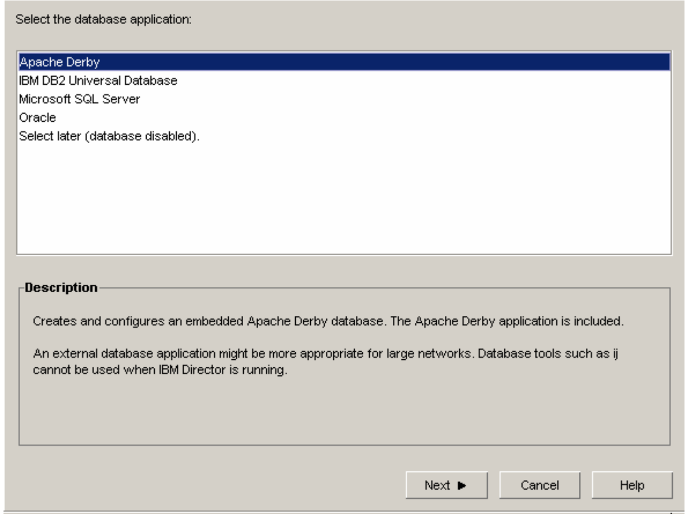
Network timeout (seconds): 15

☑ Enable Wake on LAN (if supported by the network adapter)

Remote control options

☐ Require user authorization for screen access
☐ Disable screen saver
☐ Disable background wallpaper

12. Select the database for the Director Server. Select **Apache Derby** for default database and select **Next.** **Note:** If you plan to manage 500 systems or more, it is recommended to use one of the other database options, such as DB2 or SQL Server. For test environments, you can use Apache Derby to simplify the installation.



Select the database application:

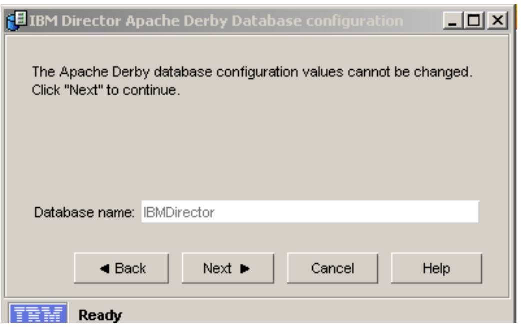
Apache Derby
IBM DB2 Universal Database
Microsoft SQL Server
Oracle
Select later (database disabled).

Description

Creates and configures an embedded Apache Derby database. The Apache Derby application is included.

An external database application might be more appropriate for large networks. Database tools such as ij cannot be used when IBM Director is running.

13. Accept the default database name and select **Next.**

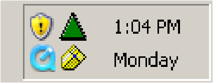

IBM Director Apache Derby Database configuration

The Apache Derby database configuration values cannot be changed. Click "Next" to continue.

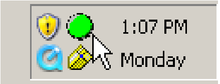
Database name: IBMDirector

14. Select **Finish** and Restart the computer.

15. After the computer reboots there will be green triangle by the clock indicating IBM Director Server is starting.

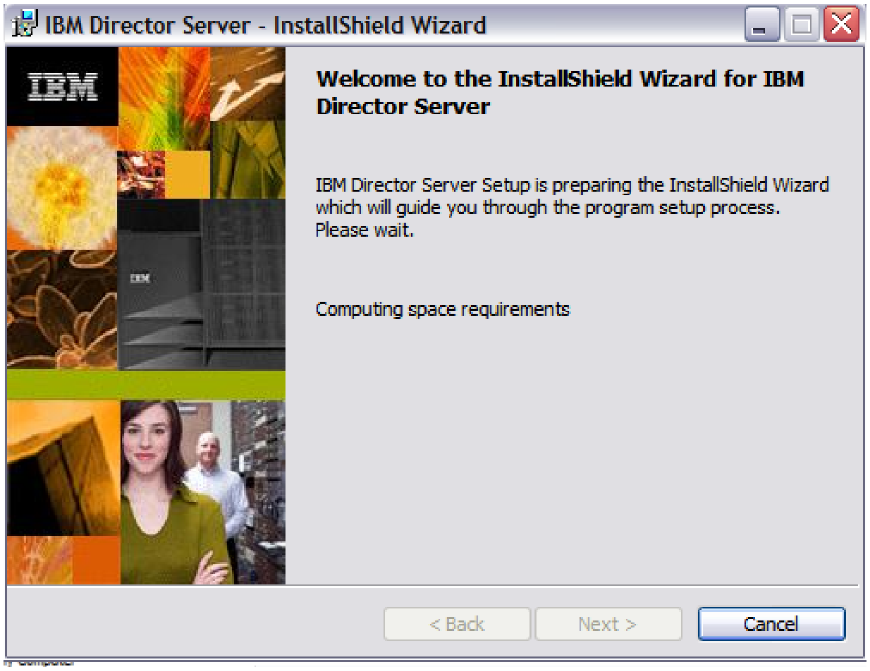


16. Once Director Server has started there will be a green circle by the clock.



17. Change to the location where you stored the Director Service Update image and extract the image from the zip file.   Then select the installation file and execute it.

18. The following screen will appear after a few minutes:



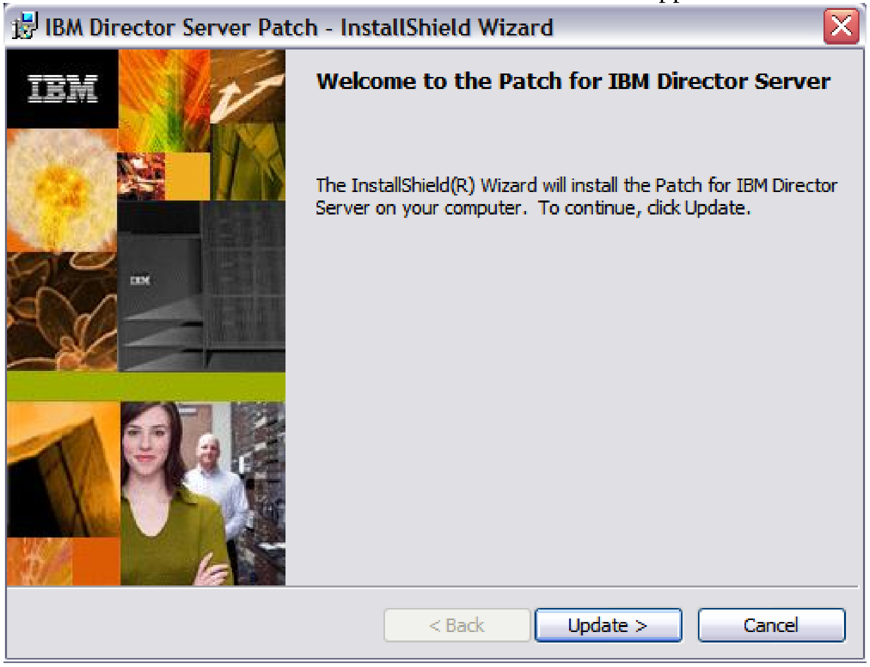
IBM Director Server - InstallShield Wizard

Welcome to the InstallShield Wizard for IBM Director Server

IBM Director Server Setup is preparing the InstallShield Wizard which will guide you through the program setup process. Please wait.

Computing space requirements

19. After a few more minutes the Welcome screen below will appear.

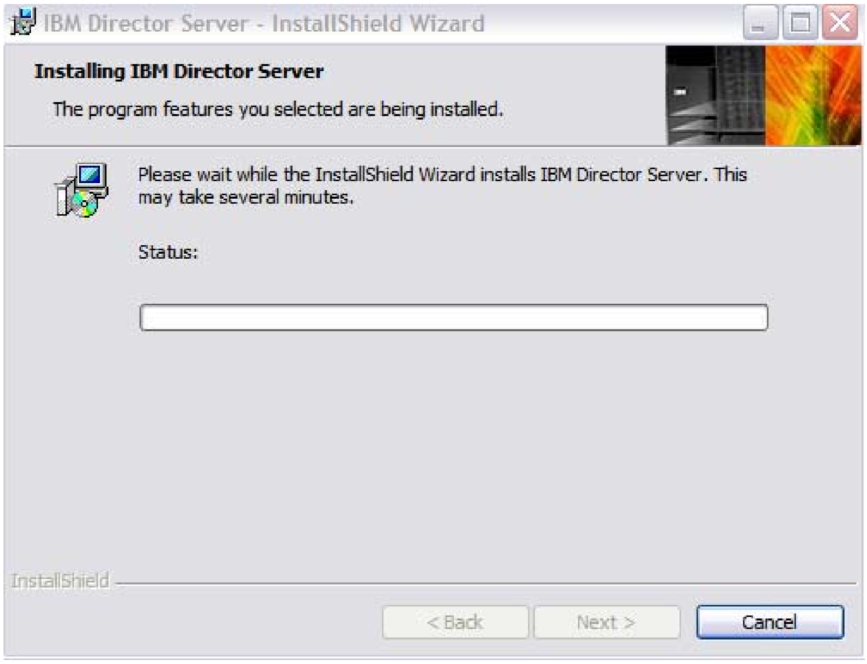


IBM Director Server Patch - InstallShield Wizard

Welcome to the Patch for IBM Director Server

The InstallShield(R) Wizard will install the Patch for IBM Director Server on your computer. To continue, click Update.

20. Click on the Update button to start the installation of the patch for Director Server. The below screen will be displayed during the update.



IBM Director Server - InstallShield Wizard

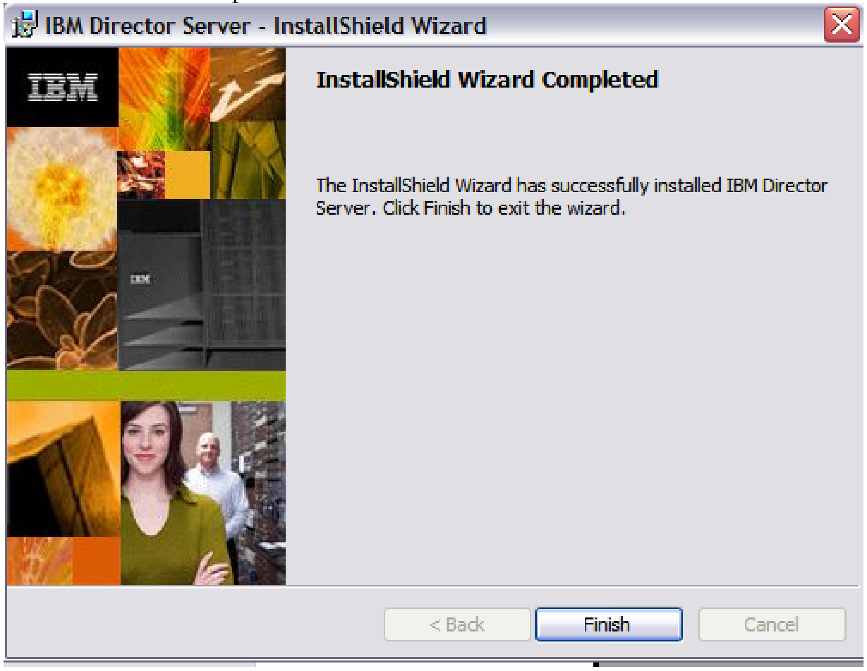
Installing IBM Director Server

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs IBM Director Server. This may take several minutes.

Status:

21. When the installation is complete, the window below will appear. Click on the Finish button to complete the install.



IBM Director Server - InstallShield Wizard

InstallShield Wizard Completed

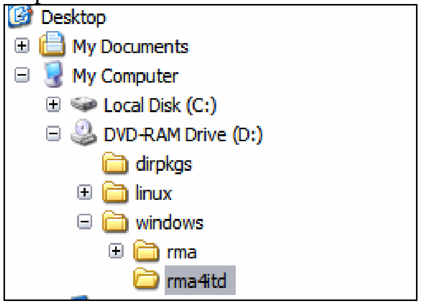
The InstallShield Wizard has successfully installed IBM Director Server. Click Finish to exit the wizard.

Step 4 – Installing RMA Retail Extensions for IBM Director Server

(Note: This should be installed on the same system as the Director Server.)

1. Insert the RMA CD. (**Note**: This CD should have been created from the ISO image that was downloaded in the previous steps.)

2. Expand the Windows > rma4itd directory



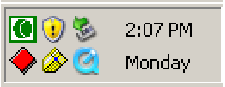
3. Run setup.exe.

4. Select **Next** on the installation screen.

5. Accept the License agreement and select **Next.**

6. Select **Next** to begin the installation.

7. The IBM Director Server is stopped. You should verify that the server stopped successfully by ensuring there is a “red diamond” in the task bar, and that the twgsrvw.exe process is no longer running:

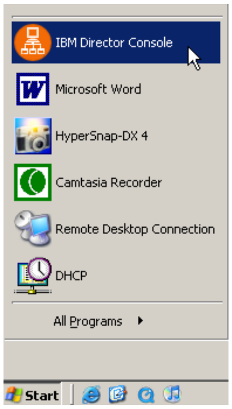


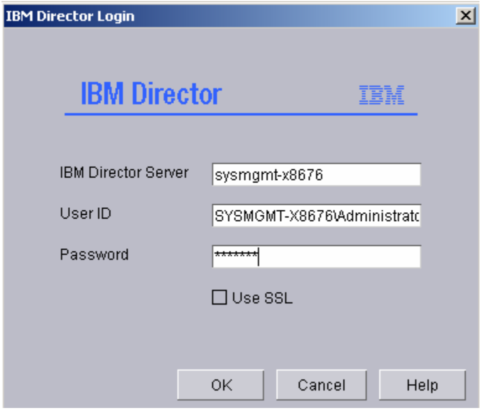
8. Installation continues.

9. Select Finish when installation is done.

Step 5 – Configure IBM Director Console to display Groups and Tasks Panes

1. Log onto the IBM Director Console





IBM Director Server: sysmgmt-x8676

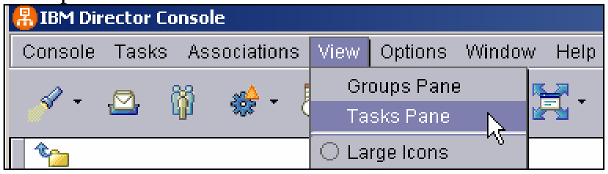
User ID: SYSMGMT-X8676\Administratc

Password: *******

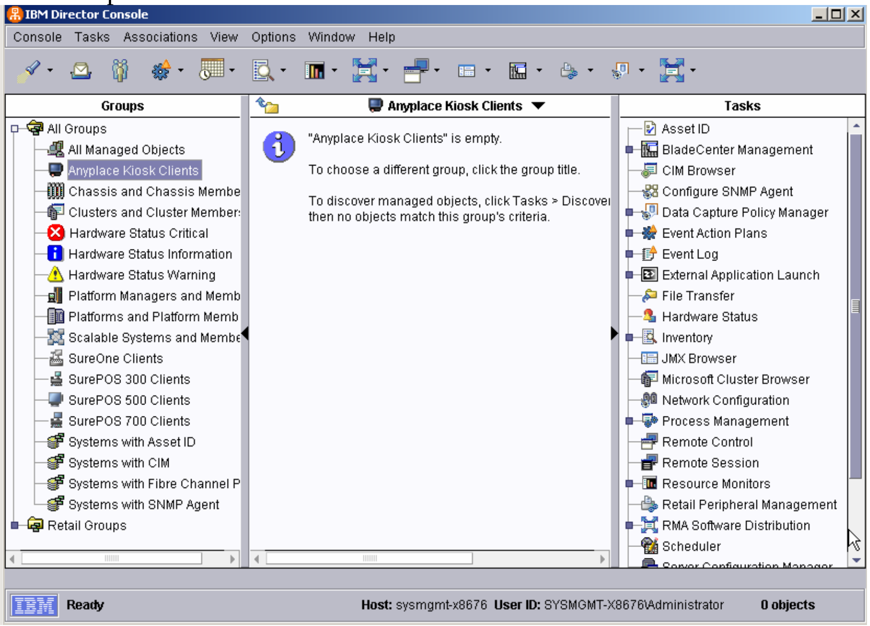
□ Use SSL

2. Close the IBM Director help window. (If desired, you can check the check-box on this help window to disable it in the future.)

3. To display the Groups and Tasks Panes, on the Director Console select View > Groups Pane and Tasks Pane.



4. The Groups and Tasks Panes are now visible in the console



"Anyplace Kiosk Clients" is empty.

To choose a different group, click the group title.

To discover managed objects, click Tasks > Discover then no objects match this group's criteria.

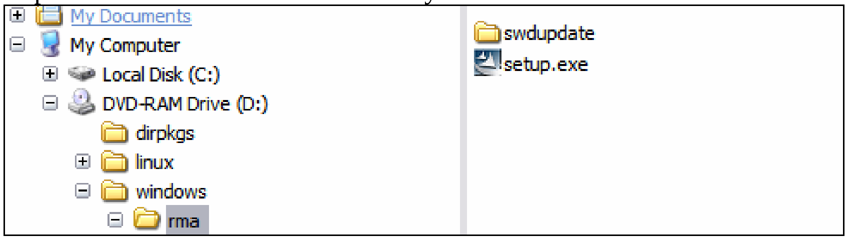
Ready Host: sysmgmt-x8676 User ID: SYSMGMT-X8676\Administrator 0 objects

Step 6 – Installing (RMA) Remote Management Agent (MA) Master Agent

(Note: This is usually installed on a single system within the store – i.e. not at the enterprise.)

1. Insert the RMA CD.

2. Expand the Windows > RMA directory



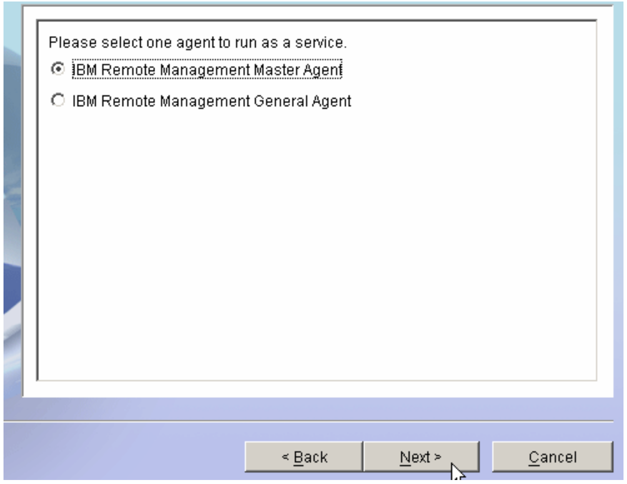
3. Run setup.exe file.

4. Select **Next** on the installation screen.

5. Accept the License agreement and select **Next.**

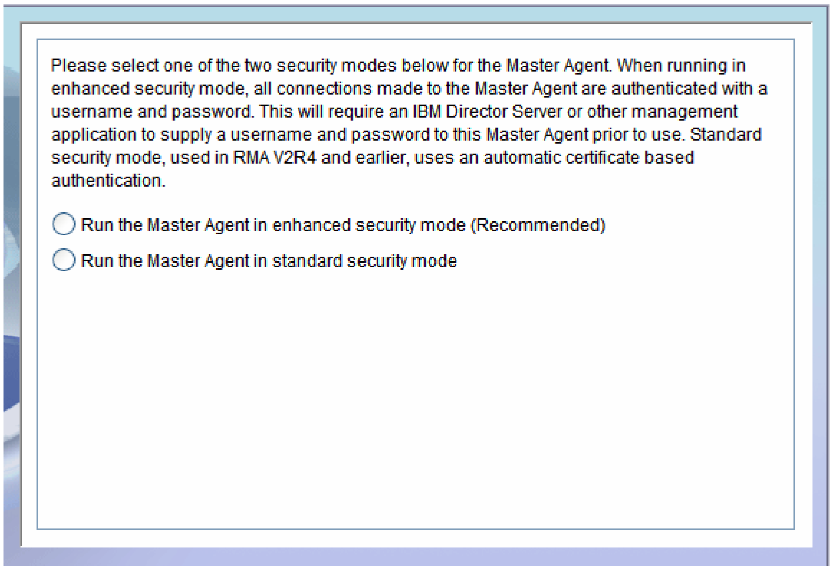
6. Enter the desired installation directory and select **Next.**

7. Select the RMA Master Agent to install and select **Next.**


Please select one agent to run as a service.
● IBM Remote Management Master Agent
○ IBM Remote Management General Agent

8. Select the security mode to enable for the Master Agent. If the Master Agent is running in enhanced security mode then the IBM Director Server will need to supply credentials before it will gain remote access to the system. Enhanced

security mode is the recommended setting. These security settings can be modified after installation by modifying the c:\Program Files\IBM\StoreIntegrator\user\rma\security\security.properties file.

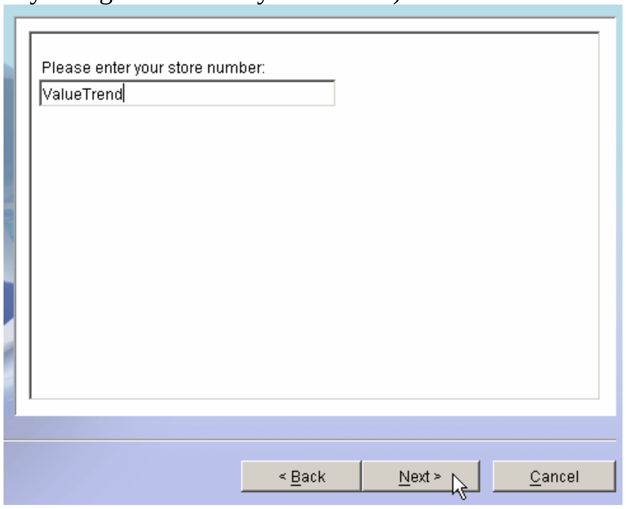


Please select one of the two security modes below for the Master Agent. When running in enhanced security mode, all connections made to the Master Agent are authenticated with a username and password. This will require an IBM Director Server or other management application to supply a username and password to this Master Agent prior to use. Standard security mode, used in RMA V2R4 and earlier, uses an automatic certificate based authentication.

○ Run the Master Agent in enhanced security mode (Recommended)

○ Run the Master Agent in standard security mode

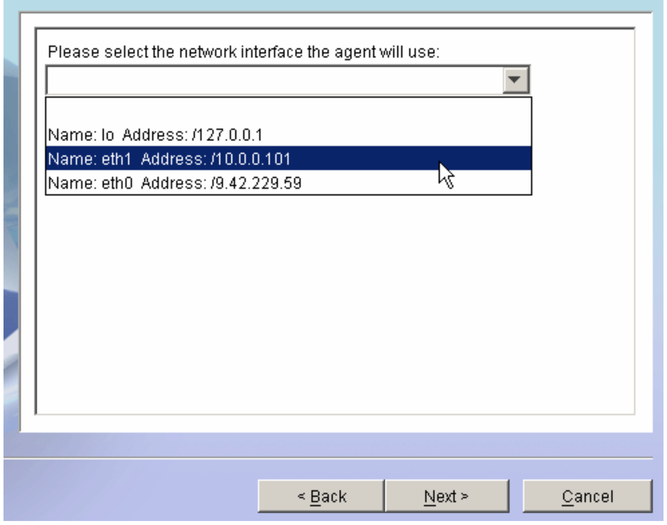
9. Enter a Store Number and select **Next.** (**Note**: The store number can be number or any string identifier of your choice.)



Please enter your store number:

ValueTrend

10. Select the interface for RMA to communicate on and select **Next.**


Please select the network interface the agent will use:

Name: lo Address: /127.0.0.1
Name: eth1 Address: /10.0.0.101
Name: eth0 Address: /9.42.229.59

11. Select **Next** to begin the installation.

12. Select **Next** to end the installation.

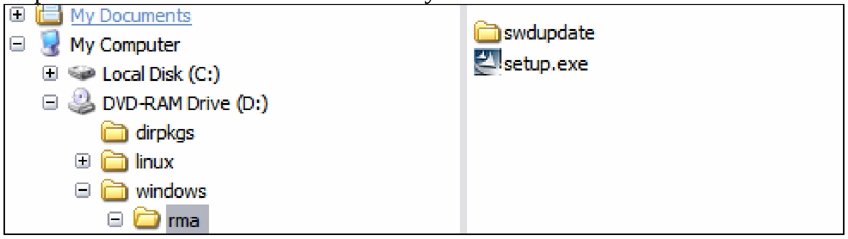
13. Restart the computer.

Step 7 – Installing (RMA) Remote Management Agent GA (General Agent)

(Note: The general agent must be installed within the store on a different system from the master agent. You can install multiple general agents within a single store – all connecting to a single master agent.)

1. Insert the RMA CD.

2. Expand the Windows > RMA directory.

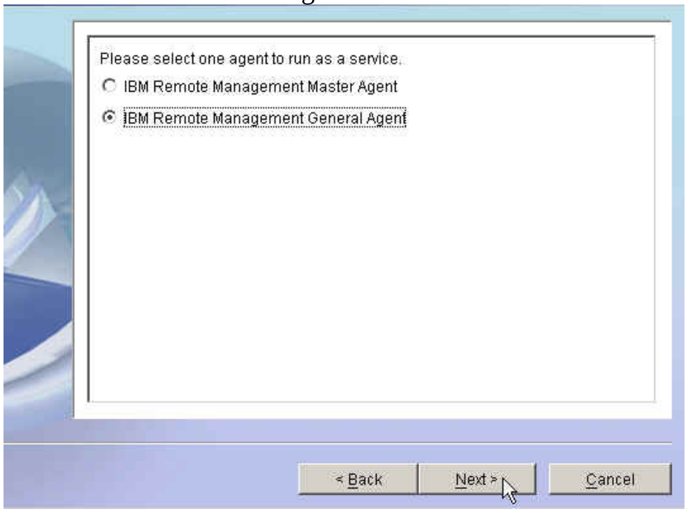


3. Run setup.exe file.

4. Select **Next** on the installation screen.

5. Accept the License agreement and select **Next.**

6. Select the RMA General Agent to install and select **Next.**

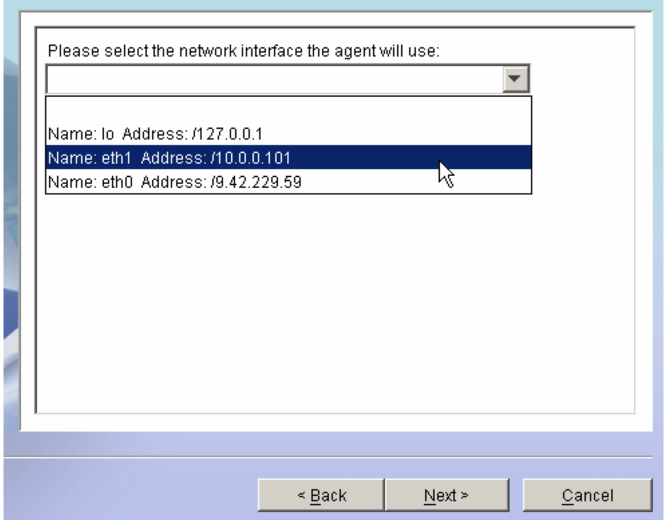


Please select one agent to run as a service.

○ IBM Remote Management Master Agent

● IBM Remote Management General Agent

7. Select the interface for RMA to communicate on and select **Next.**



Please select the network interface the agent will use:

Name: lo Address: /127.0.0.1

Name: eth1 Address: /10.0.0.101

Name: eth0 Address: /9.42.229.59

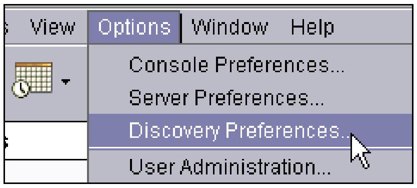
8. Select **Next** to begin the installation.

9. Select **Next** to end the installation.

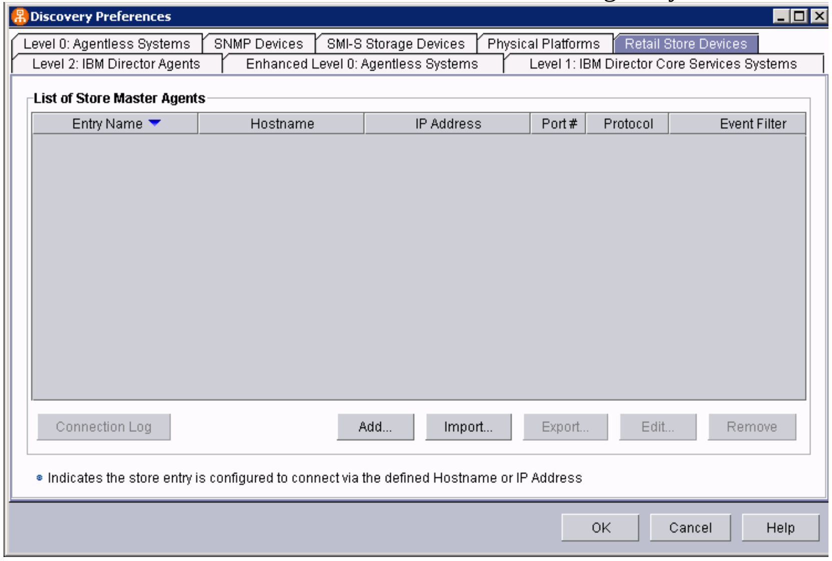
10. Restart the computer.

Step 8 – Configure IBM Director Discovery Preferences to Discover RMA MA

1. From the IBM Director Console select Options > Discovery Preferences.

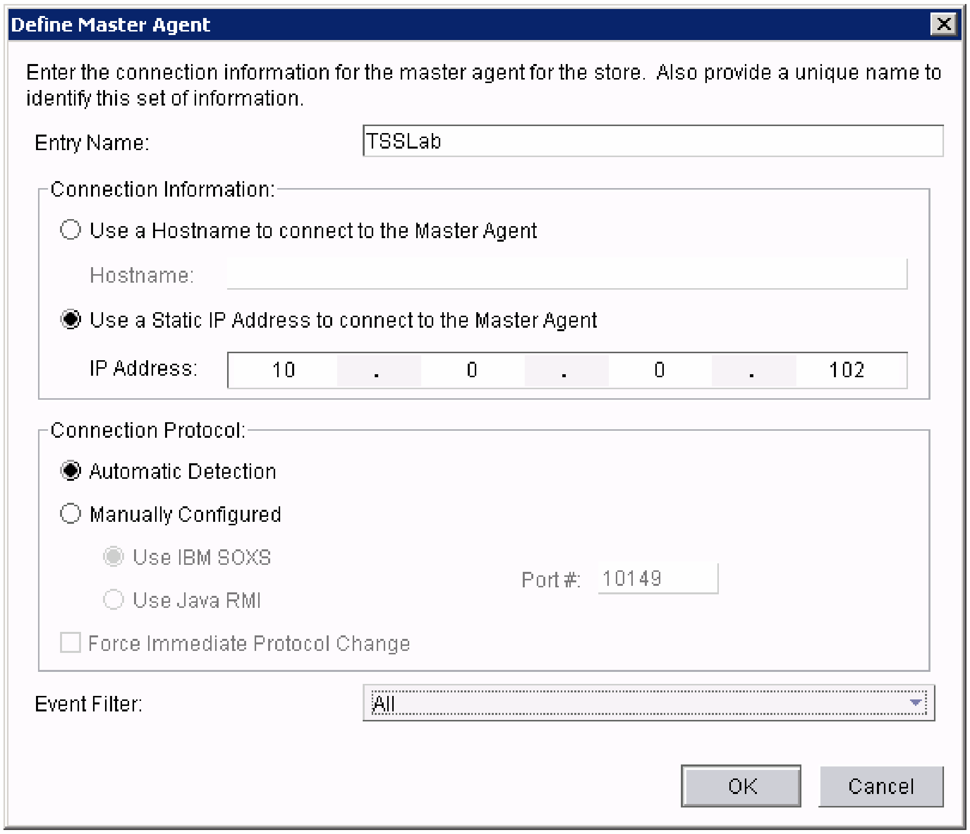


2. Select the Retail **Store Devices** tab to define Master Agent systems.



• Indicates the store entry is configured to connect via the defined Hostname or IP Address

3. Select **Add** to define a Master Agent system and select OK. Enter any string value for the store name (or it can be a store number), then enter the hostname or IP address for the system. Note that you must specify the hostname if your Master Agent uses DHCP. You may want to change the event filter to “All” to make sure Director receives all the events from RMA.



Define Master Agent

Enter the connection information for the master agent for the store. Also provide a unique name to identify this set of information.

Entry Name: TSSLab

Connection Information:

○ Use a Hostname to connect to the Master Agent

Hostname:

● Use a Static IP Address to connect to the Master Agent

IP Address: 10 . 0 . 0 . 102

Connection Protocol:

● Automatic Detection

○ Manually Configured

● Use IBM SOXS

○ Use Java RMI

Port #: 10149

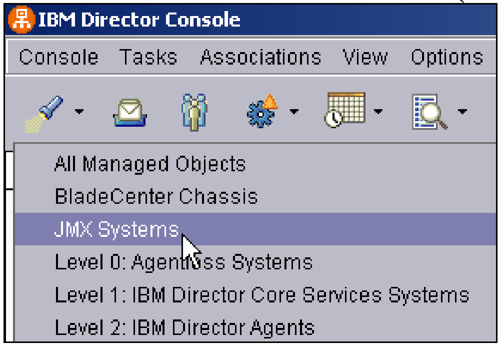
□ Force Immediate Protocol Change

Event Filter: All

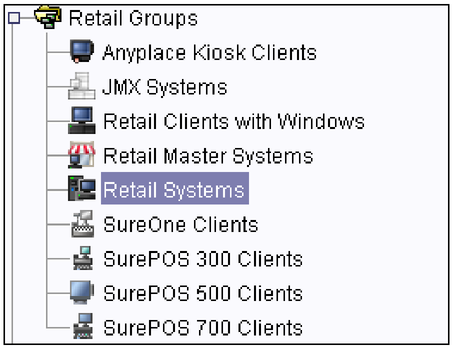
4. Select OK to close the Discovery Preferences.

Step 9 – Discover JMX Systems (RMA Agents)

1. On the Director Console select Discover (flashlight) > JMX Systems.



2. On the Director Console in the Groups pane the Retail Groups are created.

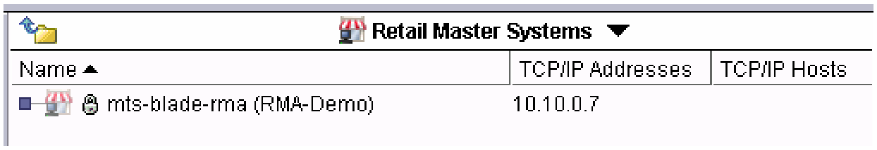


3. Select the “Retail Master Systems” group to view the master agent systems. Select the “Retail Systems” group to view all the Retail Systems.

4. If the master agent was installed with the “enhanced security” option, you will need to use the “Store Authorization Manager” to supply the username/password for the MA. See the section below for additional details.

Step 10 – Authenticating to Agents Running Enhanced Security

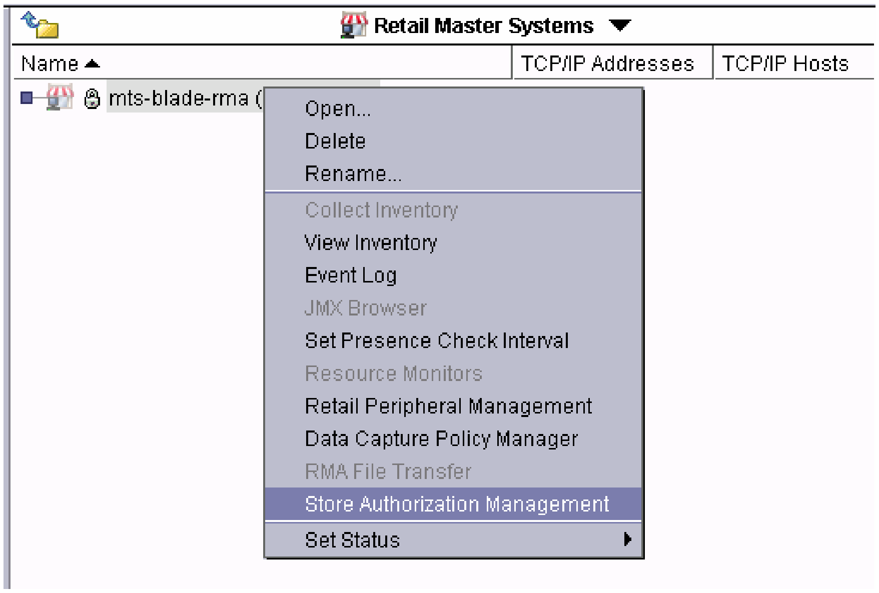
If a Master Agent is running with Enhanced Security enabled then it will show as offline and will display a lock icon when it is initially discovered.


Retail Master Systems

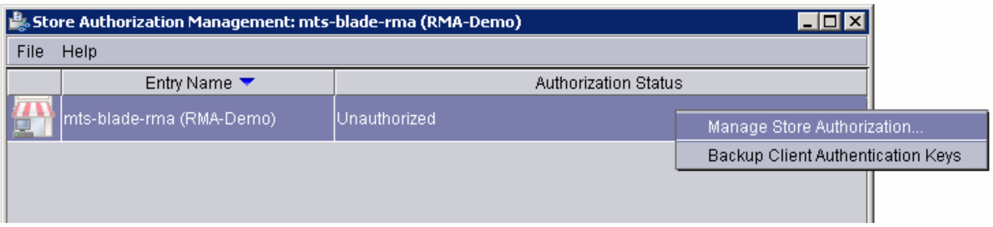
Name	TCP/IP Addresses	TCP/IP Hosts
mts-blade-rma (RMA-Demo)	10.10.0.7	

This indicates that the Master Agent is currently inaccessible and must be authenticated before it can be used. The following steps describe how to authenticate with a Master Agent.

1. Launch the Store Authorization Management task on one or many locked Master Agents by dragging and dropping from the Tasks column or by right-clicking and selecting “Store Authorization Management”.



2. Inside the Store Authorization Management task, select as many Master Agent systems as you wish, right-click, and select "Manage Store Authorization…"


Store Authorization Management: mts-blade-rma (RMA-Demo)
File
Help
Entry Name
Authorization Status
Manage Store Authorization...
Backup Client Authentication Keys

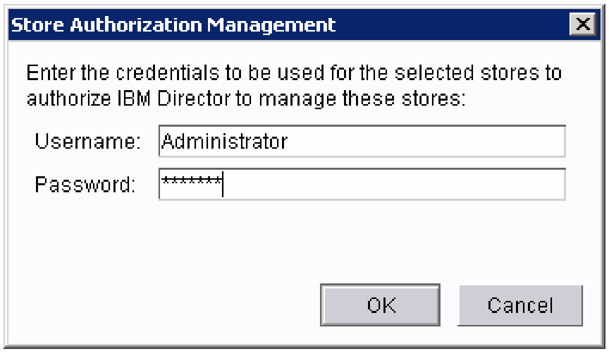
Entry Name	Authorization Status
mts-blade-rma (RMA-Demo)	Unauthorized

3. This will launch a dialog to enter a Username and Password from the Master Agent System in order to authenticate with the box. Enter a valid Username and Password and Click OK

On Windows, the user entered must be a member of the RMAAdmin group on the agent system. By default, the RMAAdmin group is populated with the Administrators group.

On Linux, the user entered must be a member of the rmaadmin group on the agent system. By default, the RMAAdmin group is populated with the root user.

On 4690, the user entered must have User Defined Attribute #8 enabled for the user id set within the Enhanced Security menus.



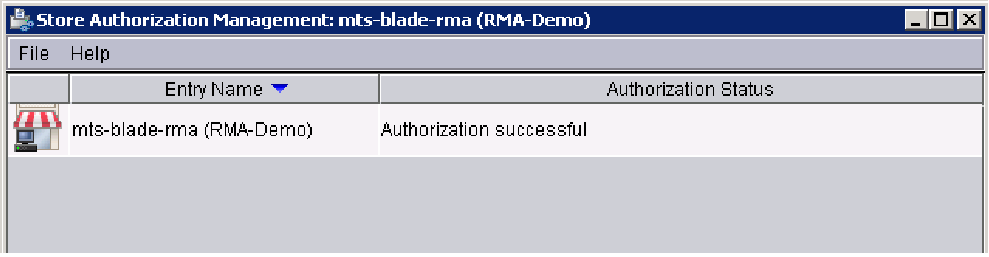
Store Authorization Management

Enter the credentials to be used for the selected stores to authorize IBM Director to manage these stores:

Username: Administrator

Password: *******

4. If the Username and Password are authenticated successfully then the Authorization Status of the agent will change to “Authorization successful”. At this point the Master Agent icon on the IBM Director console will get unlocked and the rest of the agents within the store will be discovered.



Store Authorization Management: mts-blade-rma (RMA-Demo)

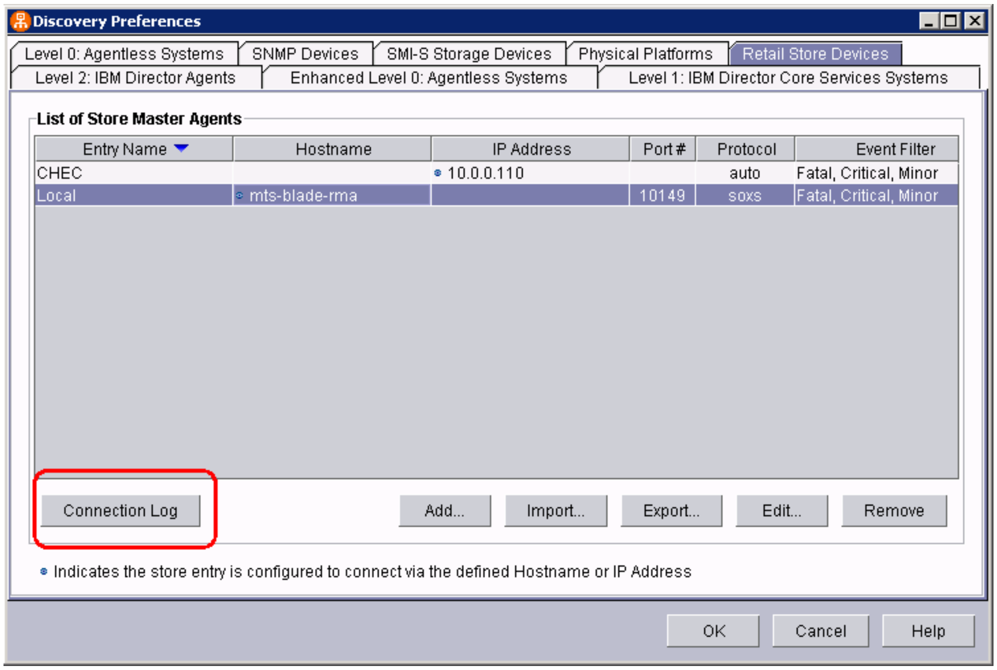
Entry Name	Authorization Status
mts-blade-rma (RMA-Demo)	Authorization successful

Diagnosing Connection Issues

If your newly added stores are not appearing in the IBM Director console after running Discovery then there is a good chance that the IBM Director Server at the enterprise can not connect to the Master Agent running on a system within a store.

To help diagnose these problems, a Connection Log is maintained for each store connection.

To view the connection log for a store entry, click on the “Connection Log” button after selecting a store entry within the Discovery Preferences Window:

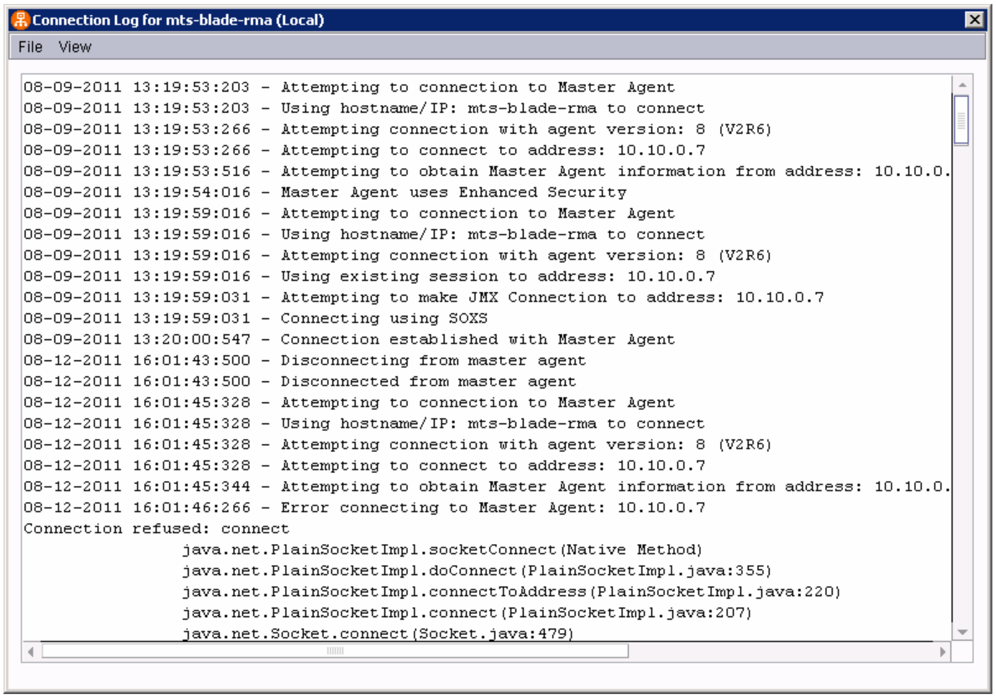

Discovery Preferences
Level 0: Agentless Systems
SNMP Devices
SMI-S Storage Devices
Physical Platforms
Retail Store Devices
Level 2: IBM Director Agents
Enhanced Level 0: Agentless Systems
Level 1: IBM Director Core Services Systems
List of Store Master Agents
Connection Log
Add...
Import...
Export...
Edit...
Remove
OK
Cancel
Help

Entry Name	Hostname	IP Address	Port #	Protocol	Event Filter
CHEC		● 10.0.0.110		auto	Fatal, Critical, Minor
Local	● mts-blade-rma		10149	soxs	Fatal, Critical, Minor

● Indicates the store entry is configured to connect via the defined Hostname or IP Address

The “Connection Log” will display connection specific history information for that store entry. Messages here can indicate problems such as issues resolving the hostname, firewall issues, configuration problems, or the like.

Please submit the Connection Log information when opening a PMR about a connection issue.



```
08-09-2011 13:19:53:203 - Attempting to connection to Master Agent
08-09-2011 13:19:53:203 - Using hostname/IP: mts-blade-rma to connect
08-09-2011 13:19:53:266 - Attempting connection with agent version: 8 (V2R6)
08-09-2011 13:19:53:266 - Attempting to connect to address: 10.10.0.7
08-09-2011 13:19:53:516 - Attempting to obtain Master Agent information from address: 10.10.0.
08-09-2011 13:19:54:016 - Master Agent uses Enhanced Security
08-09-2011 13:19:59:016 - Attempting to connection to Master Agent
08-09-2011 13:19:59:016 - Using hostname/IP: mts-blade-rma to connect
08-09-2011 13:19:59:016 - Attempting connection with agent version: 8 (V2R6)
08-09-2011 13:19:59:016 - Using existing session to address: 10.10.0.7
08-09-2011 13:19:59:031 - Attempting to make JMX Connection to address: 10.10.0.7
08-09-2011 13:19:59:031 - Connecting using SOXS
08-09-2011 13:20:00:547 - Connection established with Master Agent
08-12-2011 16:01:43:500 - Disconnecting from master agent
08-12-2011 16:01:43:500 - Disconnected from master agent
08-12-2011 16:01:45:328 - Attempting to connection to Master Agent
08-12-2011 16:01:45:328 - Using hostname/IP: mts-blade-rma to connect
08-12-2011 16:01:45:328 - Attempting connection with agent version: 8 (V2R6)
08-12-2011 16:01:45:328 - Attempting to connect to address: 10.10.0.7
08-12-2011 16:01:45:344 - Attempting to obtain Master Agent information from address: 10.10.0.
08-12-2011 16:01:46:266 - Error connecting to Master Agent: 10.10.0.7
Connection refused: connect
                java.net.PlainSocketImpl.socketConnect(Native Method)
                java.net.PlainSocketImpl.doConnect(PlainSocketImpl.java:355)
                java.net.PlainSocketImpl.connectToAddress(PlainSocketImpl.java:220)
                java.net.PlainSocketImpl.connect(PlainSocketImpl.java:207)
                java.net.Socket.connect(Socket.java:479)
```

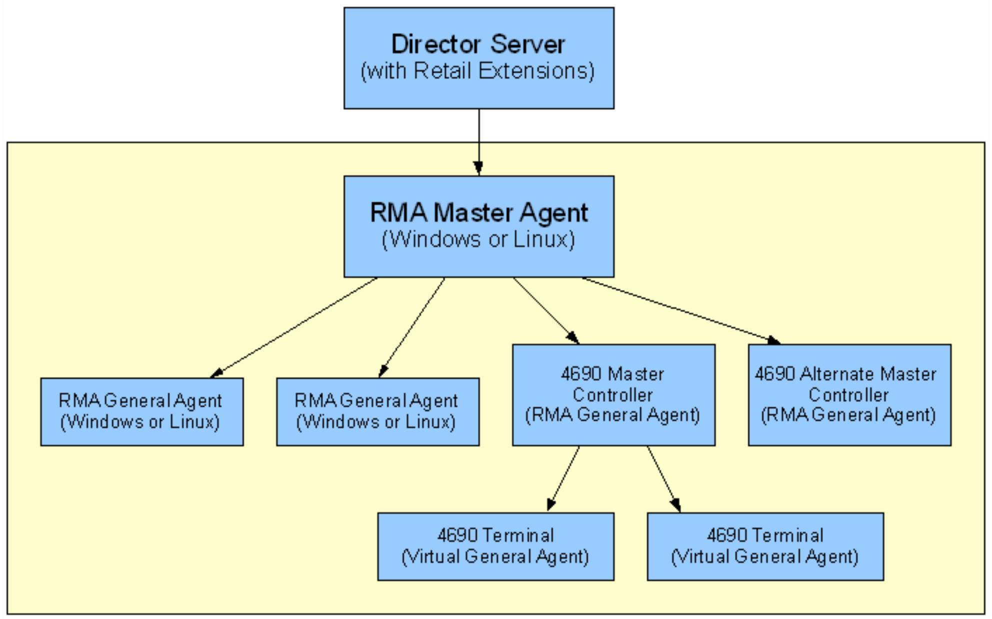
Chapter 2 – Setting Up RMA on 4690

This chapter discusses how to setup RMA on the 4690 operating system, which is possible using 4690 V5R2 and higher.

> **Note**: This chapter only explains the 4690-specific aspects of setting up a RMA solution. So, we assume here that you already know how to setup IBM Director, the RMA master agent (if needed), and how to discover devices and generally use the Director user interface. (If not, please refer to the other chapters of this cookbook, particularly "**Chapter 1 – Quick-Install Guide**".)

Overview of RMA on 4690

The following diagram illustrates a typical sample RMA deployment in a store with 4690 V5R2 or V6 classic:



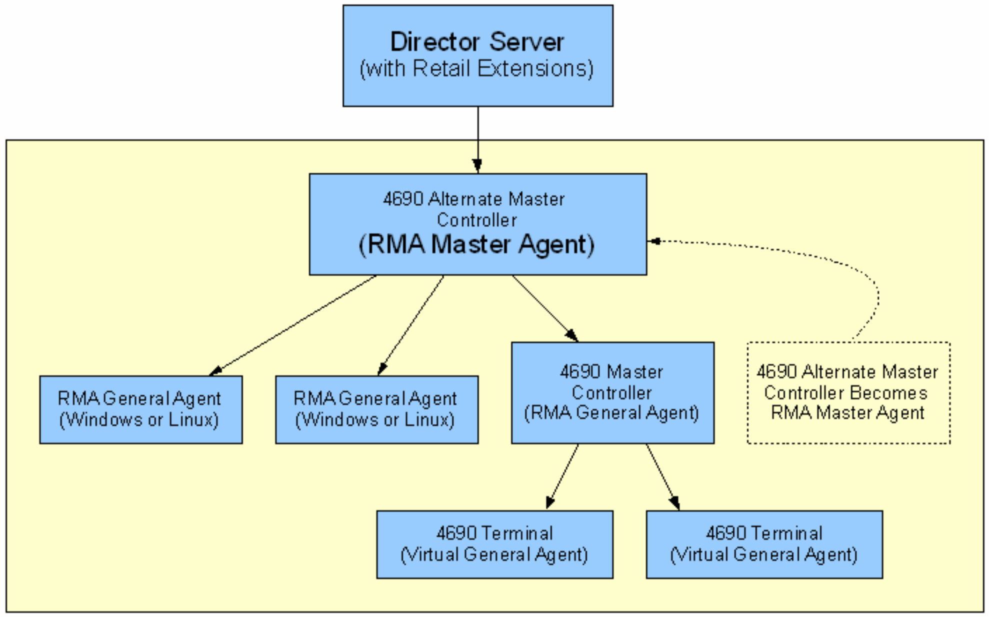
Example – This configuration is possible with 4690 V5R2, V6 classic mode, or V6 enhanced mode

As shown in the diagram above, the RMA deployment consists of the following components:

1. Director Server (with retail extensions), installed on a Windows or Linux system at the enterprise. The Director Server must have TCP/IP connectivity to the master agent.
2. RMA Master Agent, installed on a Windows or Linux system in the store.

3. 4690 Master Controller (i.e. responsible for the terminals), running the RMA General Agent
4. Optionally, the 4690 Alternate Master Controller, running the RMA General Agent (i.e. only applicable if using a multiple controller environment). Any additional controllers (not shown) would also be running the RMA General Agent.
5. 4690 Terminals, which are represented within RMA on the controller as "virtual general agents".
6. Optionally, you can have additional systems (Windows or Linux) within the store that are running the RMA General Agent. (For example, self checkout systems, kiosks, etc.)

With V6 "enhanced" mode, it's also possible to run the RMA Master Agent on one of the controllers instead of on a separate system. This eliminates the need for an additional system in the store to run the master agent. The following diagram illustrates this configuration:



Example – Master Agent on 4690 Controller, only possible with V6 enhanced mode

As shown in the diagram above, the 4690 Alternate Master runs the RMA Master Agent, instead of having a separate system for the master agent. (Note: This might also be any other 4690 controller – the choice is up to you during the setup process. See the setup instructions later in this chapter for details on making this choice.)

POS terminals are considered "virtual general agents", which means they appear as general agents within IBM Director. However, the code actually runs "virtually" within RMA on the controller responsible for those terminals (i.e. on the **Acting Master** if a multiple-controller system). If the **Master** controller goes down (in a multiple controller configuration), then the terminal's virtual agents will be recreated on the **Alternate**

Master controller when you activate it as **Master**. When this happens, your terminals will appear offline within IBM Director. You can either wait for the Master controller to be brought back up, or you can rediscover the terminals within Director once the **Alternate Master** has been activated as the **Master**. (Note that this behavior differs from the terminal backup/resume feature that is defined in system configuration under “LAN Terminal Definition”.)

If the RMA Master Agent is running on a 4690 controller and that controller goes down then you will lose RMA connectivity to the entire store. The store will remain offline until the controller running the Master Agent is brought back up, or the Master Agent is configured to run on a different system in the store environment and that new system is added to the Discovery Preferences menu.

In order for RMA to work properly, TCP/IP must be configured for both your terminals and your controller(s). It is not necessary for the TCC protocol to be TCC-IP. Either legacy TCC or TCC-IP may be specified. Controller-to-Controller communication (i.e. how controllers within an MCF system communicate) may be either NetBIOS or CCC-IP. As long as the controllers have TCP/IP enabled, either CCC variety is fine. So, basically, TCP/IP must be configured for both controller and terminals, but the protocols for 4690 communications need not be TCP/IP. See the setup instructions later in this chapter for more details on configuring the correct TCP/IP settings.

Supported Versions / Configurations

RMA is supported on the following versions of 4690 OS:

- V5R2, CSD version 0820 and higher
- V6R1 classic mode
- V6R1 enhanced mode
- V6R2 classic mode
- V6R2 enhanced mode

Note: Although RMA is included with 4690 below V5R2 CSD 0820, the RMA version does not allow management of the 4690 terminals. For that reason, this document does not discuss V5R2 below the 0820 CSD level.

The version of RMA that’s included with each release is described below:

- V5R2, CSD version 0820 and higher – RMA version 2.2
- V6R1 classic mode – RMA version 2.4
- V6R1 enhanced mode – RMA version 2.4
- V6R2 classic mode – RMA version 2.6
- V6R2 enhanced mode – RMA version 2.6

Important Note: Regardless of the version of 4690 you are using, you should always use the most current released version of the RMA Master Agent (if needed), and of the Retail Extensions for Director. At this time, this is IBM Director 5.20.3 with service update 4, Retail Extensions 2.6 (packaged with RMA 2.6 install CD), and RMA version 2.6.

This note, however, does not apply if you are also using self-checkout CHEC software – you should contact techline with any questions about versions of RMA and Director needed with a particular version of CHEC.

Prerequisites

Please be aware that RMA makes use of Java, and requires that VFS-support be enabled within 4690. If your 4690 environment doesn't include these 2 prerequisites, you need to make sure to setup Java and VFS before continuing.

Also be aware that certain Bladecenter network modules (by default) have a setting called "IGMP Snooping". This interferes with RMA multi-cast traffic, and should be disabled on your Bladecenter network module.

Resources

4690 Planning, Installation, and Configuration Guide (PICG) for V5R2:
http://www2.clearlake.ibm.com/store/support/html/pubs.html#4690v5r2

4690 Planning, Installation, and Configuration Guide (PICG) for V6R1:
http://www2.clearlake.ibm.com/store/support/html/pubs.html#4690v6r1

4690 Planning, Installation, and Configuration Guide (PICG) for V6R2:
http://www2.clearlake.ibm.com/store/support/html/pubs.html#4690v6r2

RMA Getting Started Guide (includes links for Director resources):
http://www-01.ibm.com/support/docview.wss?rs=219&uid=pos1R1004204

RMA User's Guide:
http://www2.clearlake.ibm.com/store/support/html/pubs.html#RMA

Capabilities of RMA on 4690 V6R2

The capabilities of RMA on 4690 V6R2 can be summarized as follows:

- General/Master Agent – Under 4690 "enhanced" mode, it's possible to configure a controller to run the RMA master agent (preferably the **Alternate Master** controller if using the multiple controller feature, unless the Alternate Master is also a Controller/Terminal). The other controller(s) run RMA general agents. If you would rather use a separate system (Windows or Linux) for the master agent, that's OK also. (See the “Setup Overview” for V6 below for more details.)

- Peripheral-Attached Devices -- The following terminal devices can be managed remotely (inventory and monitoring, which includes being able to use the "Retail Peripheral Management” task in Director):
    - MSR
    - Line display
    - Cash drawer
    - Tone indicator
    - Keylock
    - Printer
    - MICR
    - Check scanner
    - Keyboard

- Inventory -- Yes, hardware and software inventory, such as system model number, serial number, BIOS version, operating system version, ASM package versions, etc. 4690 V6R2 has more in-depth inventory coverage then previous releases.

- Event Management -- Yes, all 4690 system and application events are forwarded to RMA, and can be used to remotely monitor the solution for health/utilization/etc. 4690 events include extended attributes that allow you to easily filter by things such as the message number. (Note that the severity of the messages is also available within IBM Director, to allow filtering via severity – and to allow your discovery preferences to ignore low-severity messages if desired.)

- Data Capture -- Yes, you can remotely collect log files, config files, etc. for remote problem determination.

- Remote Monitoring -- Yes, all the 4690 Mbeans can be monitored remotely with string/numeric thresholds. For example, you can monitor the disk % free space, memory % free, etc. For 4800-7x4 (classic or enhanced), 4800-7x3 (classic or enhanced) and 4800-7x2 (classic) terminals and controllers, you'll be able to monitor hardware data such as temperature, voltage, fan speed, etc.

- Software Distribution -- Yes, fully integrated with "Apply Software Maintenance" (ASM) for 4690. Can be used to distribute OS updates, application updates, etc.

- Power Management -- Yes, remotely power down, suspend (S3), or restart the terminals. Wake On LAN is also supported on enhanced terminals only. 4690 Controllers only support remote power down and restart.

- File Transfer -- Yes, the RMA File Transfer task is supported to easily transfer files to or from a single 4690 Controller.

Capabilities of RMA on 4690 V6R1

The capabilities of RMA on 4690 V6R1 can be summarized as follows:

- General/Master Agent – Under 4690 "enhanced" mode, it's possible to configure a controller to run the RMA master agent (preferably the **Alternate Master** controller if using the multiple controller feature). The other controller(s) run RMA general agents. If you would rather use a separate system (Windows or Linux) for the master agent, that's OK also. (See the "Setup Overview" for V6 below for more details.)

- Peripheral-Attached Devices -- The following terminal devices can be managed remotely (inventory and monitoring, which includes being able to use the "Retail Peripheral Management" task in Director):
    - MSR
    - Line display
    - Cash drawer
    - Tone indicator
    - Keylock
    - Printer
    - MICR
    - Check scanner
    - Keyboard

- Inventory -- Yes, hardware and software inventory, such as system model number, serial number, BIOS version, operating system version, ASM package versions, etc.

- Event Management -- Yes, all 4690 system and application events are forwarded to RMA, and can be used to remotely monitor the solution for health/utilization/etc. 4690 events include extended attributes that allow you to easily filter by things such as the message number. (Note that the severity of the messages is also available within IBM Director, to allow filtering via severity – and to allow your discovery preferences to ignore low-severity messages if desired.)

- Data Capture -- Yes, you can remotely collect log files, config files, etc. for remote problem determination.

- Remote Monitoring -- Yes, all the 4690 Mbeans can be monitored remotely with string/numeric thresholds. For example, you can monitor the disk % free space, memory % free, etc. For 4800-7x3 (classic or enhanced) and 4800-7x2 (classic) terminals and controllers, you'll be able to monitor hardware data such as temperature, voltage, fan speed, etc.

- Software Distribution -- Yes, fully integrated with "Apply Software Maintenance" (ASM) for 4690. Can be used to distribute OS updates, application updates, etc.

- Power Management -- Yes, remotely power down or restart the terminals. (However, V6R1 does not support the ability to wake up the terminals.)

Capabilities of RMA on 4690 V5R2

The capabilities of RMA on 4690 V5R2 can be summarized as follows:

- General/Master Agent -- In V5R2, it's not possible to run the RMA master agent on 4690. Therefore, all the controllers run RMA as general agents, and you must install the RMA master agent on a separate system (Windows or Linux) in the store.

- Peripheral-Attached Devices -- For V5R2, the following terminal devices can be managed remotely (inventory and monitoring, which includes being able to use the "Retail Peripheral Management Task" in Director):
  - Printer
  - MICR
  - Check scanner
  - Keyboard

- Inventory -- Yes, basic hardware and software inventory, such as system model number, serial number, BIOS version, operating system version, etc. (Note: For V5R2, it's not possible to inventory the software versions of your ASM packages.)

- Event Management – Yes, all 4690 system and application events are forwarded to RMA, and can be used to remotely monitor the solution for health/utilization/etc. There are no extended attributes for events emitted on 4690 V5R2 however, so events must be filtered based on text as opposed to attributes such as message number. (Note that the severity of the messages is also available within IBM Director, to allow filtering via severity – and to allow your discovery preferences to ignore low-severity messages if desired.)

- Data Capture -- Yes, you can remotely collect log files, config files, etc. for remote problem determination.

- Remote Monitoring – No, the "Resource Monitors" task is not supported on 4690 V5R2 due to the older version of RMA that is embedded.

- Software Distribution – No, due to changes required in newer versions to support ASM package distribution, Software Distribution is not supported on pre-V6 versions of 4690.

- Power Management -- No. (Since V5R2 still relies on older RMA agents, the power management features are not available for V5R2).

Comparison of Capabilities of RMA on 4690

	4690 V5R2	4690 V6R1	4690 V6R2
Master Agent on 4690	**No**	**Yes** (for "enhanced mode" only)	**Yes** (for "enhanced mode" only)
RMA Enhanced Security	**No**	**No**	**Yes** (requires 4690 Enhanced Password feature)
Inventory – Basic	**Yes**	**Yes**	**Yes** (more comprehensive)
Inventory – ASM Versions	**No**	**Yes**	**Yes**
Remote Monitoring	**No**	**Yes** – via "Resource Monitors" task (includes sensors, light-path where applicable)	**Yes** – via "Resource Monitors" task (includes sensors, light-path where applicable)
4690 Event Management	**Yes**	**Yes** (includes message attributes)	**Yes** (includes message attributes)
Software Dist. – Basic	**No**	**Yes**	**Yes**
Software Dist. – ASM Updates	**No**	**Yes**	**Yes**
Peripheral Management	**Limited** (keyboard, printer, MICR, scanner)	**Yes** (keyboard, printer, MICR, check scanner, MSR, cash drawer, line display, tone indicator, keylock)	**Yes** (keyboard, printer, MICR, check scanner, MSR, cash drawer, line display, tone indicator, keylock)
Data Capture	**Yes**	**Yes**	**Yes**
Power Management	**No**	**Yes** (shutdown, restart)	**Yes** (shutdown, restart, suspend, WOL where applicable)
RMA File Transfer Task (different then	**No**	**No**	**Yes**

Software Dist)			

Setting up RMA on 4690 V6

Setup Overview

On V6, the RMA software is automatically installed with the operating system, so there is no need to install an additional CSD. Just install the base V6 operating system, and then follow the instructions below to configure your system for RMA.

After you've installed the operating system, you can enable RMA in the system configuration. (By default, RMA is not enabled on 4690.)

The most important choice you need to make is if and where to run the RMA master agent. The guidelines are as follows:

- If you are running V6 in "classic" mode, you cannot run the RMA master agent on 4690. Therefore, you should select "None" (within system configuration, on the systems management screen) as the controller to run the master agent.

- If you select "None", then each controller will run an instance of the RMA general agent. The master agent must be installed on a separate system within the store (Windows or Linux). The controller(s) and terminals in your store will appear within IBM Director as general agents.

- If you are running V6 in "enhanced" mode, you can decide whether to run the master agent on 4690, or on another system in the store (Windows or Linux). If you choose to run it on 4690, you must select which controller will run the master agent. In a multiple controller configuration, you should run the master agent on the **Alternate Master** controller, unless the Alternate Master controller is also running as a Controller/Terminal. (It's not generally recommended to choose the **Master** Controller, for performance reasons.) In a single controller configuration, you must evaluate for yourself whether the performance impact is significant enough to warrant a separate system for the RMA master agent.

- If you select to run the master agent on one of your controllers, then that controller will appear within IBM Director as the RMA master agent. Any other controllers in your environment will appear within Director as general agents.

> **Note**: The RMA master agent does not automatically "failover" if the controller on which it is running goes down. If the controller running the master agent goes down, the entire store will appear offline within IBM Director.

As noted in the overview of RMA on 4690 (see section above), the POS terminals are considered "virtual general agents", and they appear as general agents within IBM

Director. The manageability of the terminals is not affected by your choice of where to run the master agent.

Setup Instructions

After you've installed and properly configured the 4690 operating system using the instructions found in the "4690 Planning, Installation, and Configuration Guide", you should follow the instructions below to prepare the OS for RMA and to enable RMA on the system.

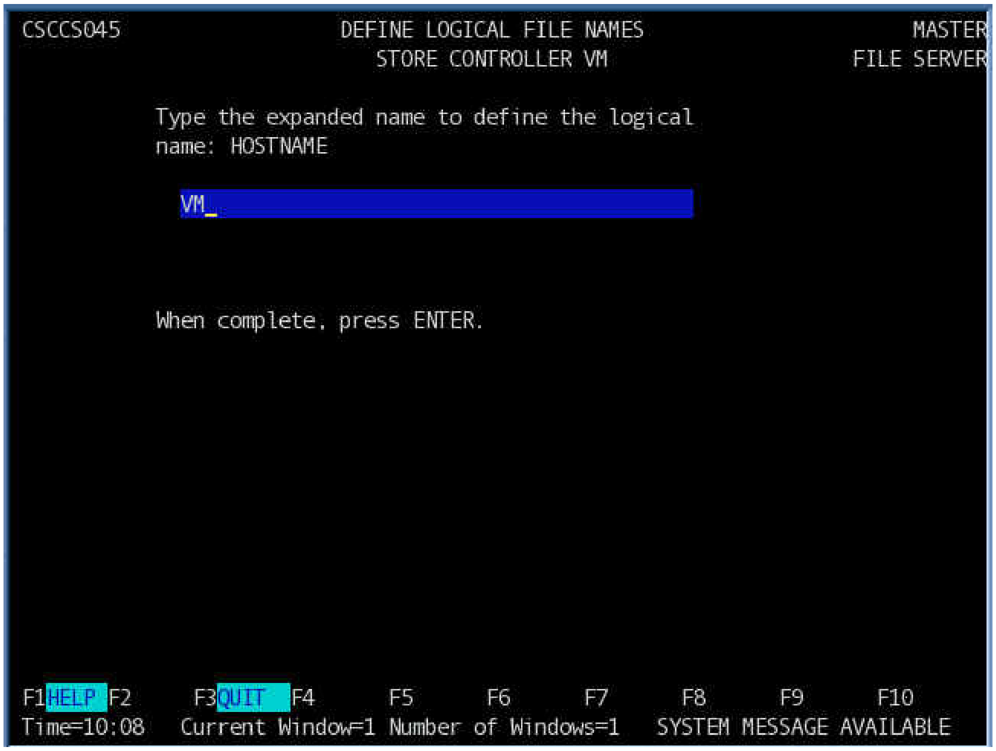
1. Follow the instructions found in the "Systems Management" section (within "Chapter 5" and "System Configuration") in the "4690 Planning, Installation, and Configuration Guide" (i.e. the PICG) -- page 144 at the time of this writing.

> **Note**: The instructions in the PICG are subject to change with new versions of 4690, so always refer to that manual when preparing the controller(s) for RMA.

As you go through the steps in the PICG, you will do the following:

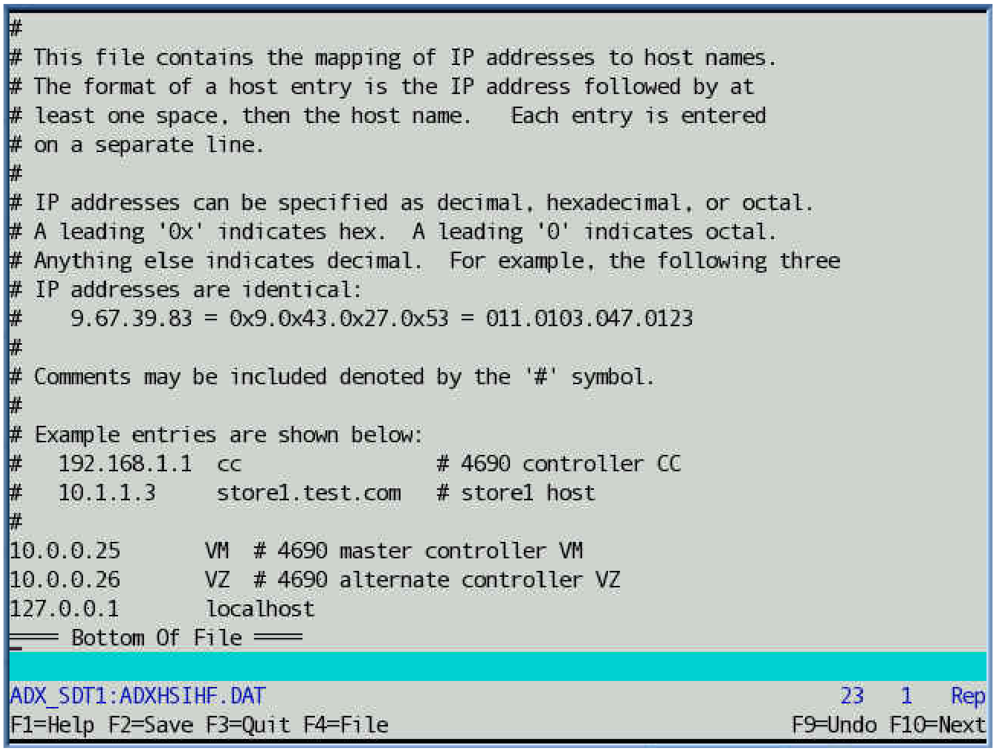
- Define a HOSTNAME logical name (on each controller).
- Make sure the system's HOSTS file has mappings for "localhost" and for each controller's node ID.
- Update the TCP/IP batch file for each controller to include the local loopback address.
- For each "enhanced" mode controller, update the TCP/IP batch file to include the appropriate "eloopaddr" statements. (Note: The "eloopaddr" address is essentially an external loopback address – you should either specify "last", or choose an unused address within the controller's subnet.)

For illustrative purposes only, here are some screenshots of those configuration settings (in these examples, the controller node ID's are "VM" and "VZ"):



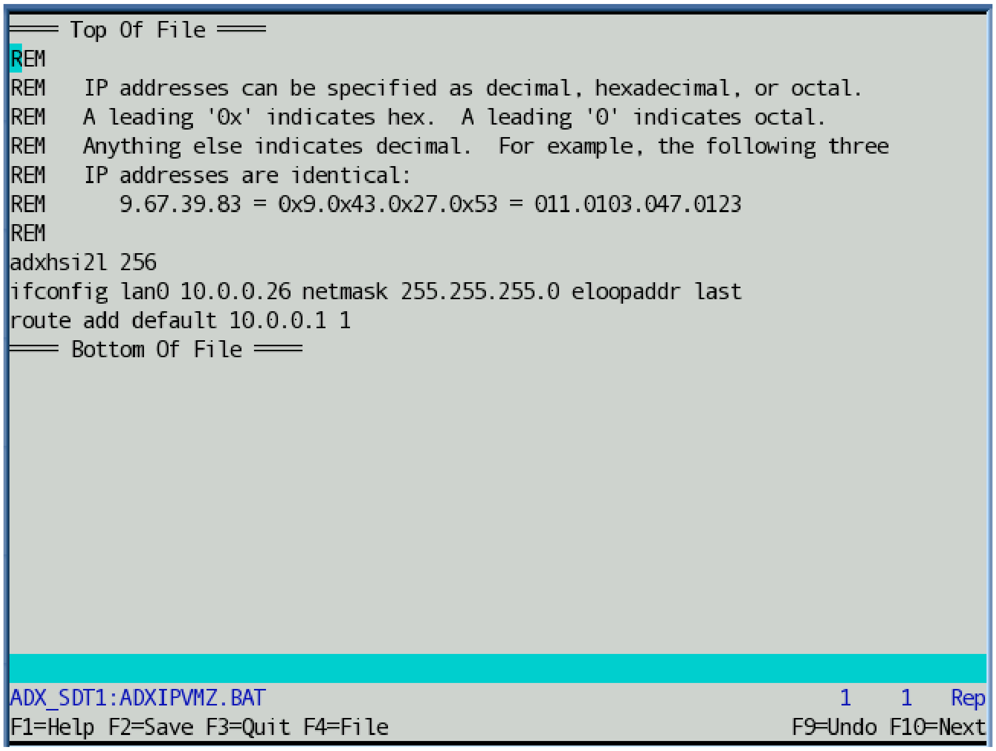
```
CSCCS045                DEFINE LOGICAL FILE NAMES                  MASTER
                           STORE CONTROLLER VM                FILE SERVER

           Type the expanded name to define the logical
           name: HOSTNAME

             VM_



           When complete, press ENTER.










F1HELP F2      F3QUIT   F4      F5      F6      F7      F8      F9      F10
Time=10:08   Current Window=1 Number of Windows=1   SYSTEM MESSAGE AVAILABLE
```

Example only … defining the HOSTNAME logical name (each controller needs this logical name defined with that controller’s node ID)



```
#
# This file contains the mapping of IP addresses to host names.
# The format of a host entry is the IP address followed by at
# least one space, then the host name.   Each entry is entered
# on a separate line.
#
# IP addresses can be specified as decimal, hexadecimal, or octal.
# A leading '0x' indicates hex.  A leading '0' indicates octal.
# Anything else indicates decimal.  For example, the following three
# IP addresses are identical:
#    9.67.39.83 = 0x9.0x43.0x27.0x53 = 011.0103.047.0123
#
# Comments may be included denoted by the '#' symbol.
#
# Example entries are shown below:
#   192.168.1.1  cc                # 4690 controller CC
#   10.1.1.3     store1.test.com   # store1 host
#
10.0.0.25       VM  # 4690 master controller VM
10.0.0.26       VZ  # 4690 alternate controller VZ
127.0.0.1       localhost
==== Bottom Of File ====

ADX_SDT1:ADXHSIHF.DAT                                        23   1   Rep
F1=Help F2=Save F3=Quit F4=File                        F9=Undo F10=Next
```

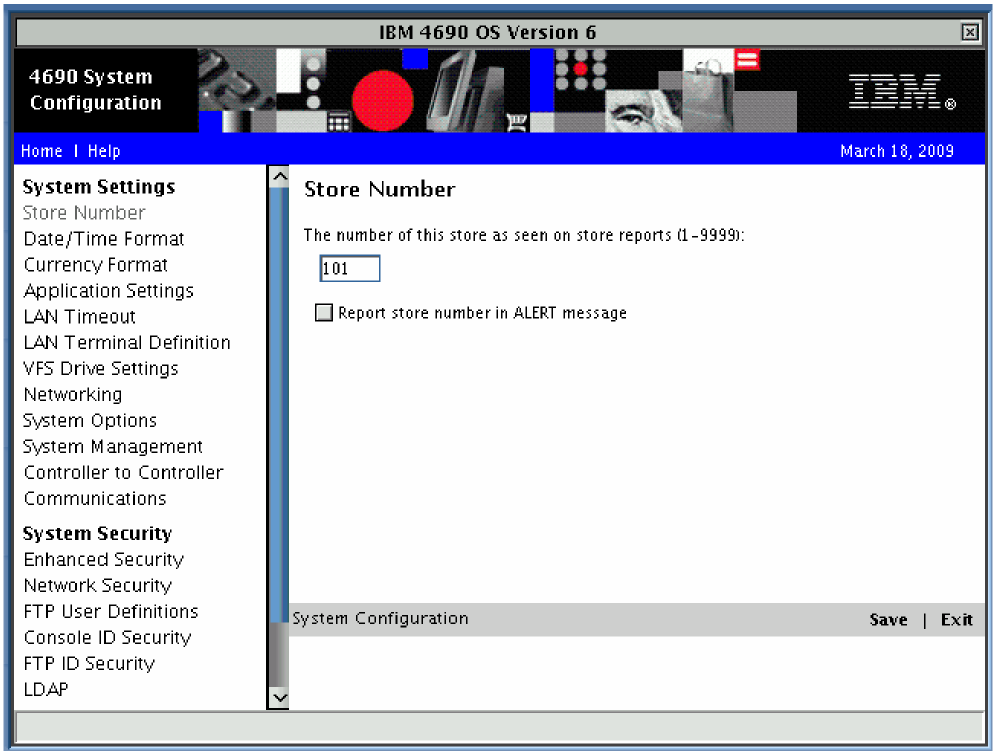
Example only … HOSTS file with localhost and each controller's node ID



```
════ Top Of File ════
REM
REM   IP addresses can be specified as decimal, hexadecimal, or octal.
REM   A leading '0x' indicates hex.  A leading '0' indicates octal.
REM   Anything else indicates decimal.  For example, the following three
REM   IP addresses are identical:
REM      9.67.39.83 = 0x9.0x43.0x27.0x53 = 011.0103.047.0123
REM
adxhsi2l 256
ifconfig lan0 10.0.0.26 netmask 255.255.255.0 eloopaddr last
route add default 10.0.0.1 1
════ Bottom Of File ════
```

Example only … TCP/IP bat file for an enhanced-mode controller (each controller needs a file similar to this one)

2. If you are planning to manage multiple stores within Director and you plan to run the Master Agent on 4690, then it is very important to set the store number (in system configuration) to a unique value for each store.

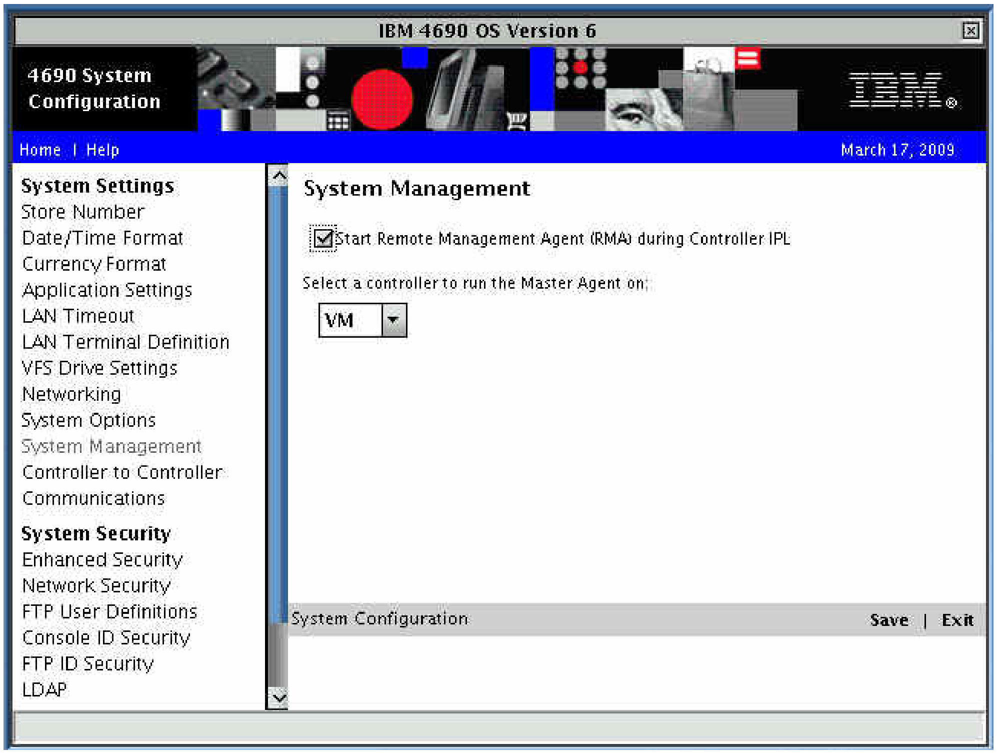


Store Number

The number of this store as seen on store reports (1-9999): 101

□ Report store number in ALERT message

3. The next step is to enable RMA within system configuration. On this screen, you will need to choose whether to run the master agent on 4690 (and specify which controller will be used).



System Management

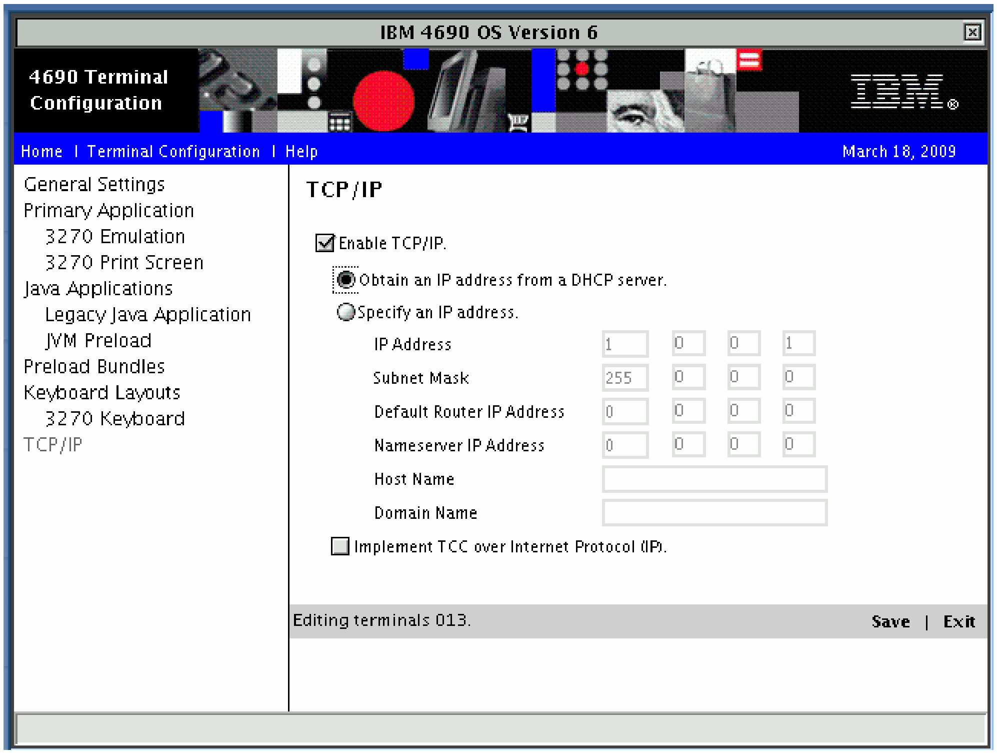
☑ Start Remote Management Agent (RMA) during Controller IPL

Select a controller to run the Master Agent on:

VM

4. Save your setting within system configuration, then “activate” your new system configuration (and reboot).

5. Make sure TCP/IP is enabled for any terminals you want to manage using RMA. To do that, make sure the “Enable TCP/IP” check-box is checked within the terminal load definition for each terminal. The terminal may use DHCP or static IP. Either legacy TCC or TCC/IP may be selected. (After enabling TCP/IP, don’t forget to activate your configuration and reboot the controller and terminals.)



TCP/IP

☑ Enable TCP/IP.

● Obtain an IP address from a DHCP server.

○ Specify an IP address.

IP Address	1	0	0	1
Subnet Mask	255	0	0	0
Default Router IP Address	0	0	0	0
Nameserver IP Address	0	0	0	0
Host Name				
Domain Name				

□ Implement TCC over Internet Protocol (IP).

Editing terminals 013.

6. Verify your setup using the instructions found further below (in the section "Verifying Your RMA Setup").

Setting up RMA on 4690 V5R2

Setup Overview

In V5R2, RMA is released with the base operating system, but it still comes on a separate CSD ("Corrective Service Diskette"). So, the first step in setting up RMA on V5R2 is to obtain and install the CSD for systems management. This is done via the same ASM ("Apply Software Maintenance") process that's used for other operating system CSD's.

> **Note**: It's very important that the CSD version for systems management match the CSD version for the base operating system. For example, if the 4690 OS is at version 0900, then the systems management CSD must also be at version 0900!

After you've installed the CSD for systems management, then the setup process is very similar to the setup process for V6. You will prepare the controller(s) with the correct TCP/IP settings, enable RMA, and enable your terminals for TCP/IP so RMA can manage them also.

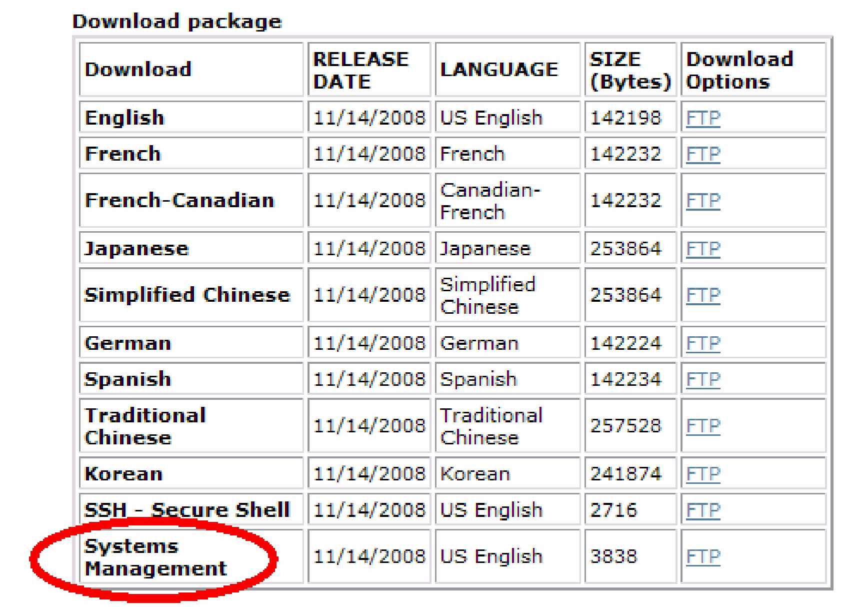
On V5R2, you do not have the option to run the RMA master agent on 4690. Therefore, you **must install the RMA master agent on a separate system** (Windows or Linux) within the store. The controller(s) in your 4690 environment will all appear as RMA general agents within IBM Director.

As noted in the overview of RMA on 4690 (see section above), the POS terminals are considered "virtual general agents", and they appear as general agents within IBM Director.

Setup Instructions

After you've installed and properly configured the 4690 operating system using the instructions found in the "4690 Planning, Installation, and Configuration Guide", you should follow the instructions below to install RMA, prepare the OS for RMA, and to enable RMA on the system.

1. Make sure you install the CSD for systems management on 4690. The CSD level for systems management MUST match the CSD level of the OS. You can download it here: http://www-01.ibm.com/support/docview.wss?rs=219&uid=pos1R4000217



Download package

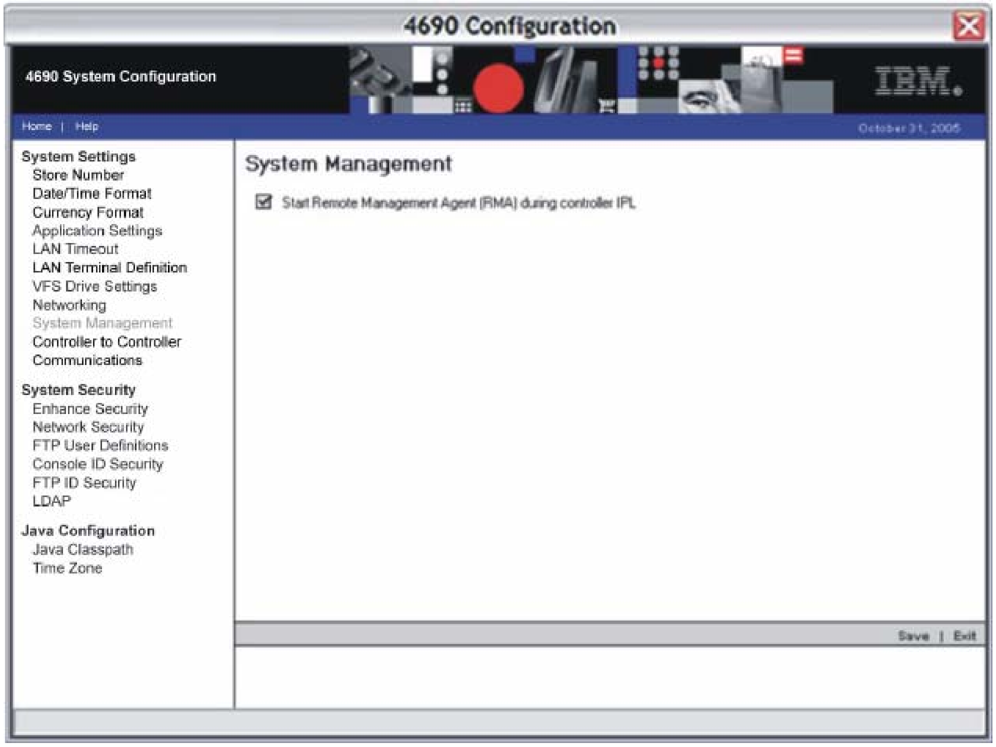
Download	RELEASE DATE	LANGUAGE	SIZE (Bytes)	Download Options
English	11/14/2008	US English	142198	FTP
French	11/14/2008	French	142232	FTP
French-Canadian	11/14/2008	Canadian-French	142232	FTP
Japanese	11/14/2008	Japanese	253864	FTP
Simplified Chinese	11/14/2008	Simplified Chinese	253864	FTP
German	11/14/2008	German	142224	FTP
Spanish	11/14/2008	Spanish	142234	FTP
Traditional Chinese	11/14/2008	Traditional Chinese	257528	FTP
Korean	11/14/2008	Korean	241874	FTP
SSH - Secure Shell	11/14/2008	US English	2716	FTP
Systems Management	11/14/2008	US English	3838	FTP

2. Follow the instructions in this document to make sure the controller is ready for RMA on 4690 V5R2: http://www-01.ibm.com/support/docview.wss?rs=219&uid=pos1R1003787

   As with V6, you will need to do the following as you follow the instructions at the above URL:

- Define a HOSTNAME logical name (on each controller).
- Make sure the system’s HOSTS file has mappings for “localhost” and for each controller’s node ID.
- Update the TCP/IP batch file for each controller to include the local loopback address.
- Make sure the TCP/IP batch file includes a “default route” command.

3. The next step is to enable RMA within system configuration.



System Management

☑ Start Remote Management Agent (RMA) during controller IPL

4. Save your setting within system configuration, then “activate” your new system configuration (and reboot).

5. Make sure TCP/IP is enabled for any terminals you want to manage using RMA. To do that, make sure the “Enable TCP/IP” check-box is checked within the terminal load definition for each terminal. The terminal may use DHCP or static IP. Either legacy TCC or TCC/IP may be selected. (After enabling TCP/IP, don’t forget to activate your configuration and reboot the controller and terminals.)

6. Verify your setup using the instructions found further below (in the section “Verifying Your RMA Setup”).

Verifying Your 4690 RMA Setup

At this point, your 4690 controller(s) and terminals should be running RMA, but you have not yet verified that it's working properly. Follow these steps to complete the solution, and verify everything is working as it should be:

1. You may want to double-check the following:
   - ✓ Java and VFS support must be enabled on the controllers
   - ✓ (V5R2 only) Make sure the CSD for systems management is installed at the same CSD level as the OS
   - ✓ HOSTNAME logical name is defined for each controller
   - ✓ adxhsihf.dat (i.e. the HOSTS file) has an entry for each controller's node ID, and an entry for localhost.
   - ✓ adxipXXz.bat (i.e. where XX is the node ID) is set up correctly for each controller – it should have an entry for "lan0", "lo0", and a "default route" command.
   - ✓ (V6 only) For enhanced-mode controllers, adxipXXz.bat contains the "eloopaddr" parameter for lan0.
   - ✓ RMA is enabled in system configuration
   - ✓ Terminals have TCP/IP enabled
   - ✓ If using certain Bladecenter network modules, "IGMP Snooping" must be disabled

   > **Note**: As a sanity check, it's a good idea to try to "ping" the IP address of each controller and terminal from outside the system, just to make sure your TCP/IP settings are correct.

2. You may want to verify that RMA appears to be working OK, by examining the RMA log file. To do that, open the following file using "xe" (or any text editor):

   On V5R2:

   ```
   M:\rma\logs\RMA_XX.0 (where XX = controller node ID)
   ```

   On V6:

   ```
   F:\rma\logs\simgmt.0
   ```

   Scroll through the file, making sure there are no "severe" messages or java exceptions in the file. ("Warning" messages are generally OK, but may be of interest if problems arise later in your use of RMA.)

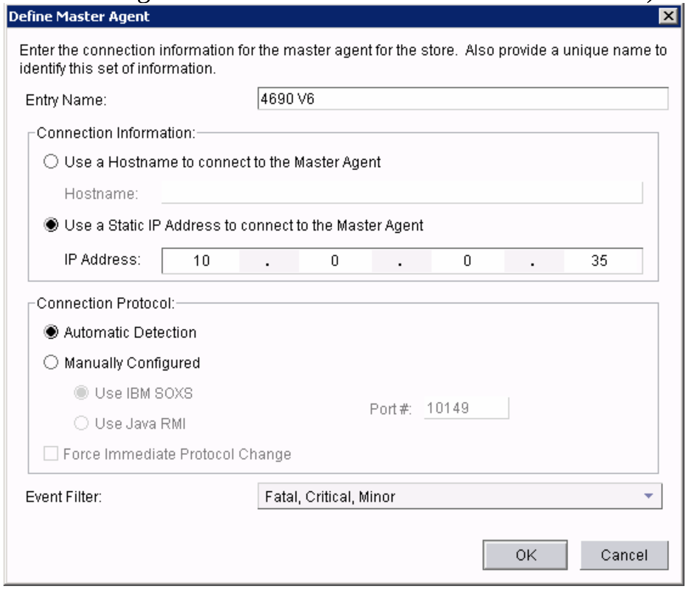
   > **Note**: If the log file doesn't exist, RMA is not running. (Make sure you "activated" your system configuration!) If the Controller in question is a Controller/Terminal, then RMA will not start until the Terminal side of the

Controller/Terminal is up and running. Verify that the terminal side is running before looking for the RMA logs.

3. If you're not running the master agent on one of the 4690 controllers, make sure you've installed the RMA master agent on a separate system within the store. You should make sure the master agent can "ping" the controller. (For help, see "**Chapter 1 – Quick-Install Guide**".)

4. Make sure IBM Director is set up on a Windows or Linux system that has connectivity to the store. You should make sure it can "ping" the master agent's IP address in the store. (For help, see "**Chapter 1 – Quick-Install Guide**".)

5. Add your master agent into the discovery preferences for Director, and click the discovery icon in the toolbar to discover your device. (In our lab example system, the master agent is the same as the 4690 master controller.)



Define Master Agent

Enter the connection information for the master agent for the store. Also provide a unique name to identify this set of information.

Entry Name: 4690 V6

Connection Information:

○ Use a Hostname to connect to the Master Agent

Hostname:

● Use a Static IP Address to connect to the Master Agent

IP Address: 10 . 0 . 0 . 35

Connection Protocol:

● Automatic Detection

○ Manually Configured

● Use IBM SOXS

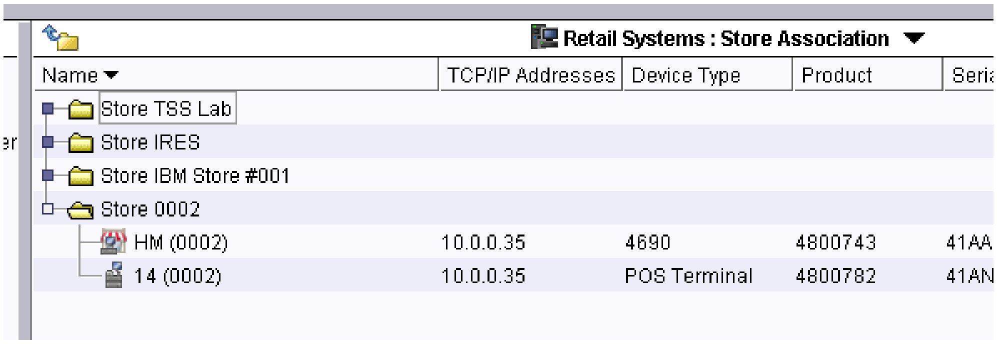
○ Use Java RMI

Port #: 10149

□ Force Immediate Protocol Change

Event Filter: Fatal, Critical, Minor

6. You should now see your master agent, your controller(s), and your terminals in the main Director console.



Retail Systems : Store Association

Name	TCP/IP Addresses	Device Type	Product	Seria
Store TSS Lab				
Store IRES				
Store IBM Store #001				
Store 0002				
HM (0002)	10.0.0.35	4690	4800743	41AA
14 (0002)	10.0.0.35	POS Terminal	4800782	41AN

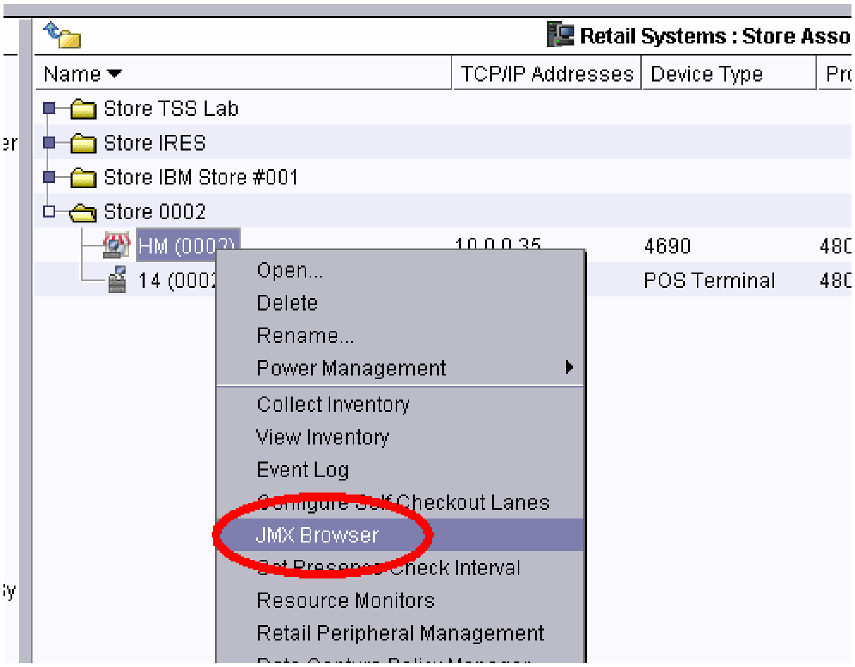
In the screenshot above, you can see:

- HM – the RMA master agent, which is also the 4690 Master controller
- 14 – the only terminal set up for this controller
- Store “0002” was configured in 4690 as the store number, and it appears in parentheses next to each of the 4690 managed objects

Note: The Director inventory will show your terminals as having the same IP address as your controller. The reason for this is that the terminal’s “virtual” RMA code is actually running on the controller.

Also note: If you are using IBM Store Integrator components on the controller (i.e. such as SI GUI, AEF, DIF, etc.), you may see more managed objects in addition to those shown above.

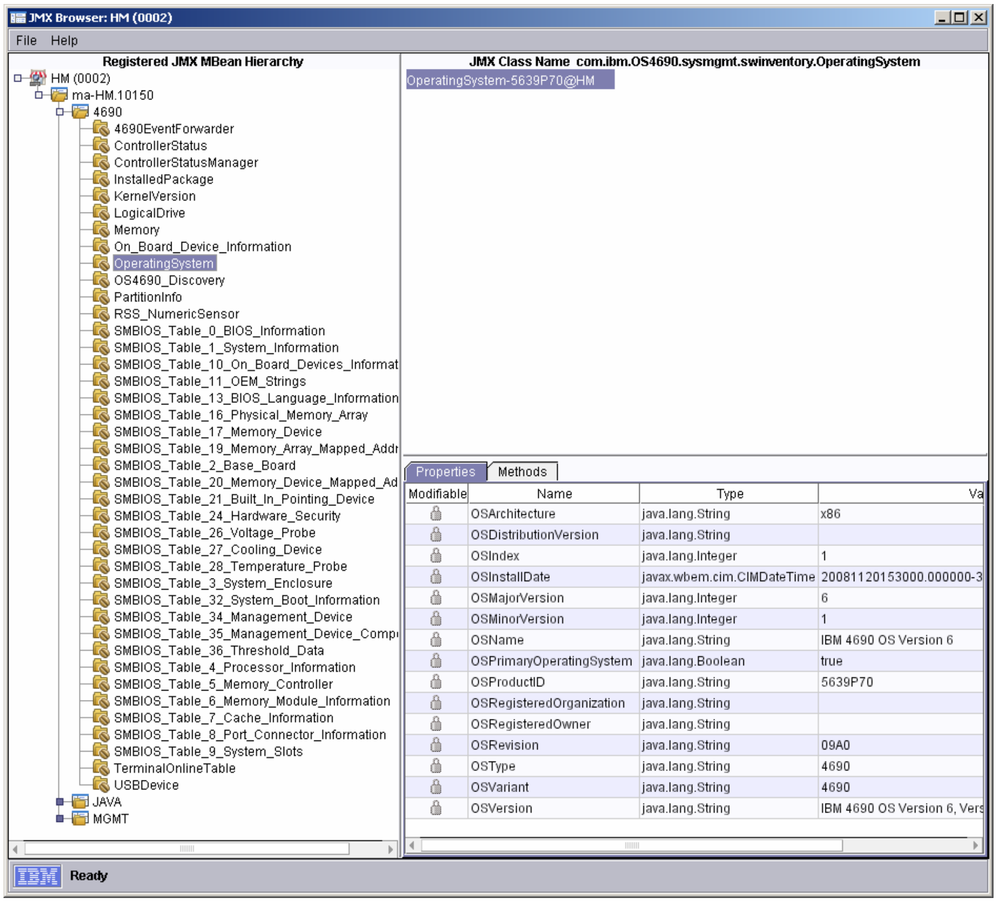
7. Next, open the JMX browser for the controller.



Retail Systems : Store Asso
Open...
Delete
Rename...
Power Management
Collect Inventory
View Inventory
Event Log
Configure Self Checkout Lanes
JMX Browser
Set Presence Check Interval
Resource Monitors
Retail Peripheral Management
Data Capture Policy Manager

Name	TCP/IP Addresses	Device Type	Pr
Store TSS Lab			
Store IRES			
Store IBM Store #001			
Store 0002			
HM (0002)	10.0.0.35	4690	480
14 (0002		POS Terminal	480

8. The MBeans for a 4690 controller should look similar to the screenshot below. (Please be aware that this screenshot represents a 4690 V6 controller, which contains more instrumentation than for V5R2, but even for V5R2 you should see most of the content shown here.)



Registered JMX MBean Hierarchy

```
HM (0002)
  ma-HM.10150
    4690
      4690EventForwarder
      ControllerStatus
      ControllerStatusManager
      InstalledPackage
      KernelVersion
      LogicalDrive
      Memory
      On_Board_Device_Information
      OperatingSystem
      OS4690_Discovery
      PartitionInfo
      RSS_NumericSensor
      SMBIOS_Table_0_BIOS_Information
      SMBIOS_Table_1_System_Information
      SMBIOS_Table_10_On_Board_Devices_Informat
      SMBIOS_Table_11_OEM_Strings
      SMBIOS_Table_13_BIOS_Language_Information
      SMBIOS_Table_16_Physical_Memory_Array
      SMBIOS_Table_17_Memory_Device
      SMBIOS_Table_19_Memory_Array_Mapped_Addr
      SMBIOS_Table_2_Base_Board
      SMBIOS_Table_20_Memory_Device_Mapped_Ad
      SMBIOS_Table_21_Built_In_Pointing_Device
      SMBIOS_Table_24_Hardware_Security
      SMBIOS_Table_26_Voltage_Probe
      SMBIOS_Table_27_Cooling_Device
      SMBIOS_Table_28_Temperature_Probe
      SMBIOS_Table_3_System_Enclosure
      SMBIOS_Table_32_System_Boot_Information
      SMBIOS_Table_34_Management_Device
      SMBIOS_Table_35_Management_Device_Comp
      SMBIOS_Table_36_Threshold_Data
      SMBIOS_Table_4_Processor_Information
      SMBIOS_Table_5_Memory_Controller
      SMBIOS_Table_6_Memory_Module_Information
      SMBIOS_Table_7_Cache_Information
      SMBIOS_Table_8_Port_Connector_Information
      SMBIOS_Table_9_System_Slots
      TerminalOnlineTable
      USBDevice
    JAVA
    MGMT
```

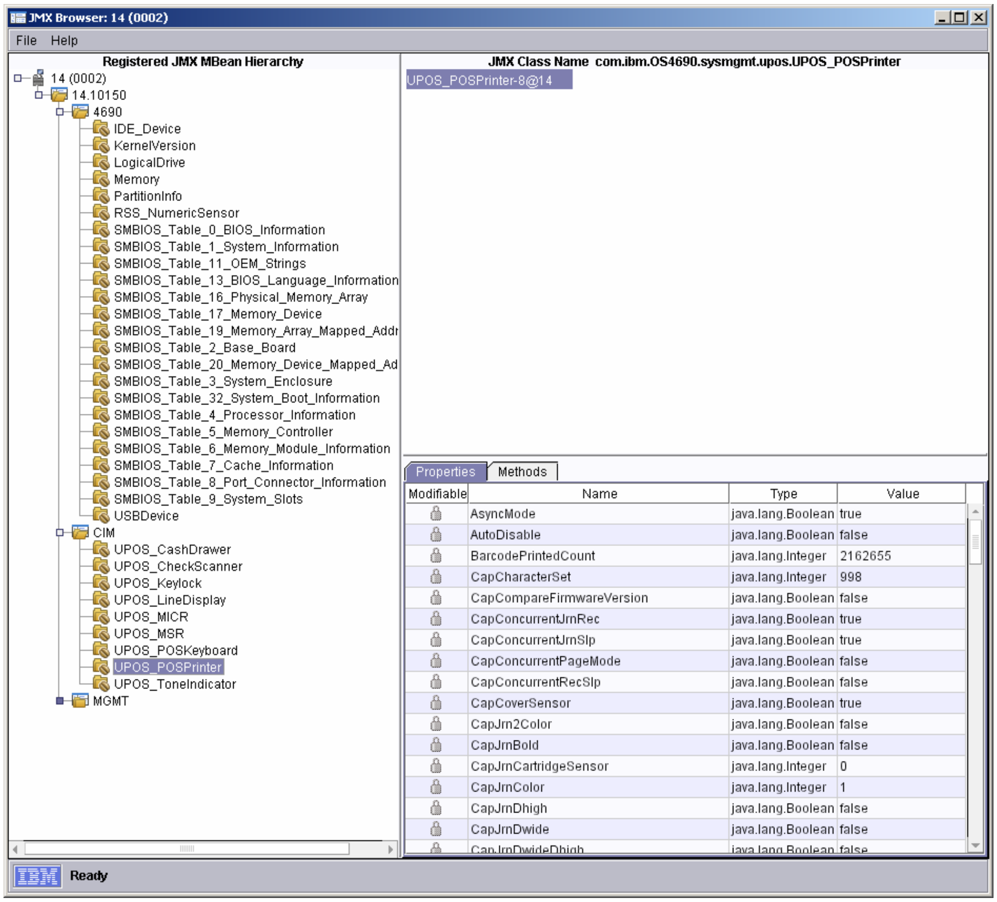
JMX Class Name com.ibm.OS4690.sysmgmt.swinventory.OperatingSystem

OperatingSystem-5639P70@HM

Modifiable	Name	Type	Va
🔒	OSArchitecture	java.lang.String	x86
🔒	OSDistributionVersion	java.lang.String	
🔒	OSIndex	java.lang.Integer	1
🔒	OSInstallDate	javax.wbem.cim.CIMDateTime	20081120153000.000000-3
🔒	OSMajorVersion	java.lang.Integer	6
🔒	OSMinorVersion	java.lang.Integer	1
🔒	OSName	java.lang.String	IBM 4690 OS Version 6
🔒	OSPrimaryOperatingSystem	java.lang.Boolean	true
🔒	OSProductID	java.lang.String	5639P70
🔒	OSRegisteredOrganization	java.lang.String	
🔒	OSRegisteredOwner	java.lang.String	
🔒	OSRevision	java.lang.String	09A0
🔒	OSType	java.lang.String	4690
🔒	OSVariant	java.lang.String	4690
🔒	OSVersion	java.lang.String	IBM 4690 OS Version 6, Vers

In the screenshot above, you can see MBeans that describe SMBIOS information, system memory, hard disk drive attributes, and more. If you are using a 4800-7x2, 4800-7x3 or 4800-7x4, you'll see the "RSS_NumericSensor" MBeans in the "4690" category. These represent the system's sensors and/or service processor values (i.e. motherboard, power supply, temperature(s), voltage(s), etc.).

9. Next, use the JMX browser to view the terminal's instrumentation. The MBeans for a 4690 terminal should look similar to the screenshot below. (Again, note that this screenshot represents a V6 terminal rather than a V5R2 terminal.)


JMX Browser: 14 (0002)
File
Help
Registered JMX MBean Hierarchy
14 (0002)
14.10150
4690
IDE_Device
KernelVersion
LogicalDrive
Memory
PartitionInfo
RSS_NumericSensor
SMBIOS_Table_0_BIOS_Information
SMBIOS_Table_1_System_Information
SMBIOS_Table_11_OEM_Strings
SMBIOS_Table_13_BIOS_Language_Information
SMBIOS_Table_16_Physical_Memory_Array
SMBIOS_Table_17_Memory_Device
SMBIOS_Table_19_Memory_Array_Mapped_Addr
SMBIOS_Table_2_Base_Board
SMBIOS_Table_20_Memory_Device_Mapped_Ad
SMBIOS_Table_3_System_Enclosure
SMBIOS_Table_32_System_Boot_Information
SMBIOS_Table_4_Processor_Information
SMBIOS_Table_5_Memory_Controller
SMBIOS_Table_6_Memory_Module_Information
SMBIOS_Table_7_Cache_Information
SMBIOS_Table_8_Port_Connector_Information
SMBIOS_Table_9_System_Slots
USBDevice
CIM
UPOS_CashDrawer
UPOS_CheckScanner
UPOS_Keylock
UPOS_LineDisplay
UPOS_MICR
UPOS_MSR
UPOS_POSKeyboard
UPOS_POSPrinter
UPOS_ToneIndicator
MGMT
JMX Class Name com.ibm.OS4690.sysmgmt.upos.UPOS_POSPrinter
UPOS_POSPrinter-8@14
Properties
Methods
IBM
Ready

Modifiable	Name	Type	Value
🔒	AsyncMode	java.lang.Boolean	true
🔒	AutoDisable	java.lang.Boolean	false
🔒	BarcodePrintedCount	java.lang.Integer	2162655
🔒	CapCharacterSet	java.lang.Integer	998
🔒	CapCompareFirmwareVersion	java.lang.Boolean	false
🔒	CapConcurrentJrnRec	java.lang.Boolean	true
🔒	CapConcurrentJrnSlp	java.lang.Boolean	true
🔒	CapConcurrentPageMode	java.lang.Boolean	false
🔒	CapConcurrentRecSlp	java.lang.Boolean	false
🔒	CapCoverSensor	java.lang.Boolean	true
🔒	CapJrn2Color	java.lang.Boolean	false
🔒	CapJrnBold	java.lang.Boolean	false
🔒	CapJrnCartridgeSensor	java.lang.Integer	0
🔒	CapJrnColor	java.lang.Integer	1
🔒	CapJrnDhigh	java.lang.Boolean	false
🔒	CapJrnDwide	java.lang.Boolean	false
🔒	CapJrnDwideDhigh	java.lang.Boolean	false

In the screenshot above, you can see the "RSS_NumericSensor" MBean for the 4800-7x2 sensors on the terminal, in addition to many other instrumentation MBeans for the terminal – including comprehensive SMBIOS information, memory, disk drive, etc.

You can also see a variety of "UPOS" MBeans in the "CIM" section of the browser. These represent the peripheral devices (such as a 4610 printer) that are attached to the terminal. Refer to the "Retail Peripheral Management" section of the RMA cookbook for more information about leveraging this information. (Note that on V5R2, the peripheral information is more limited than on V6.)

10. After you've verified that all the MBeans look correct for 4690 within the JMX Browser, you're now ready to begin using all the other features of RMA and IBM Director to manage your 4690 environment – such as inventory, resource monitoring, software distribution, power management, etc. (For help, please refer to the other chapters of this cookbook, the RMA user's guide, and the IBM Director documentation.)

Chapter 3 – Setting Up RMA on Novell Linux

This chapter describes how to setup RMA on Novell's SuSE Linux Enterprise 11 operating systems. RMA V2R6 is not supported on any other Linux distributions.

RMA includes support for Novell-based Linux distributions as follows:

- SLED (SuSE Linux Enterprise Desktop) 11 SP1. RMA version 2.6 supports SuSE Linux Enterprise Desktop (SLED) 11 SP1.

- SLES (SuSE Linux Enterprise Server) 11 SP1. RMA version 2.6 supports SuSE Linux Enterprise Server (SLES) 11 SP1.

- SLEPOS (SuSE Linux Enterprise Point Of Service) 11 SP1. RMA version 2.6 supports SuSE Linux Enterprise Point Of Service (SLEPOS) 11 SP1.

  Starting with SLE 11 (and RMA 2.5), IBM now offers full-featured systems management capabilities for Linux, including the following:
  - Sensor drivers to monitor hardware sensor values and service processor "light-path" LED status
  - CIM instrumentation for the operating system to allow inventory and monitoring for the OS
  - Systems management instrumentation available via UPOS 1.12 and higher
  - Event forwarding for Linux CIM instrumentation – for the first time on Linux, it is possible to receive events and alerts from UPOS-based peripheral-attached devices.

Setting up RMA on SLED / SLES 11 SP1

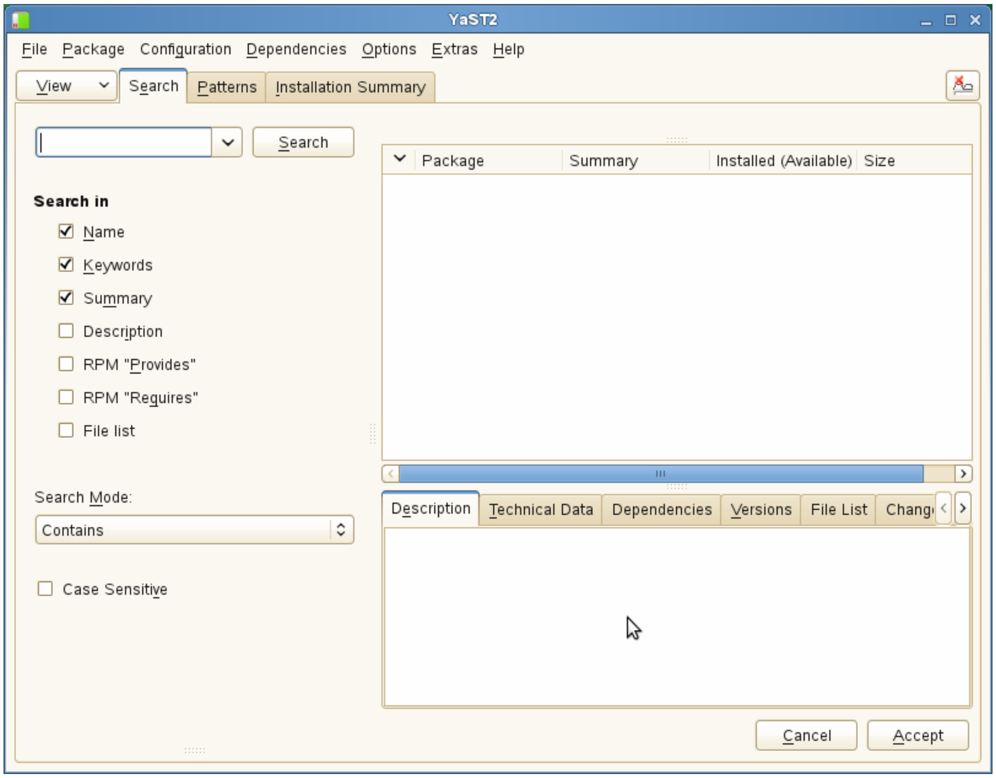
Either the RMA Master Agent or RMA General Agent can be installed on SuSE Linux Enterprise Desktop (SLED) or SuSE Linux Enterprise Server (SLES) 11 SP1. The RMA Master Agent will be required on a single system within the store environment. All of the other systems within the store should run the RMA General Agent.

Prerequisites

Prior to installing the RMA agent on SLED 11 SP1, the systems need to be installed and configured with SFCB. SFCB stands for the "Small Footprint CIM Broker" and is what provides hardware information about the system to the RMA Agent. It is similar to WMI on Windows. SFCB works in conjunction with several SBLIM packages that do the actual data population. SBLIM stands for the "Standards Based Linux Instrumentations for Manageability".

The following steps explain how to get SFCB installed and configured on a SLED / SLES 11 system:

1. To install the SFCB and SBLIM packages, click on Computer -> Install Packages. This will bring up a browser that will allow you to search for particular RPM packages to install:



Search in

☑ Name
☑ Keywords
☑ Summary
□ Description
□ RPM "Provides"
□ RPM "Requires"
□ File list

Search Mode: Contains

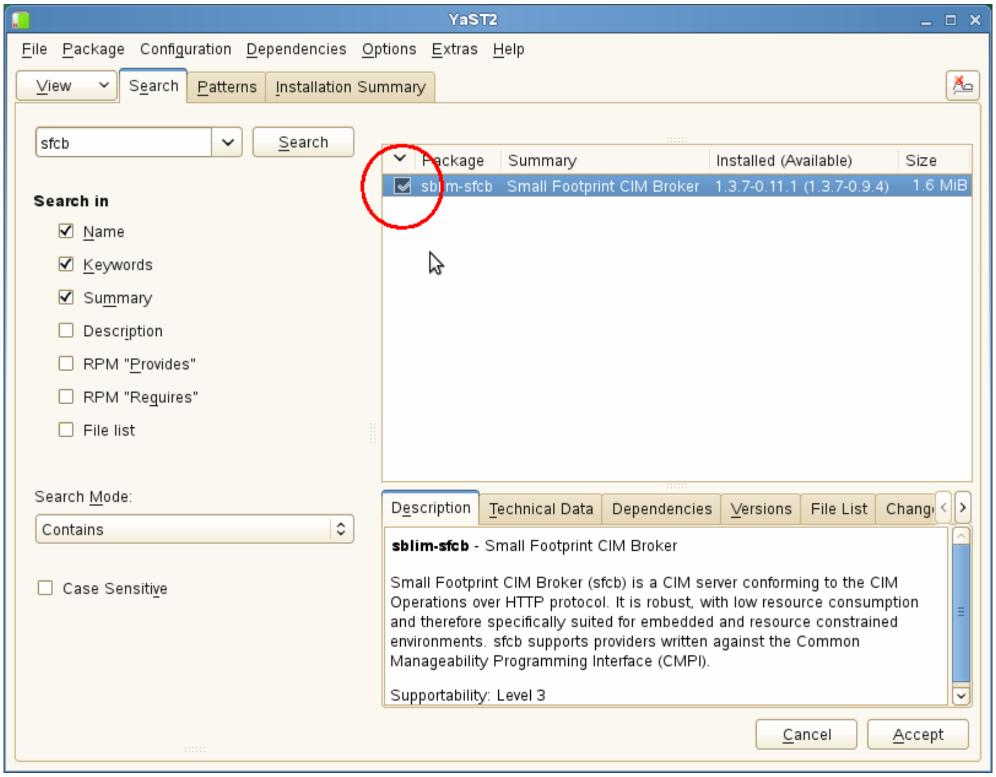
□ Case Sensitive

2. Click on the “Search” tab and search for each of the following packages:

- sblim-sfcb
- sblim-sfcc
- cim-schema
- cmpi-provider-register
- libRaTools0
- libsblim-cmpiutil1
- sblim-cim-client2
- sblim-cmpi-base
- sblim-cmpi-dhcp
- sblim-cmpi-fsvol
- sblim-cmpi-network

- sblim-cmpi-nfsv3
- sblim-cmpi-nfsv4
- sblim-cmpi-params
- sblim-cmpi-smbios
- sblim-cmpi-sysfs
- sblim-indication_helper
- sblim-wbemcli

3. As each package is brought up, ensure that the box is checked next to the package name so that the package will get installed:



sfcb

Search in

☑ Name
☑ Keywords
☑ Summary
☐ Description
☐ RPM "Provides"
☐ RPM "Requires"
☐ File list

Search Mode: Contains

☐ Case Sensitive

	Package	Summary	Installed (Available)	Size
☑	sblim-sfcb	Small Footprint CIM Broker	1.3.7-0.11.1 (1.3.7-0.9.4)	1.6 MiB

Description | Technical Data | Dependencies | Versions | File List | Chang

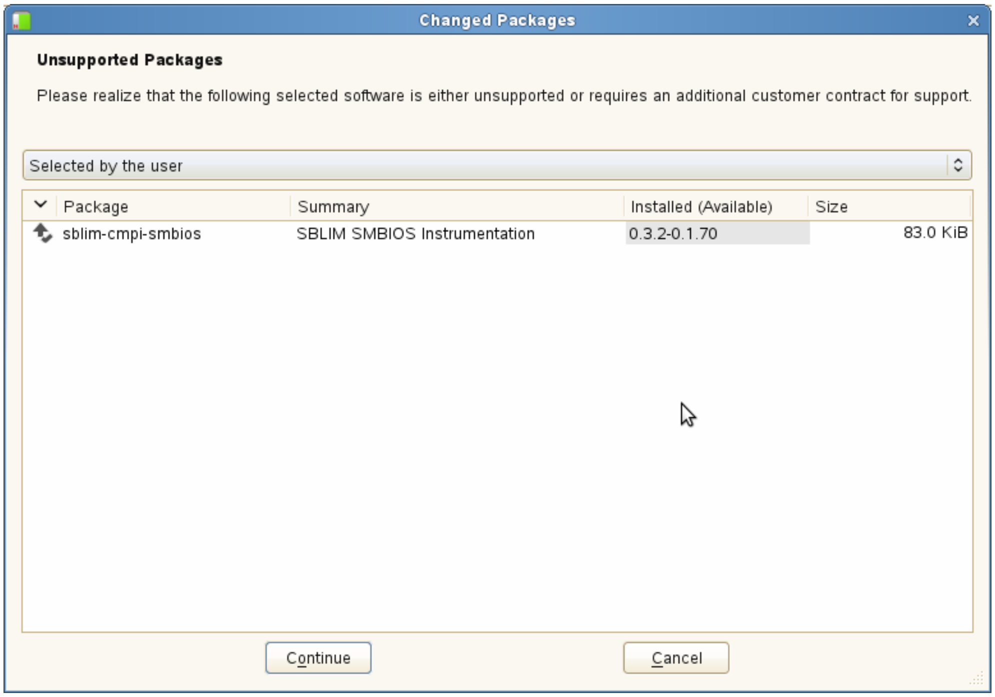
sblim-sfcb - Small Footprint CIM Broker

Small Footprint CIM Broker (sfcb) is a CIM server conforming to the CIM Operations over HTTP protocol. It is robust, with low resource consumption and therefore specifically suited for embedded and resource constrained environments. sfcb supports providers written against the Common Manageability Programming Interface (CMPI).

Supportability: Level 3

4. Once all of the packages have been selected, click “Accept” to start the install.

5. Click “Continue” on any warning or dependency pop-ups that may appear:



Changed Packages

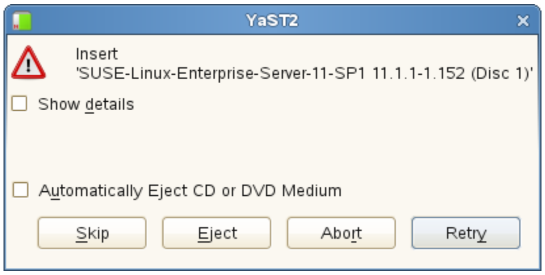
Unsupported Packages

Please realize that the following selected software is either unsupported or requires an additional customer contract for support.

Selected by the user

Package	Summary	Installed (Available)	Size
sblim-cmpi-smbios	SBLIM SMBIOS Instrumentation	0.3.2-0.1.70	83.0 KiB

6. Be sure to have the installation media handy as it will be required to add the packages:



YaST2

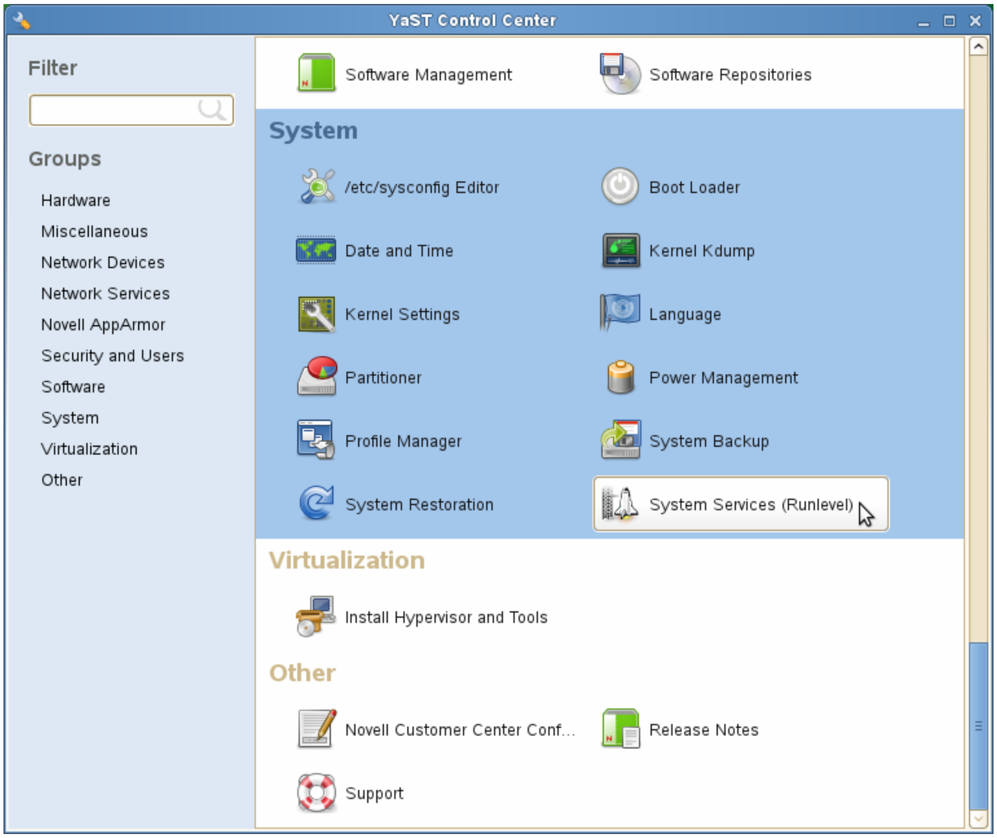
Insert 'SUSE-Linux-Enterprise-Server-11-SP1 11.1.1-1.152 (Disc 1)'

□ Show details

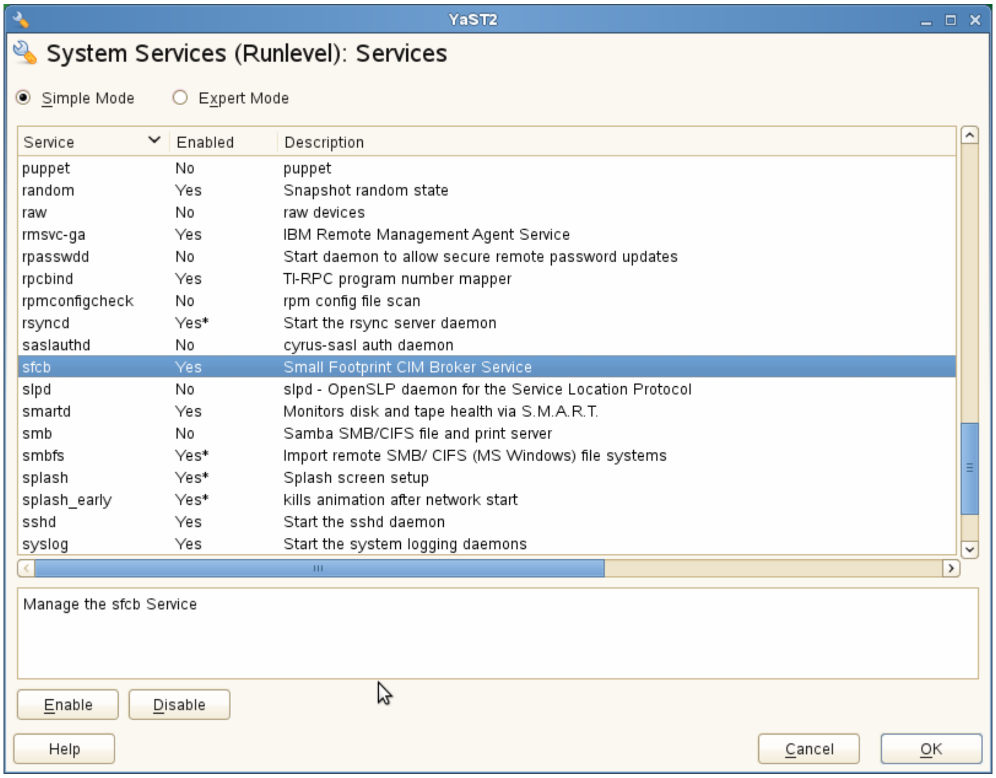
□ Automatically Eject CD or DVD Medium

7. After the packages are installed, use a text editor to modify the SFCB Configuration File:
   a. Edit **/etc/sfcb/sfcb.cfg**
   b. Set **enableHttp** to **true**
   c. Set **doBasicAuth** to **false**
   d. Set **provProcs** to **40**
   e. Save the file and restart sfcb: **/etc/init.d/sfcb restart**

8. Launch the Control Center and select the “System Service (Runlevel)” option under “System”:



9. Verify that the sfcb service in Enabled. If not, select it and click the “Enable” button:

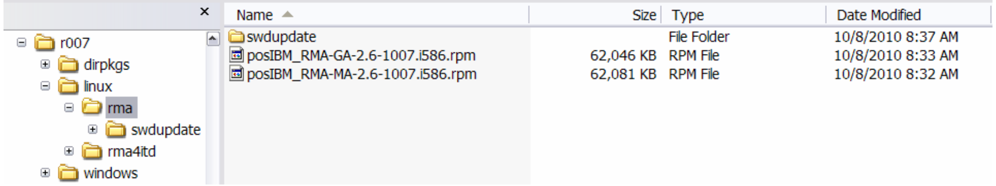


Service	Enabled	Description
puppet	No	puppet
random	Yes	Snapshot random state
raw	No	raw devices
rmsvc-ga	Yes	IBM Remote Management Agent Service
rpasswdd	No	Start daemon to allow secure remote password updates
rpcbind	Yes	TI-RPC program number mapper
rpmconfigcheck	No	rpm config file scan
rsyncd	Yes*	Start the rsync server daemon
saslauthd	No	cyrus-sasl auth daemon
sfcb	Yes	Small Footprint CIM Broker Service
slpd	No	slpd - OpenSLP daemon for the Service Location Protocol
smartd	Yes	Monitors disk and tape health via S.M.A.R.T.
smb	No	Samba SMB/CIFS file and print server
smbfs	Yes*	Import remote SMB/ CIFS (MS Windows) file systems
splash	Yes*	Splash screen setup
splash_early	Yes*	kills animation after network start
sshd	Yes	Start the sshd daemon
syslog	Yes	Start the system logging daemons

Manage the sfcb Service

Installing the RMA Agent

On the installation media there are two rpm's for the RMA Agent installs:



Name	Size	Type	Date Modified
swdupdate		File Folder	10/8/2010 8:37 AM
posIBM_RMA-GA-2.6-1007.i586.rpm	62,046 KB	RPM File	10/8/2010 8:33 AM
posIBM_RMA-MA-2.6-1007.i586.rpm	62,081 KB	RPM File	10/8/2010 8:32 AM

The RMA-GA rpm is for the RMA General Agent install, and the RMA-MA rpm is for the RMA Master Agent install.

To install the RMA Agent, execute the following command on the desired rpm file from a terminal window:

```
rpm –ivh posIBM_RMA-GA-2.6-1007.i586.rpm
```

After the initial install, the agent has to be configured by running the rma-config.sh script

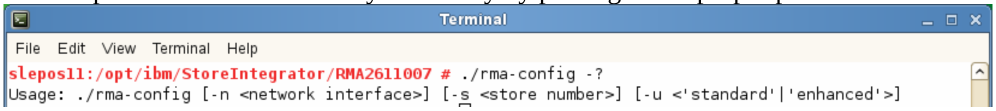
This script will be in a location similar to the following:

/opt/ibm/StoreIntegrator/RMA26110007/rma-config.sh

On a Master Agent system, the rma-config.sh script is used to set the following parameters:

- Store Name
- Network Interface
- Security Mode

The script can be run interactively or silently by passing in the proper parameters:



```
sleposl1:/opt/ibm/StoreIntegrator/RMA2611007 # ./rma-config -?
Usage: ./rma-config [-n <network interface>] [-s <store number>] [-u <'standard'|'enhanced'>]
```

The rma-config.sh script works the same way on a General Agent system except that only the network interface is required.

After running the configuration script, simply start the agent service by running one of the following two commands based on the agent type:

/etc/init.d/rmsvc-ga start
/etc/init.d/rmsvc-ma start

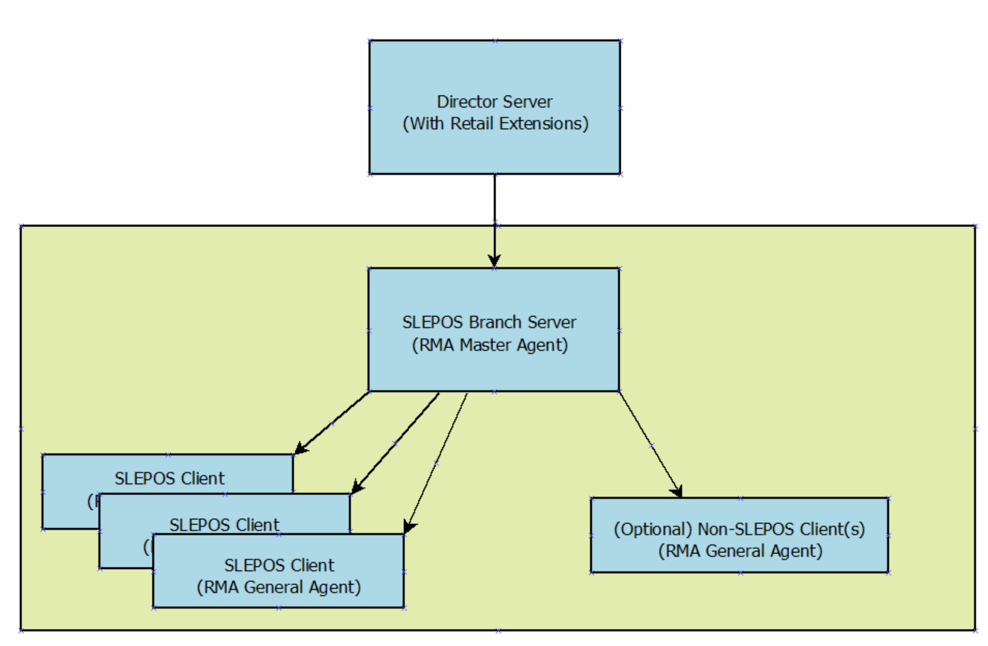
Setting up RMA on SLEPOS 11 SP1

Either the RMA Master Agent or RMA General Agent can be installed on SuSE Linux Enterprise Point Of Service (SLEPOS) 11 SP1. The RMA Master Agent will be required on a single system within the store environment. All of the other systems within the store should run the RMA General Agent.

Overview of RMA on SLEPOS 11 SP1

In an SLEPOS environment, RMA runs on both the SLEPOS branch server and the SLEPOS clients. On the branch server, RMA would typically run as a master agent. On the SLEPOS client RMA runs as a general agent. It’s possible to have a “mixed” environment where additional GA’s (running any supported OS) are also managed by the master agent on the SLEPOS branch server, or where the branch server runs a General Agent that is supported by an additional Master Agent within the store.

A typical SLEPOS store configuration is shown below:



As shown in the diagram above, the typical configuration consists of the following:

- IBM Director Server, at the enterprise (Windows or Linux)
- SLEPOS branch server, in the store, running the RMA master agent
- SLEPOS clients, in the store, running the RMA general agent
- Optionally, additional POS terminals in the store, running the RMA general agent on any supported OS (Windows, etc.)

Installing the RMA Agent on a SLEPOS Branch Server

To install an RMA Agent on a SLEPOS Branch Server, follow the setup and configuration steps described in the “Setting up RMA on SLED / SLES 11 SP1” section. As far as RMA is concerned, the SLEPOS Branch Server is the same as a standalone SLED or SLES server running in a store environment.

Installing the RMA Agent on a SLEPOS Terminal

Installing RMA on a SLEPOS Terminal means that the terminal image will need to be built with the required agent RPM’s and configuration included.

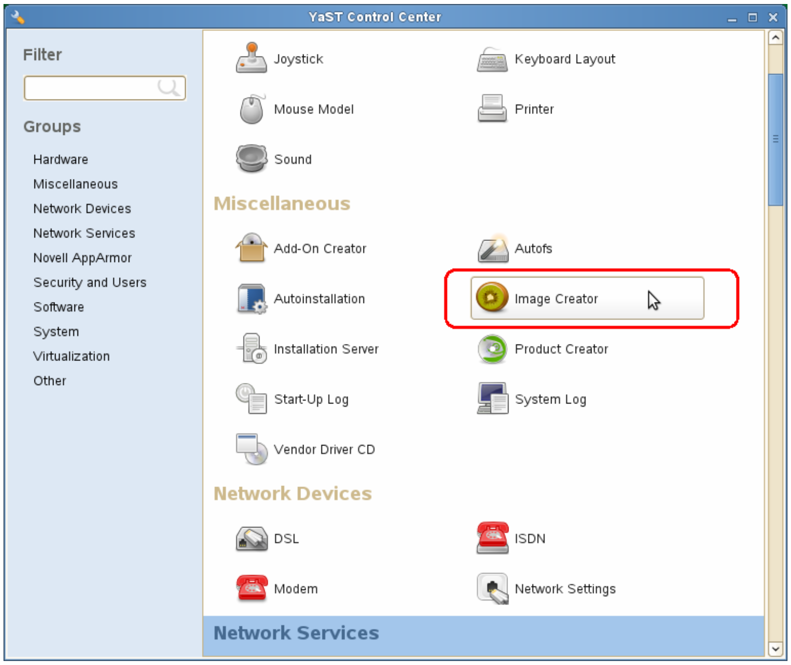
The steps in this document will assume that you have already followed the procedure in the "SLEPOS 11 Quick Installation Guide" to create the "first_image" described there: http://www-01.ibm.com/support/docview.wss?rs=220&uid=pos1R1004407

Prior to creating the image, you must have the RMA installation RPM's saved to a directory on the SLEPOS Image Server.

Creating a SLEPOS terminal image with RMA included

The following steps explain how to create and deploy a SLEPOS image with the RMA General Agent included:

1. Launch the Image Creator on your Admin / Image Server from YaST:



2. Click "Add" to create a new image

3. Specify a name for the image under "Kiwi configuration". Select "Base on Existing Configuration" and specify the path to the "first_image" that was created in the SLEPOS 11 Quick Installation Guide: http://www-01.ibm.com/support/docview.wss?rs=220&uid=pos1R1004407

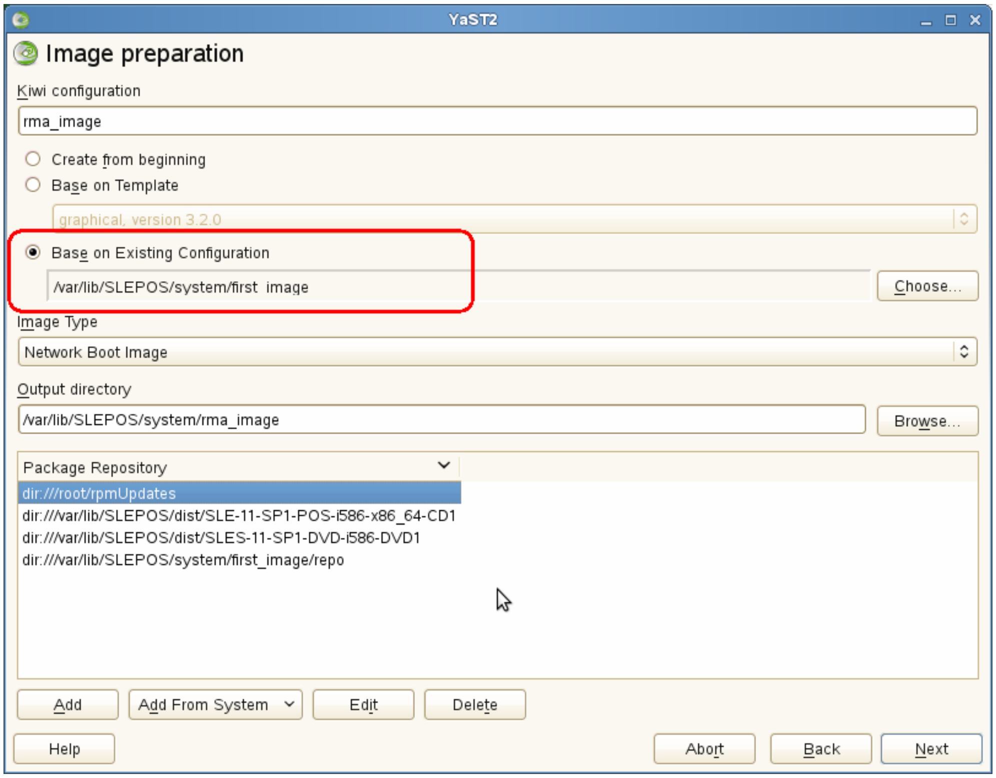


Image preparation

Kiwi configuration: rma_image

○ Create from beginning

○ Base on Template: graphical, version 3.2.0

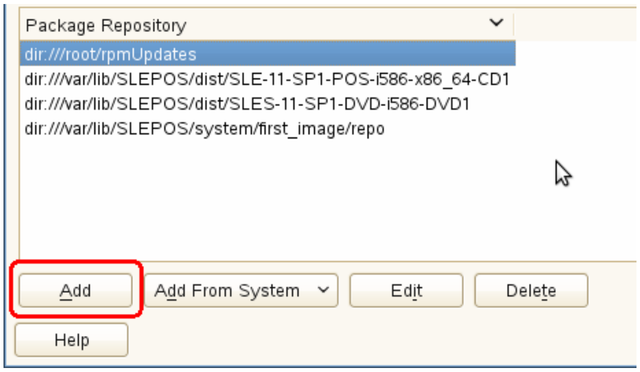
● Base on Existing Configuration: /var/lib/SLEPOS/system/first_image

Image Type: Network Boot Image

Output directory: /var/lib/SLEPOS/system/rma_image

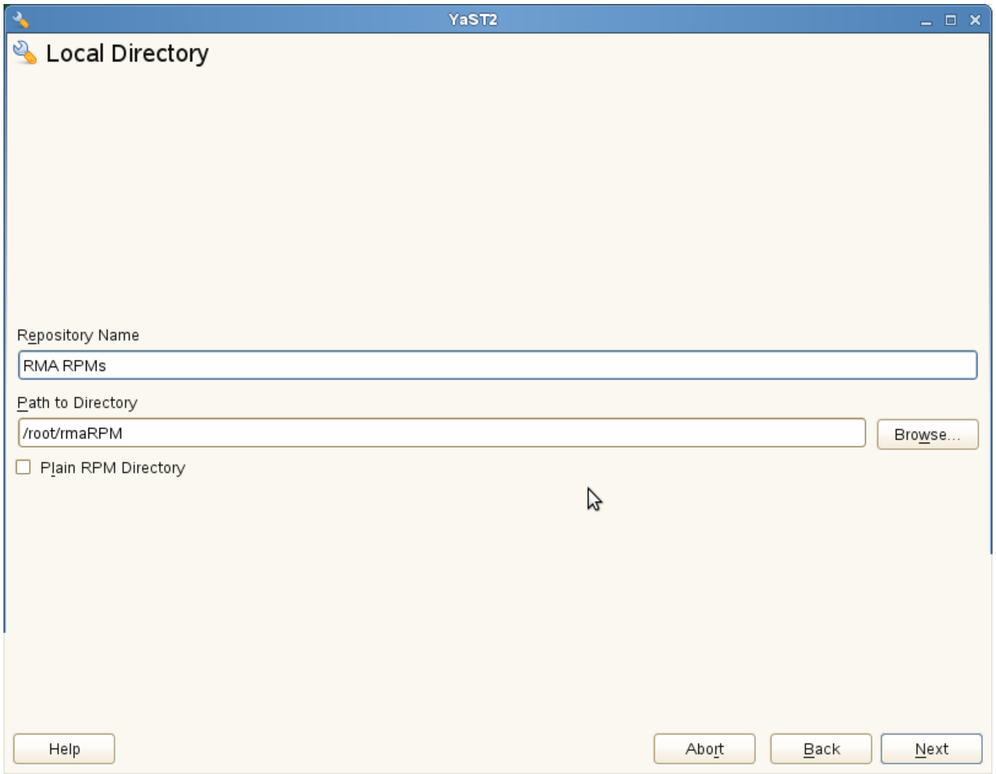
Package Repository
- dir:///root/rpmUpdates
- dir:///var/lib/SLEPOS/dist/SLE-11-SP1-POS-i586-x86_64-CD1
- dir:///var/lib/SLEPOS/dist/SLES-11-SP1-DVD-i586-DVD1
- dir:///var/lib/SLEPOS/system/first_image/repo

4. Click the “Add” button at the bottom in order to add a repository for the RMA RPM’s:



Package Repository
- dir:///root/rpmUpdates
- dir:///var/lib/SLEPOS/dist/SLE-11-SP1-POS-i586-x86_64-CD1
- dir:///var/lib/SLEPOS/dist/SLES-11-SP1-DVD-i586-DVD1
- dir:///var/lib/SLEPOS/system/first_image/repo

5. Select “Local Directory” and specify the path to where you have the RMA installation RPM’s saved on the system:



Repository Name

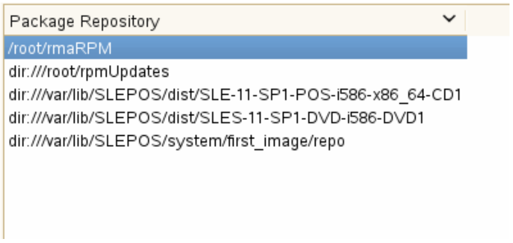
RMA RPMs

Path to Directory

/root/rmaRPM

☐ Plain RPM Directory

6. Click “Next” and verify that the repository is added successfully to the Package Repository list:


Package Repository

/root/rmaRPM
dir:///root/rpmUpdates
dir:///var/lib/SLEPOS/dist/SLE-11-SP1-POS-i586-x86_64-CD1
dir:///var/lib/SLEPOS/dist/SLES-11-SP1-DVD-i586-DVD1
dir:///var/lib/SLEPOS/system/first_image/repo

7. Click “Next” to proceed to the Image Configuration screen.

8. Clear any packages listed in the “Packages to Delete” section and then click the “Change” button to add additional packages to the image:

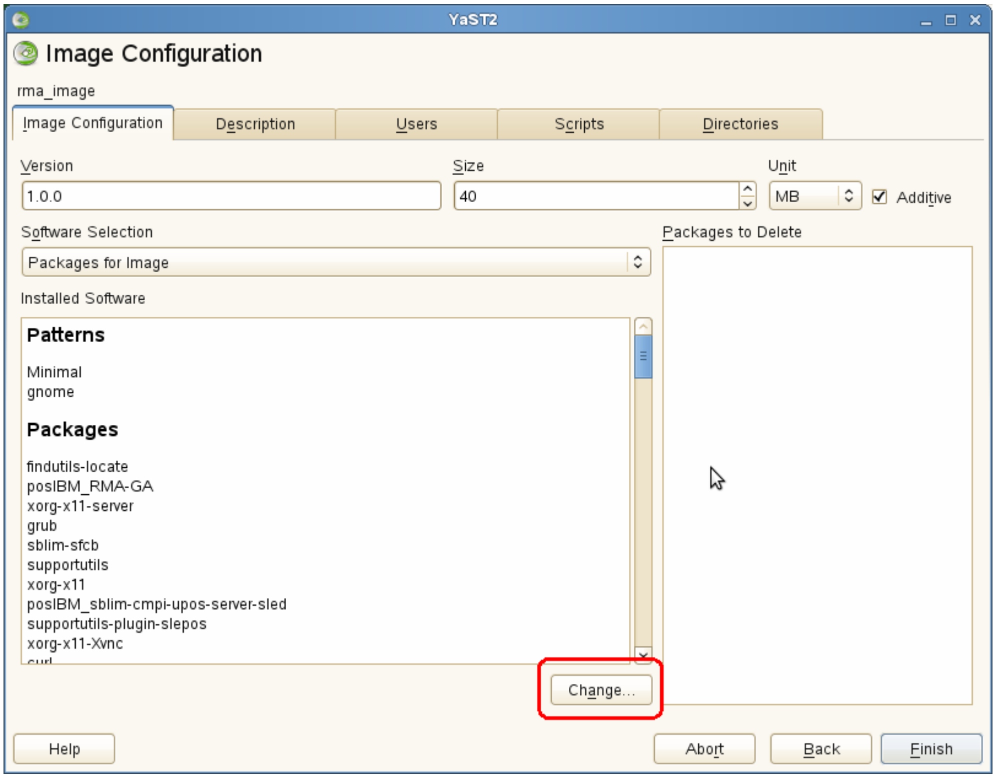


Image Configuration

rma_image

Version: 1.0.0

Size: 40

Unit: MB

☑ Additive

Software Selection: Packages for Image

Installed Software

Patterns

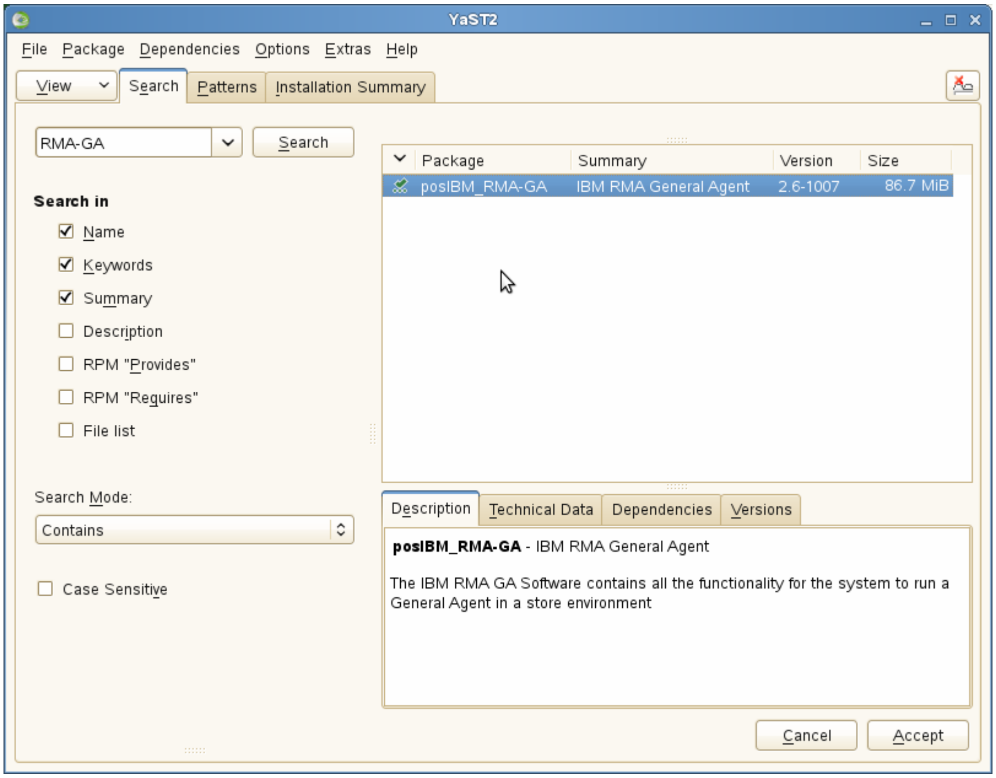
Minimal
gnome

Packages

findutils-locate
posIBM_RMA-GA
xorg-x11-server
grub
sblim-sfcb
supportutils
xorg-x11
posIBM_sblim-cmpi-upos-server-sled
supportutils-plugin-slepos
xorg-x11-Xvnc
curl

Packages to Delete

9. Inside the package browser, search for the RMA rpm and check the box to include it in the image:



RMA-GA

Search in

☑ Name
☑ Keywords
☑ Summary
☐ Description
☐ RPM "Provides"
☐ RPM "Requires"
☐ File list

Search Mode: Contains

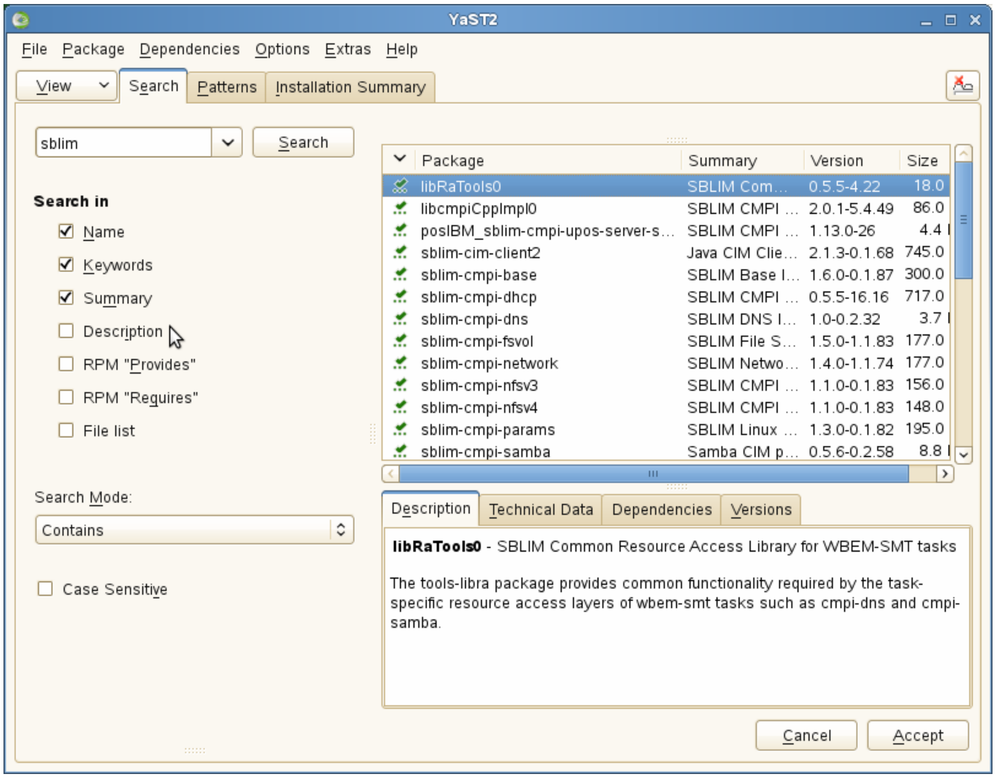
☐ Case Sensitive

	Package	Summary	Version	Size
	posIBM_RMA-GA	IBM RMA General Agent	2.6-1007	86.7 MiB

posIBM_RMA-GA - IBM RMA General Agent

The IBM RMA GA Software contains all the functionality for the system to run a General Agent in a store environment

10. Additionally, search for and include all of the sfcb and sblim rpm’s that are specified in the “Setting up RMA on SLED / SLES 11 SP1” section:



sblim

☑ Name
☑ Keywords
☑ Summary
☐ Description
☐ RPM "Provides"
☐ RPM "Requires"
☐ File list

Search Mode: Contains

☐ Case Sensitive

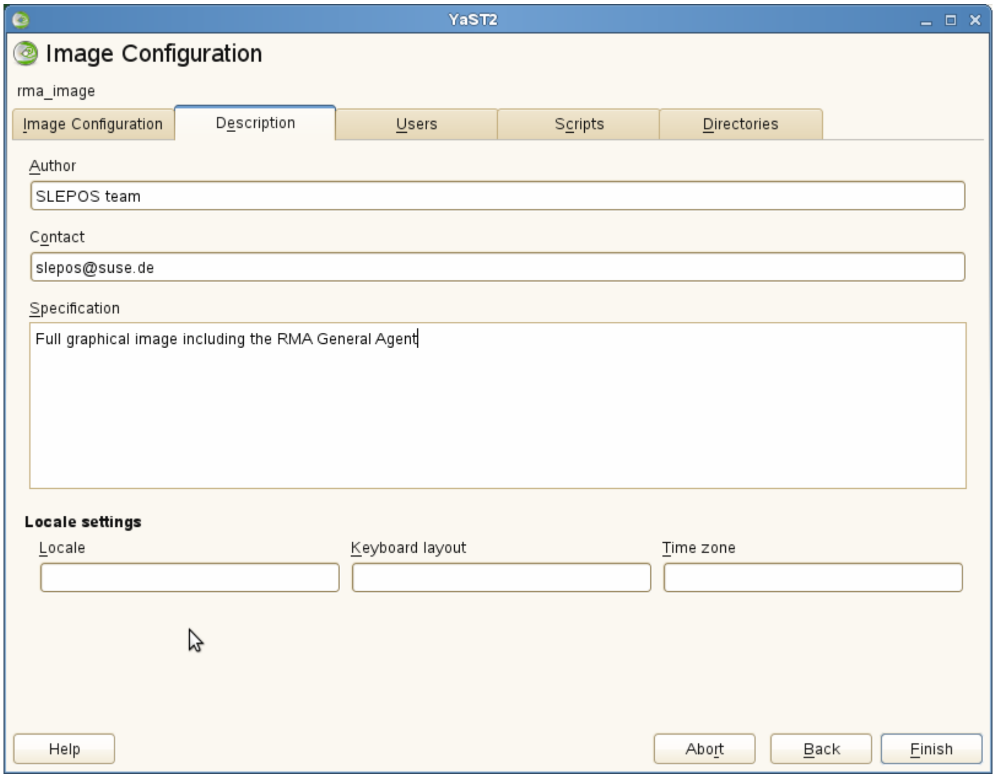
Package	Summary	Version	Size
libRaTools0	SBLIM Com...	0.5.5-4.22	18.0
libcmpiCppImpl0	SBLIM CMPI ...	2.0.1-5.4.49	86.0
posIBM_sblim-cmpi-upos-server-s...	SBLIM CMPI ...	1.13.0-26	4.4
sblim-cim-client2	Java CIM Clie...	2.1.3-0.1.68	745.0
sblim-cmpi-base	SBLIM Base I...	1.6.0-0.1.87	300.0
sblim-cmpi-dhcp	SBLIM CMPI ...	0.5.5-16.16	717.0
sblim-cmpi-dns	SBLIM DNS I...	1.0-0.2.32	3.7
sblim-cmpi-fsvol	SBLIM File S...	1.5.0-1.1.83	177.0
sblim-cmpi-network	SBLIM Netwo...	1.4.0-1.1.74	177.0
sblim-cmpi-nfsv3	SBLIM CMPI ...	1.1.0-0.1.83	156.0
sblim-cmpi-nfsv4	SBLIM CMPI ...	1.1.0-0.1.83	148.0
sblim-cmpi-params	SBLIM Linux ...	1.3.0-0.1.82	195.0
sblim-cmpi-samba	Samba CIM p...	0.5.6-0.2.58	8.8

libRaTools0 - SBLIM Common Resource Access Library for WBEM-SMT tasks

The tools-libra package provides common functionality required by the task-specific resource access layers of wbem-smt tasks such as cmpi-dns and cmpi-samba.

11. When finished, click “Accept” to add the packages to the image. Accept any dependencies that also need to be installed.

12. Click on the “Description” tab and add a meaningful description for your image:



Author: SLEPOS team

Contact: slepos@suse.de

Specification: Full graphical image including the RMA General Agent

Locale:

Keyboard layout:

Time zone:

13. Click on the Scripts tab. In the “Cleanup Script”, you will need to specify commands to configure / start the RMA Agent and SFCB. Enter the following immediately after the #!/bin/bash line. Note that the path to the RMA installation for the rma-config script may change pending on the level you are installing:

```
# Commands for the RMA General Agent
/opt/ibm/StoreIntegrator/RMA2611007/rma-config –n
chkconfig sfcb 235
/etc/init.d/sfcb start
/etc/init.d/rmsvc-ga start
```

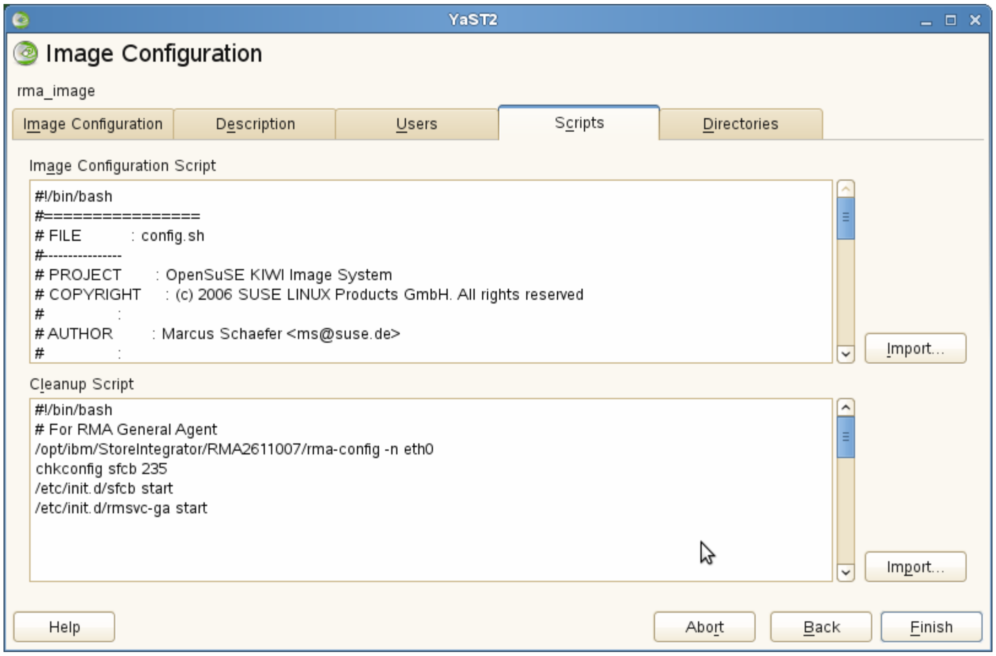


Image Configuration Script

```
#!/bin/bash
#================
# FILE          : config.sh
#----------------
# PROJECT       : OpenSuSE KIWI Image System
# COPYRIGHT     : (c) 2006 SUSE LINUX Products GmbH. All rights reserved
#               :
# AUTHOR        : Marcus Schaefer <ms@suse.de>
#               :
```

Cleanup Script

```
#!/bin/bash
# For RMA General Agent
/opt/ibm/StoreIntegrator/RMA2611007/rma-config -n eth0
chkconfig sfcb 235
/etc/init.d/sfcb start
/etc/init.d/rmsvc-ga start
```

14. Click “Finish” to create the Image. Verify that the image creation finishes with a message stating “Image creation succeeded”. Then click “OK”.

Note: If you have SFCB running on your image server system, you may need to stop SFCB manually prior to creating the image (/etc/init.d/sfcb stop) as it can cause conflicts during the creation.

Preparing the server to boot the POS Terminal

The following steps explain how to prepare the SLEPOS Admin and Branch Servers in order to boot a POS Terminal with the RMA Image.

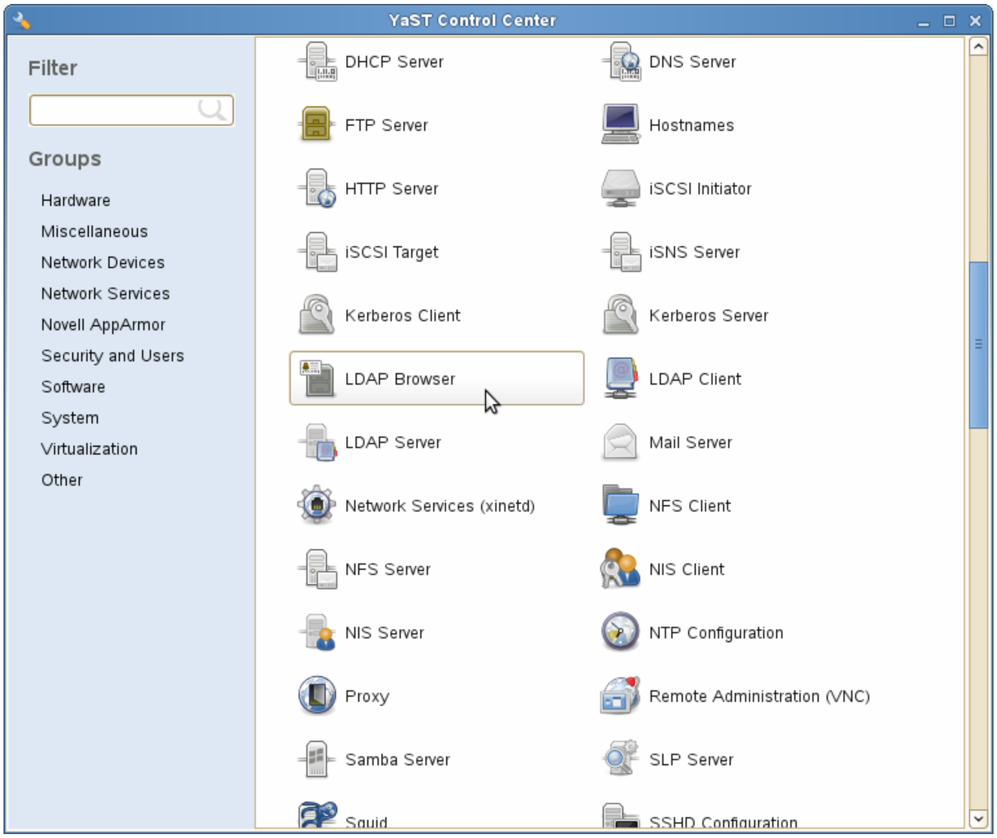
1. Use the registerImages command to copy the boot and system images:

   registerImages --gzip --no-hardlinks --ldap --kernel /var/lib/SLEPOS/system/images/<image_name_directory>/initrd-netboot-SLEPOS11.i686-3.2.0.kernel --initrd /var/lib/SLEPOS/system/images/<image_name_directory>/initrd-netboot-SLEPOS11.i686-3.2.0.gz /var/lib/SLEPOS/system/images/<image_name_directory>/<image_name>.i686-<image_version>

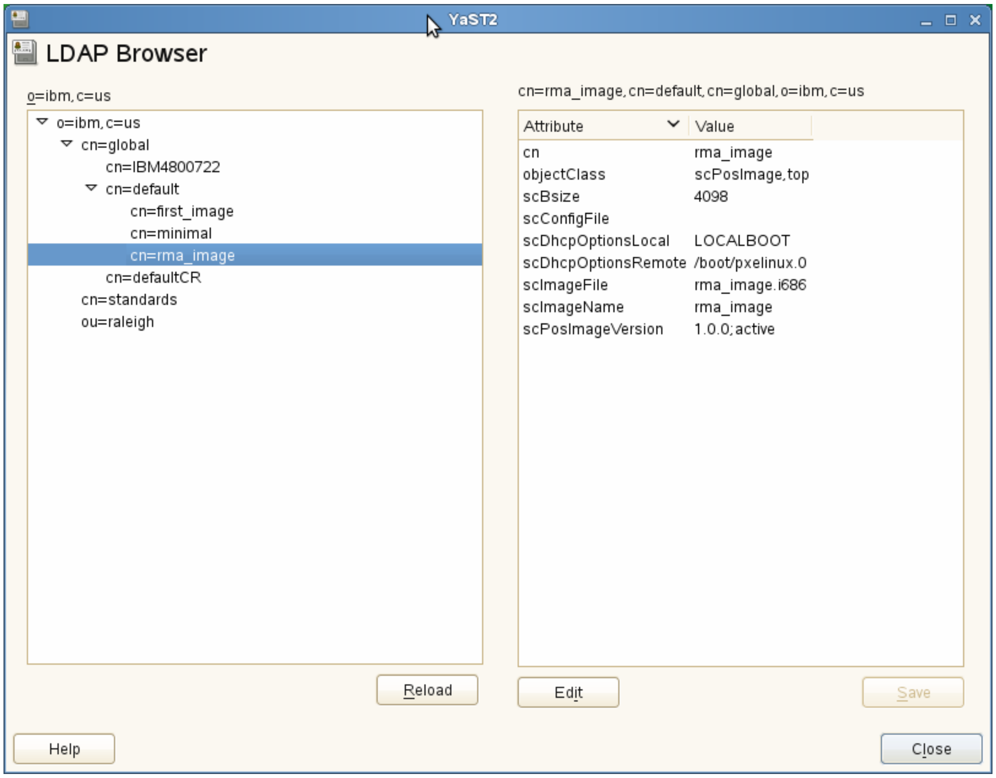
2. Use the posAdmin.pl command to register the new RMA image with LDAP:

```
posAdmin.pl --user cn=admin,o=ibm,c=us --password password --base
cn=default,cn=global,o=ibm,c=us --add --scPosImage --cn rma_image --
scImageName rma_image --scPosImageVersion "1.0.0;active" --
scDhcpOptionsRemote /boot/pxelinux.0 --scDhcpOptionsLocal LOCALBOOT --
scImageFile rma_image.i686 --scBsize 8192
```

3. Launch the LDAP Browser from YaST:



4. Verify that your new image is visible



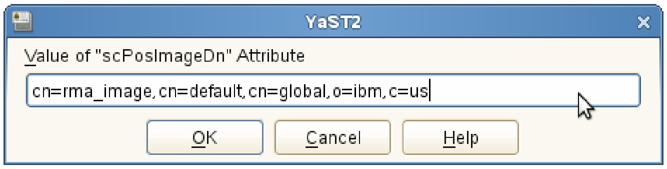
o=ibm,c=us

```
o=ibm,c=us
  cn=global
    cn=IBM4800722
    cn=default
      cn=first_image
      cn=minimal
      cn=rma_image
    cn=defaultCR
  cn=standards
  ou=raleigh
```

cn=rma_image,cn=default,cn=global,o=ibm,c=us

Attribute	Value
cn	rma_image
objectClass	scPosImage,top
scBsize	4098
scConfigFile	
scDhcpOptionsLocal	LOCALBOOT
scDhcpOptionsRemote	/boot/pxelinux.0
scImageFile	rma_image.i686
scImageName	rma_image
scPosImageVersion	1.0.0;active

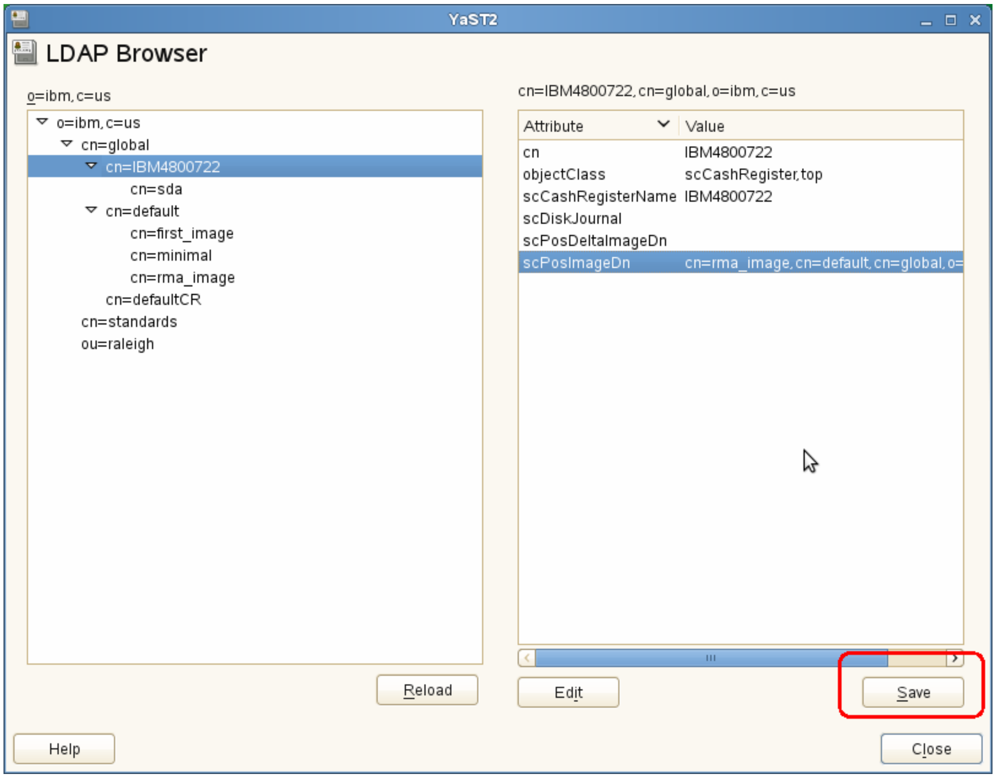
5. Double click on the scPosImageDn attribute of the POS terminal that you want to load the image (example: cn=IBM4800722,cn=global,o=ibm,c=us) to edit it, and set it to load the newly created rma_image.



Value of "scPosImageDn" Attribute

cn=rma_image,cn=default,cn=global,o=ibm,c=us

6. The change will be reflected after you click OK, but you **must** click Save in order for the change to be saved in LDAP:



Attribute	Value
cn	IBM4800722
objectClass	scCashRegister,top
scCashRegisterName	IBM4800722
scDiskJournal	
scPosDeltaImageDn	
scPosImageDn	cn=rma_image,cn=default,cn=global,o=

7. The last thing that is needed is to add the proper sfcb configuration to the terminal boot properties. Set up the SFCB configuration file as specified in the “Setting up RMA on SLED / SLES 11 SP1” section:

   a. Edit **/etc/sfcb/sfcb.cfg**
   b. Set **enableHttp** to **true**
   c. Set **doBasicAuth** to **false**
   d. Set **provProcs** to **40**

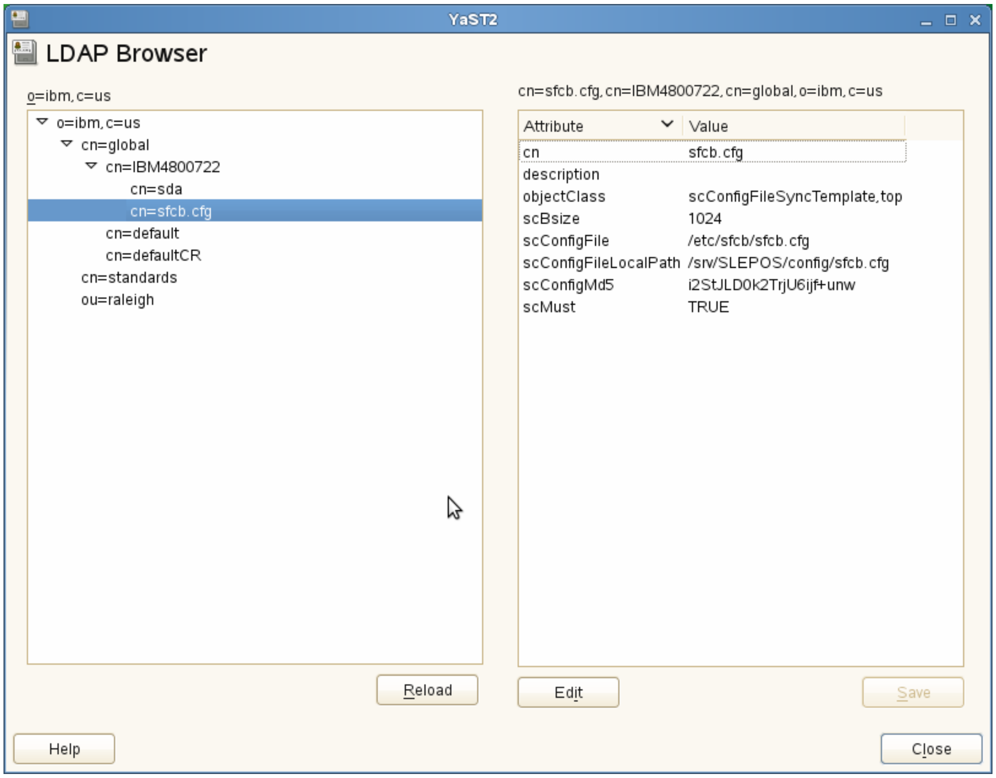
8. Copy the sfcb.cfg to the /srv/SLEPOS/config directory.

9. Add the sfcb.cfg file to the LDAP tree by using the posAdmin.pl command to add an scConfigFileSyncTemplate object to the terminal definition that you want.

   posAdmin.pl --user cn=admin,o=ibm,c=us --password password --base cn=IBM4800743,cn=global,o=ibm,c=us --add --scConfigFileSyncTemplate --cn sfcb.cfg --scConfigFile /etc/sfcb/sfcb.cfg --scMust TRUE --scBsize 1024 --scConfigFileLocalPath /srv/SLEPOS/config/sfcb.cfg

Note: The sfcb.cfg file stored in the LDAP in this scConfigFileSyncTemplate object will only be loaded onto terminals at the time of first boot. Subsequent boots will not receive this file. Therefore, please remember that re-imaging is necessary to push down new configuration files.

10. Return to the LDAP browser and verify that you can see the sfcb.cfg attached to the terminal:



cn=sfcb.cfg,cn=IBM4800722,cn=global,o=ibm,c=us

Attribute	Value
cn	sfcb.cfg
description	
objectClass	scConfigFileSyncTemplate,top
scBsize	1024
scConfigFile	/etc/sfcb/sfcb.cfg
scConfigFileLocalPath	/srv/SLEPOS/config/sfcb.cfg
scConfigMd5	i2StJLD0k2TrjU6ijf+unw
scMust	TRUE

11. Run the possyncimages command to synchronize the new image between the branch and admin servers.

12. Run "posldap2crconfig --dumpall" to update the terminals configurations.

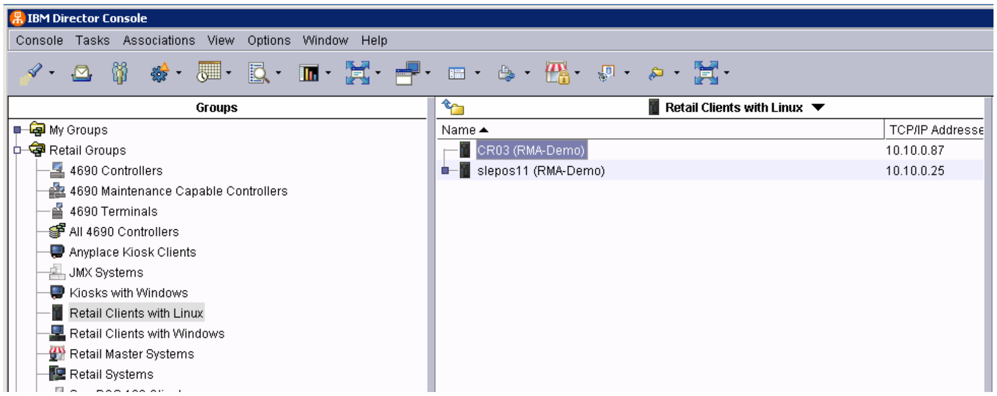
13. Check to make sure that both leases2ldap and image2ldap services are running by executing the "/etc/init.d/posleases2ldap status" command.

14. Boot the POS Terminal and ensure the new rma_image loads successfully.

Verifying the SLEPOS Terminal Image with RMA

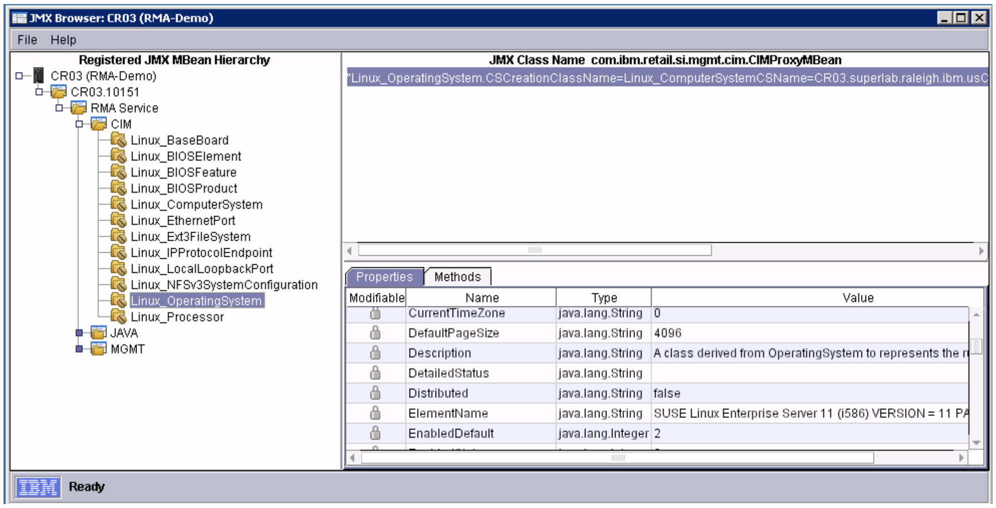
After the terminal boots, the RMA service should already be running. At this point, you should be able to discover the terminal on the IBM Director Console the same as you would any other general agent.

RMA General Agents running on SLEPOS 11 will be listed under the "Retail Clients with Linux" group:



Name ▲	TCP/IP Addresse
CR03 (RMA-Demo)	10.10.0.87
slepos11 (RMA-Demo)	10.10.0.25

Using the JMX Browser, you can verify that SFCB is running successfully by ensuring there are several "Linux" MBeans listed under CIM.

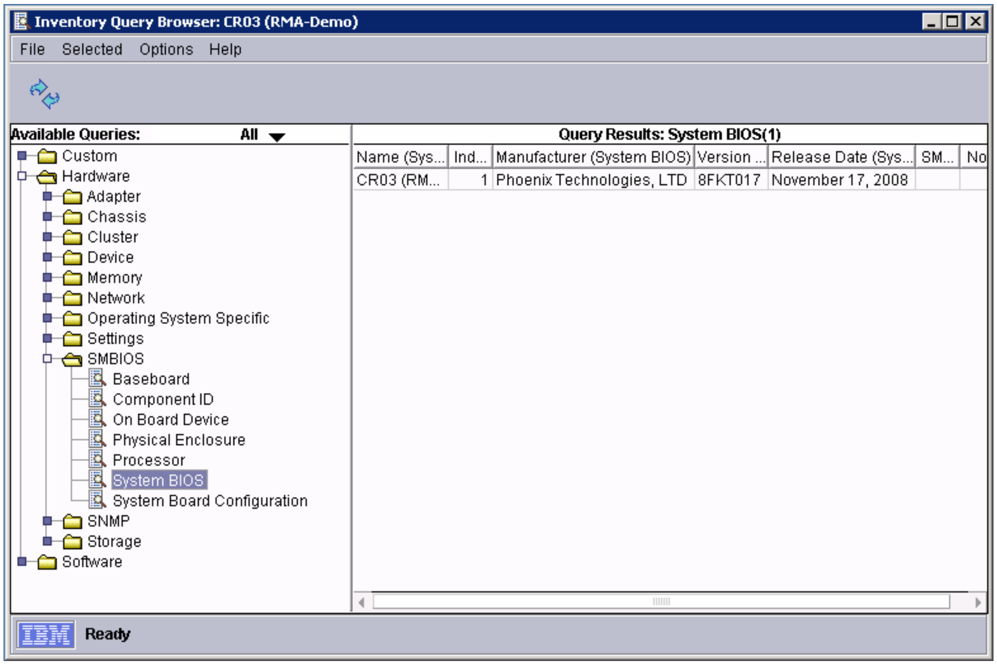


JMX Class Name com.ibm.retail.si.mgmt.cim.CIMProxyMBean

"Linux_OperatingSystem.CSCreationClassName=Linux_ComputerSystemCSName=CR03.superlab.raleigh.ibm.usC

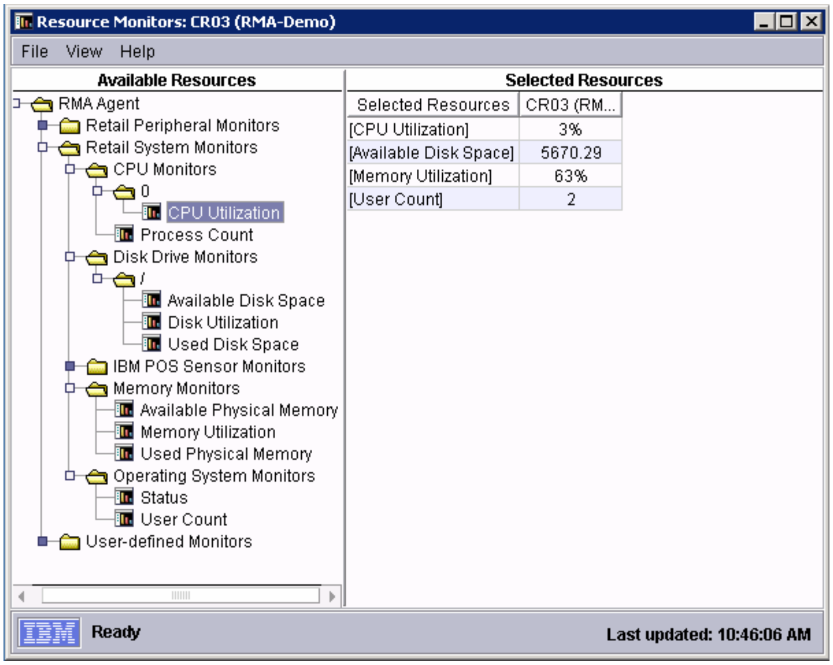
Modifiable	Name	Type	Value
🔒	CurrentTimeZone	java.lang.String	0
🔒	DefaultPageSize	java.lang.String	4096
🔒	Description	java.lang.String	A class derived from OperatingSystem to represents the r
🔒	DetailedStatus	java.lang.String	
🔒	Distributed	java.lang.String	false
🔒	ElementName	java.lang.String	SUSE Linux Enterprise Server 11 (i586) VERSION = 11 PA
🔒	EnabledDefault	java.lang.Integer	2

At that point, you can collect and view Inventory on the system, set up monitors, and use it as you would any other RMA Agent.



Query Results: System BIOS(1)

Name (Sys...	Ind...	Manufacturer (System BIOS)	Version ...	Release Date (Sys...	SM...	No
CR03 (RM...	1	Phoenix Technologies, LTD	8FKT017	November 17, 2008		



Selected Resources

Selected Resources	CR03 (RM...
[CPU Utilization]	3%
[Available Disk Space]	5670.29
[Memory Utilization]	63%
[User Count]	2

Last updated: 10:46:06 AM

Chapter 4 – Setting Up RMA on IRES

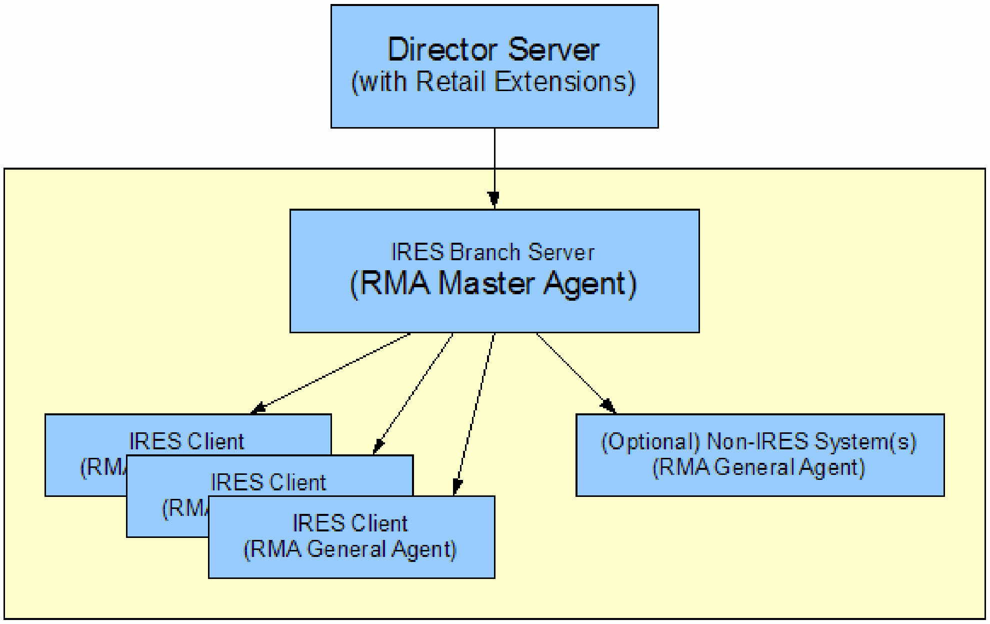
This chapter describes how to setup RMA on IRES 2.1.5, and how to verify the installation. It also describes how to verify that the retail peripherals (using JavaPOS) are working properly with RMA on the IRES client.

> **Note**: This chapter assumes that the reader is already familiar with how to install and configure IRES build servers, branch servers, and clients. It also assumes the reader already understands basic usage of RMA and IBM Director, including how to discover the master agent using IBM Director. (If not, please refer to the other chapters of this cookbook, particularly "**Chapter 1 – Quick-Install Guide**".)

Overview of RMA on IRES

In an IRES environment, RMA runs on both the IRES branch server and the IRES clients. On the branch server, RMA runs as a master agent. On the IRES client, RMA runs as a general agent. It's possible to have a "mixed" environment where additional GA's (running any supported OS) are also managed by the master agent on the IRES branch server.

A typical IRES store configuration is shown below:



As shown in the diagram above, the typical configuration consists of the following:

- IBM Director Server, at the enterprise (Windows or Linux)
- IRES branch server, in the store, running the RMA master agent

- IRES clients, in the store, running the RMA general agent
- Optionally, additional POS terminals in the store, running the RMA general agent on any supported OS (Windows, etc.)

Supported Versions / Configurations

IRES 2.1.5 includes RMA version 2.3 by default, but it can be upgraded to RMA version 2.4. IBM does not support upgrading RMA to higher versions beyond RMA 2.4 on IRES, so the RMA version should remain at 2.3 or 2.4 in production environments (for the RMA master agent and general agents). The Director Server, however, can be installed with higher versions, including the latest level of RMA retail extensions for Director.

The JavaPOS version included with IRES 2.1.5 is JavaPOS version 1.9.5. While it's possible for retailers to upgrade to 1.9.6b or higher, the instructions below assume that version 1.9.5 will be used with IRES. Contact IBM support or techline for information about upgrading the JavaPOS version on IRES.

Setup Instructions for RMA on IRES 2.1.5

Follow the instructions below to setup RMA on IRES 2.1.5:

1. Follow the instructions in the IRES developer's guide to install the build server and branch server.

> **Note**: During the installation process for the build server, be sure to follow the instructions carefully related to OpenSSL, as this package is important for the pegasus server on the IRES client.
>
> ***Hint**:* The following steps could later be used on the client to verify that the above step was done correctly.
>
> On the client, run the following command:
>
> ```
> /etc/init.d/tog-pegasus status
> ```
>
> This should show a series of numbers and a status of "running". If this command shows a status of "not running", attempt to start the pegasus service with the following command:
>
> ```
> /etc/init.d/tog-pegasus start
> ```
>
> If this command fails with an error about missing ".pem" files, then the OpenSSL instructions were not followed correctly.

2. Ensure that RMA is running on the branch server by using the following command:

```
/etc/init.d/rmsvc-ma status
```

3. Obtain the XML4C rpm file, as this is missing from IRES 2.1.5, and it's required for the IRES client to run RMA with pegasus.

   The XML4C rpm is available as part of the JavaPOS package.

   JavaPOS can be downloaded here:
   http://www2.clearlake.ibm.com/store/support/html/driverss.html

   Use the following selections when you download JavaPOS:
   - OS: IRES/Linux
   - System: your choice
   - API: JavaPOS

   For JavaPOS 1.9.5, the package name is "jposires215.zip". To extract the necessary rpm, unzip the file which will produce a ".tar" file in the "./jposires215" directory. Included in this directory will be a tar file. Extract the contents of the tar file with:

```
tar xvf ibm-javapos-1.9.5-17jre-for-ires2.tar
```

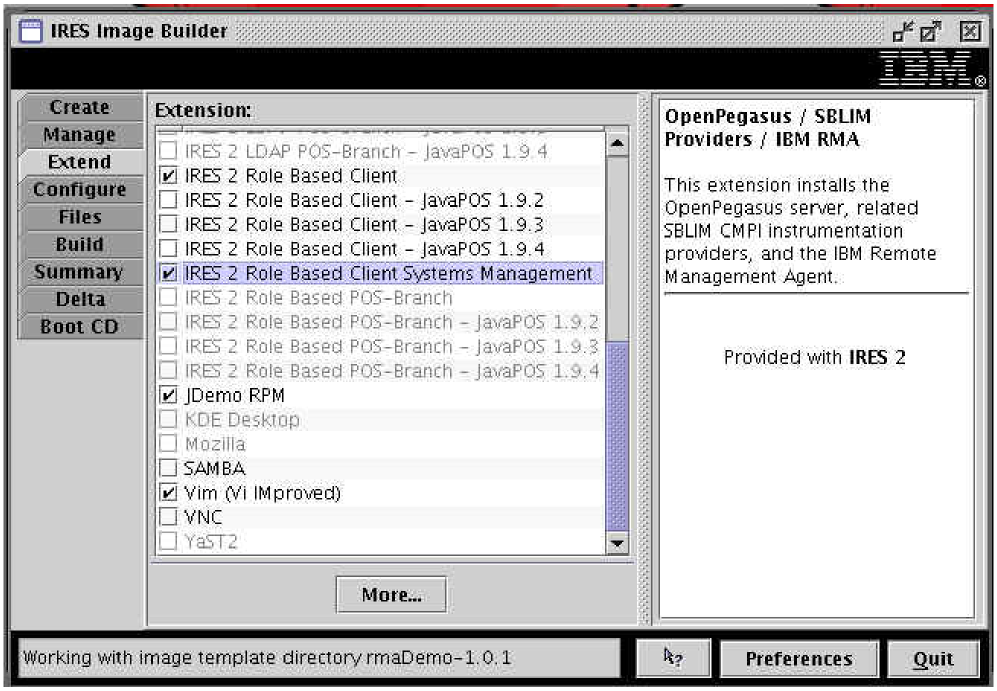
   Then copy the XML4C rpm (on the build server) as follows:

```
cp posIBM_XML4C-5.4.6-1.i586.rpm /opt/ibm/ires/rpms
```

   The XML4C rpm can now be selected in the IRES Image Building GUI.

4. Open the IRES image builder tool and build the client image. The screenshots below illustrate the selections that are needed for RMA to work properly on the client image:

   Select "IRES 2 Role Based Client Systems Management":



Extension:

- □ IRES 2 LDAP POS-Branch – JavaPOS 1.9.4
- ☑ IRES 2 Role Based Client
- □ IRES 2 Role Based Client – JavaPOS 1.9.2
- □ IRES 2 Role Based Client – JavaPOS 1.9.3
- □ IRES 2 Role Based Client – JavaPOS 1.9.4
- ☑ IRES 2 Role Based Client Systems Management
- □ IRES 2 Role Based POS-Branch
- □ IRES 2 Role Based POS-Branch – JavaPOS 1.9.2
- □ IRES 2 Role Based POS-Branch – JavaPOS 1.9.3
- □ IRES 2 Role Based POS-Branch – JavaPOS 1.9.4
- ☑ JDemo RPM
- □ KDE Desktop
- □ Mozilla
- □ SAMBA
- ☑ Vim (Vi IMproved)
- □ VNC
- □ YaST2

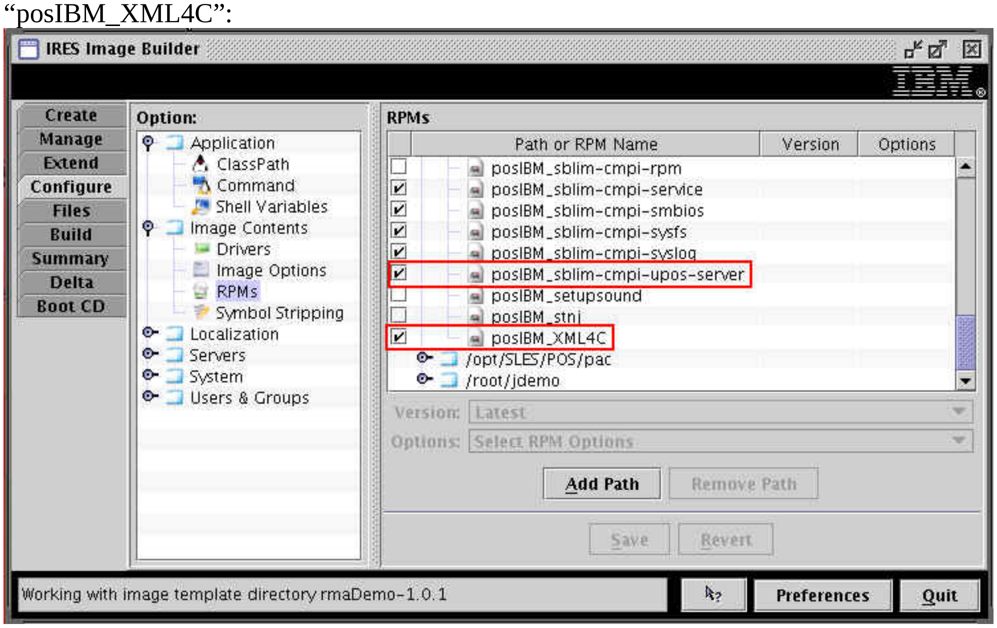
OpenPegasus / SBLIM Providers / IBM RMA

This extension installs the OpenPegasus server, related SBLIM CMPI instrumentation providers, and the IBM Remote Management Agent.

Provided with **IRES 2**

Working with image template directory rmaDemo-1.0.1

You must manually select “posIBM_sblim-cmpi-upos-server” and “posIBM_XML4C”:



RPMs

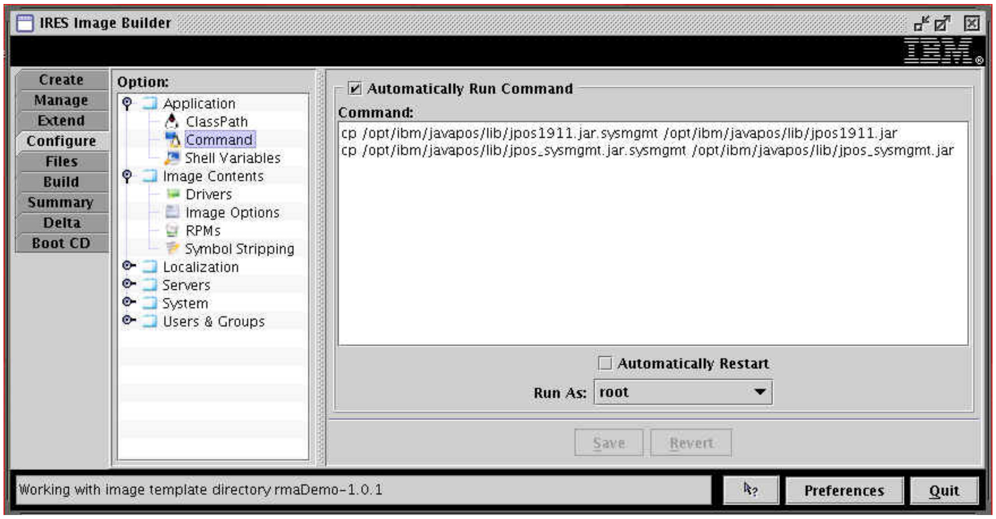
	Path or RPM Name	Version	Options
□	posIBM_sblim-cmpi-rpm		
☑	posIBM_sblim-cmpi-service		
☑	posIBM_sblim-cmpi-smbios		
☑	posIBM_sblim-cmpi-sysfs		
☑	posIBM_sblim-cmpi-syslog		
☑	posIBM_sblim-cmpi-upos-server		
□	posIBM_setupsound		
□	posIBM_stnj		
☑	posIBM_XML4C		
	/opt/SLES/POS/pac		
	/root/jdemo		

Version: Latest

Options: Select RPM Options

Working with image template directory rmaDemo-1.0.1

You must manually type the commands illustrated below:



☑ Automatically Run Command

Command:

```
cp /opt/ibm/javapos/lib/jpos1911.jar.sysmgmt /opt/ibm/javapos/lib/jpos1911.jar
cp /opt/ibm/javapos/lib/jpos_sysmgmt.jar.sysmgmt /opt/ibm/javapos/lib/jpos_sysmgmt.jar
```

□ Automatically Restart

Run As: root

Working with image template directory rmaDemo-1.0.1

The exact commands (from the last screenshot) are:

```
   cp /opt/ibm/javapos/lib/jpos1911.jar.sysmgmt
/opt/ibm/javapos/lib/jpos1911.jar
```

```
   cp /opt/ibm/javapos/lib/jpos sysmgmt.jar.sysmgmt
/opt/ibm/javapos/lib/jpos_sysmgmt.jar
```

Note: If the two “cp” commands above are omitted or typed incorrectly, you can always run them manually on the client system after you have loaded the client. However, if you type them manually, you MUST reboot the system after running these two commands!

5. Load the client image on a POS system using the normal client loading procedure. After the client image is loaded, you can verify the status of RMA and pegasus on the client by checking the following:

   a. Check to make sure that RMA is started:

```
   /etc/init.d/rmsvc-ga status
```

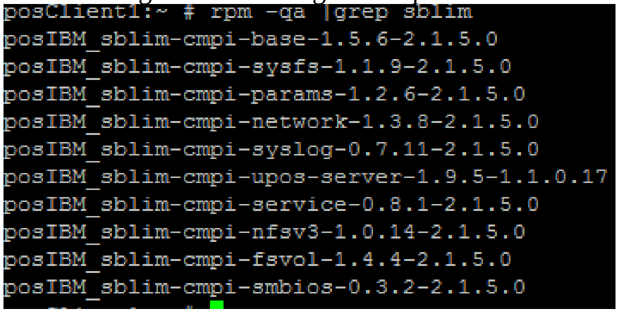
   b. Check to make sure pegasus is started:

```
   /etc/init.d/tog-pegasus status
```

6. You may issue the following command on the POS client to verify the necessary “sblim” rpm files are installed:

```
   rpm -qa | grep sblim
```

You should get the following list of rpm files:

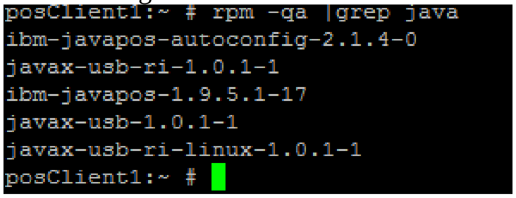


```
posClient1:~ # rpm -qa |grep sblim
posIBM_sblim-cmpi-base-1.5.6-2.1.5.0
posIBM_sblim-cmpi-sysfs-1.1.9-2.1.5.0
posIBM_sblim-cmpi-params-1.2.6-2.1.5.0
posIBM_sblim-cmpi-network-1.3.8-2.1.5.0
posIBM_sblim-cmpi-syslog-0.7.11-2.1.5.0
posIBM_sblim-cmpi-upos-server-1.9.5-1.1.0.17
posIBM_sblim-cmpi-service-0.8.1-2.1.5.0
posIBM_sblim-cmpi-nfsv3-1.0.14-2.1.5.0
posIBM_sblim-cmpi-fsvol-1.4.4-2.1.5.0
posIBM_sblim-cmpi-smbios-0.3.2-2.1.5.0
posClient1:~ #
```

7. You may issue the following command on the POS client to verify the level of UPOS/JavaPOS that is installed on the client:

```
rpm -qa | grep java
```

You should get a list similar to the below screen shot:

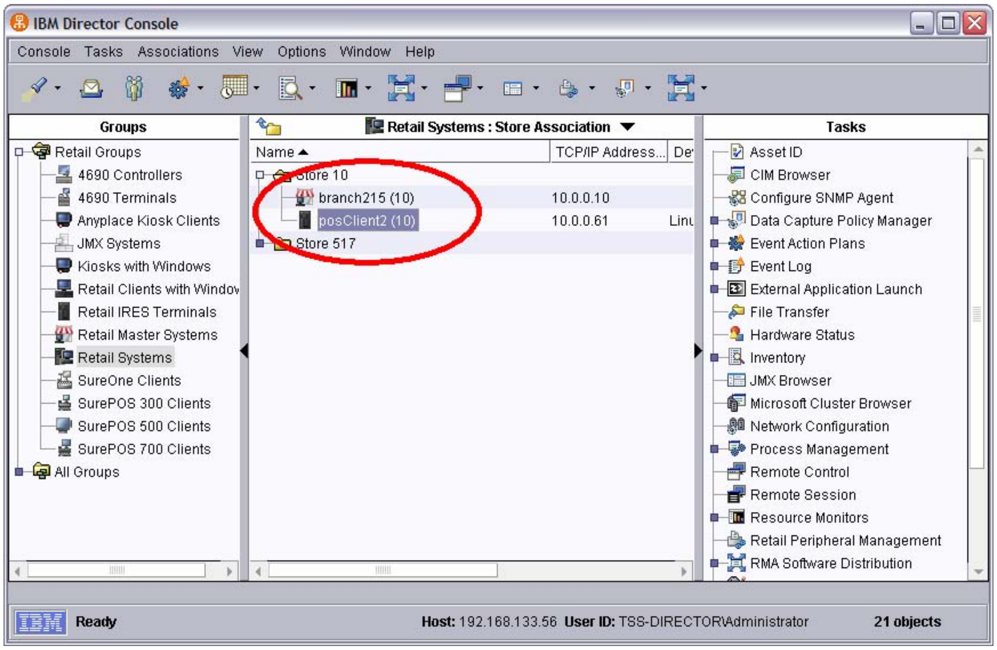


```
posClient1:~ # rpm -qa |grep java
ibm-javapos-autoconfig-2.1.4-0
javax-usb-ri-1.0.1-1
ibm-javapos-1.9.5.1-17
javax-usb-1.0.1-1
javax-usb-ri-linux-1.0.1-1
posClient1:~ #
```

In the example above, the JavaPOS version is the line “ibm-javapos-1.9.5.1-17” which is JavaPOS 1.9.5.

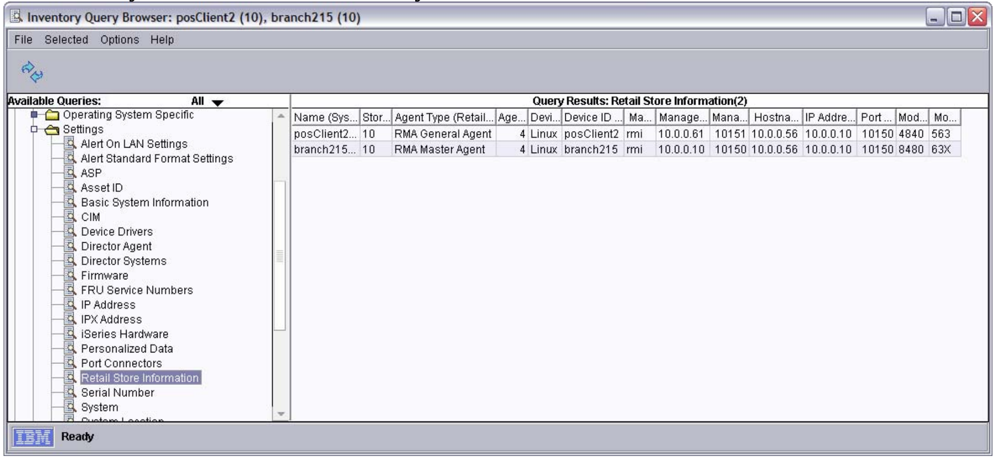
8. Use IBM Director to discover the MA and/or GA’s. After the discovery is complete, you can quickly verify the following:

    a. Check that the MA and/or GA is online in Director (icon should not be grayed out).



Host: 192.168.133.56 User ID: TSS-DIRECTOR\Administrator 21 objects

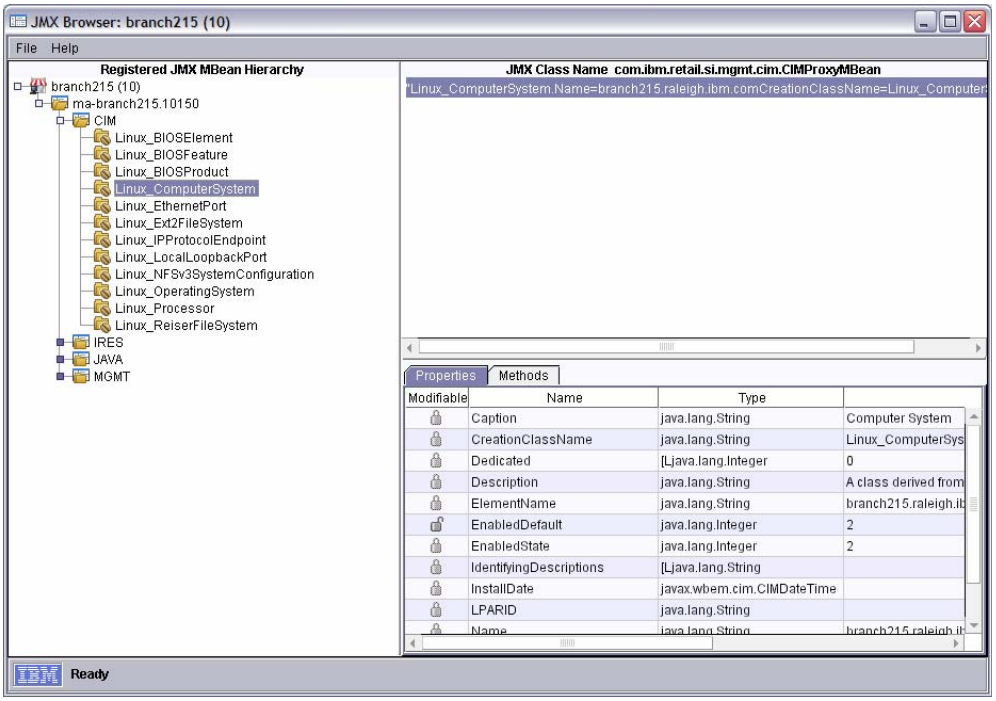
b. Check that you can view the inventory for the MA and/or GA’s.



Query Results: Retail Store Information(2)

Name (Sys...	Stor...	Agent Type (Retail...	Age...	Devi...	Device ID ...	Ma...	Manage...	Mana...	Hostna...	IP Addre...	Port ...	Mod...	Mo...
posClient2...	10	RMA General Agent	4	Linux	posClient2	rmi	10.0.0.61	10151	10.0.0.56	10.0.0.10	10150	4840	563
branch215...	10	RMA Master Agent	4	Linux	branch215	rmi	10.0.0.10	10150	10.0.0.56	10.0.0.10	10150	8480	63X

c. Check that you can get to the JMX Browser and browse the “Linux_” CIM classes, as shown in the diagram below:



JMX Class Name com.ibm.retail.si.mgmt.cim.CIMProxyMBean

"Linux_ComputerSystem.Name=branch215.raleigh.ibm.comCreationClassName=Linux_Computer

Modifiable	Name	Type	
🔒	Caption	java.lang.String	Computer System
🔒	CreationClassName	java.lang.String	Linux_ComputerSys
🔒	Dedicated	[Ljava.lang.Integer	0
🔒	Description	java.lang.String	A class derived from
🔒	ElementName	java.lang.String	branch215.raleigh.ib
🔓	EnabledDefault	java.lang.Integer	2
🔒	EnabledState	java.lang.Integer	2
🔒	IdentifyingDescriptions	[Ljava.lang.String	
🔒	InstallDate	javax.wbem.cim.CIMDateTime	
🔒	LPARID	java.lang.String	
🔒	Name	java.lang.String	branch215.raleigh.ib

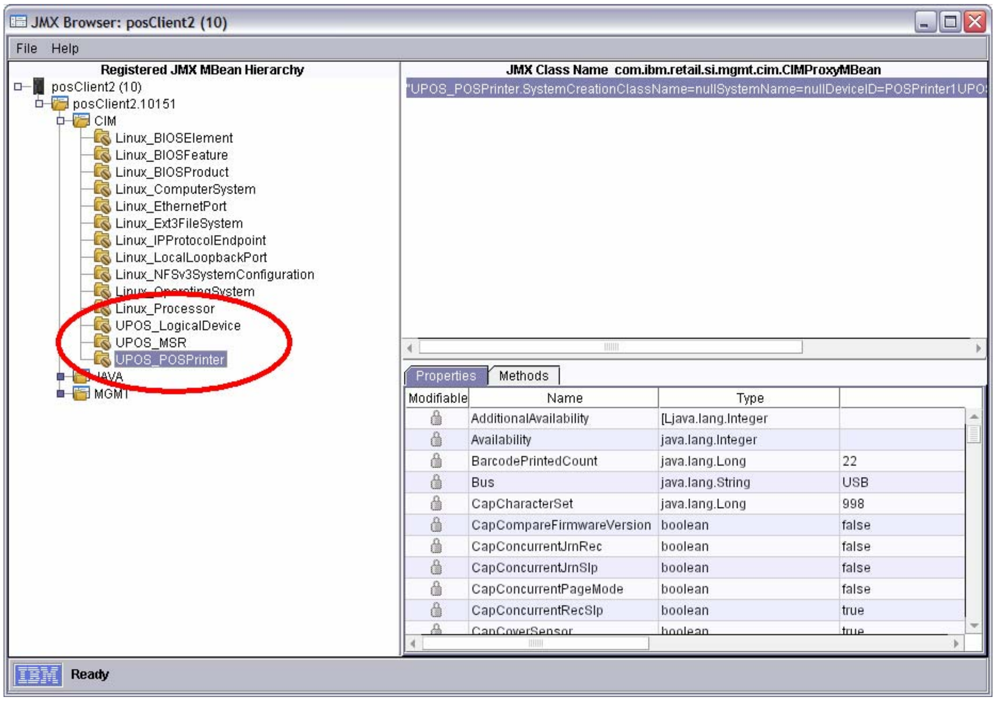
9. To verify retail peripherals:

   a. Use the test application of your choice to "open" a retail peripheral device. (Note: The device MUST be "open" for it to appear in RMA/Director!)

      Hint: One example is to issue the startx command to start an X session. Then use the Programs Menu pull down, select Accessories, then Terminal to start a terminal session. Issue the following command to start the POS Control Center:
      /opt/ibm/javapos/bin/POSControlCenter

      The POS Control Center utility allows you to select a device in the left side column (one with a green check mark) and then select the test device tab on the right panel. If you select the Keyboard device for example, then select the button to start test the test, the keyboard device will be opened, claimed, and enabled. This allows RMA to discover the device.

   b. It will take a few minutes for RMA to become aware of the new CIM classes in Pegasus. You can either wait a few minutes, or you can restart RMA GA to immediately expose the new CIM classes. After you have either waited a few minutes or you have restarted RMA GA, open the JMX Browser to view the peripheral classes, as shown below:



Registered JMX MBean Hierarchy

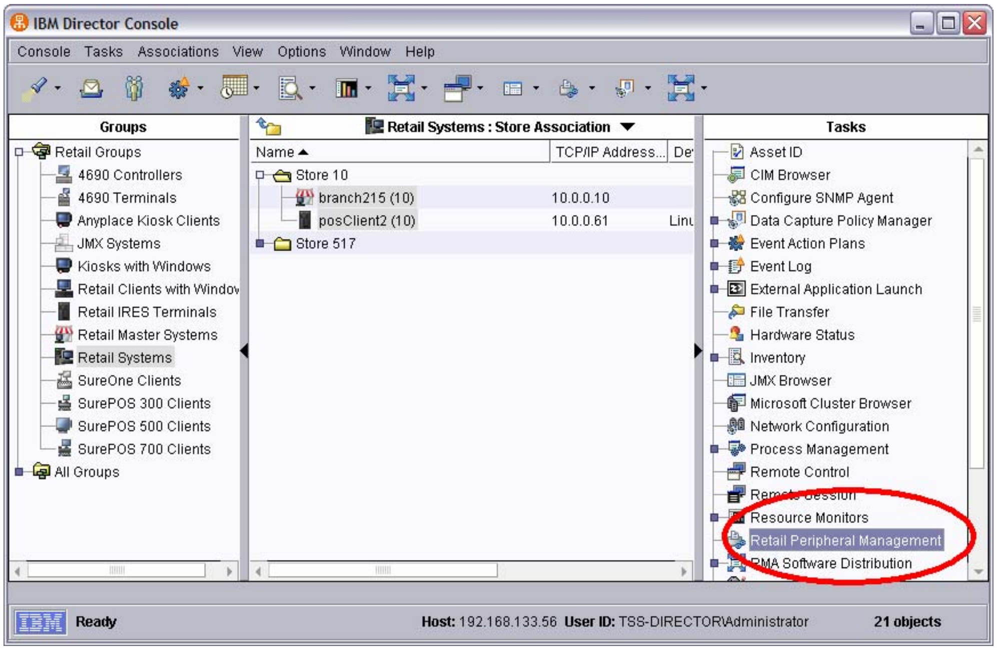
- posClient2 (10)
  - posClient2.10151
    - CIM
      - Linux_BIOSElement
      - Linux_BIOSFeature
      - Linux_BIOSProduct
      - Linux_ComputerSystem
      - Linux_EthernetPort
      - Linux_Ext3FileSystem
      - Linux_IPProtocolEndpoint
      - Linux_LocalLoopbackPort
      - Linux_NFSv3SystemConfiguration
      - Linux_OperatingSystem
      - Linux_Processor
      - UPOS_LogicalDevice
      - UPOS_MSR
      - UPOS_POSPrinter
    - JAVA
    - MGMT

JMX Class Name com.ibm.retail.si.mgmt.cim.CIMProxyMBean

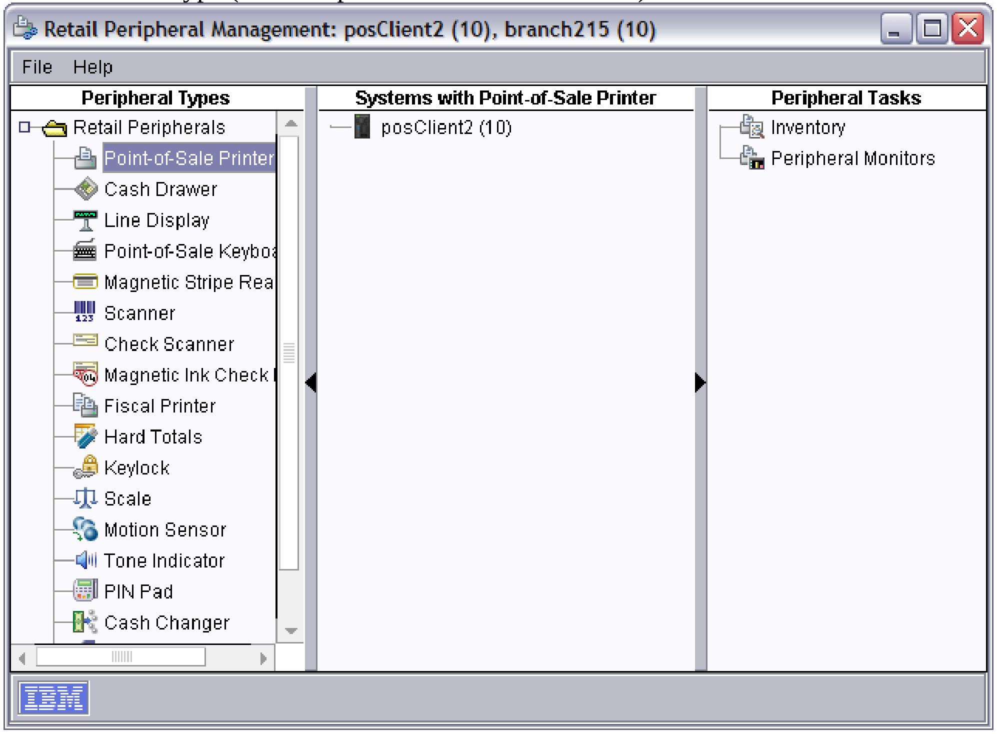
"UPOS_POSPrinter.SystemCreationClassName=nullSystemName=nullDeviceID=POSPrinter1UPO

Modifiable	Name	Type	
🔒	AdditionalAvailability	[Ljava.lang.Integer	
🔒	Availability	java.lang.Integer	
🔒	BarcodePrintedCount	java.lang.Long	22
🔒	Bus	java.lang.String	USB
🔒	CapCharacterSet	java.lang.Long	998
🔒	CapCompareFirmwareVersion	boolean	false
🔒	CapConcurrentJrnRec	boolean	false
🔒	CapConcurrentJrnSlp	boolean	false
🔒	CapConcurrentPageMode	boolean	false
🔒	CapConcurrentRecSlp	boolean	true
🔒	CapCoverSensor	boolean	true

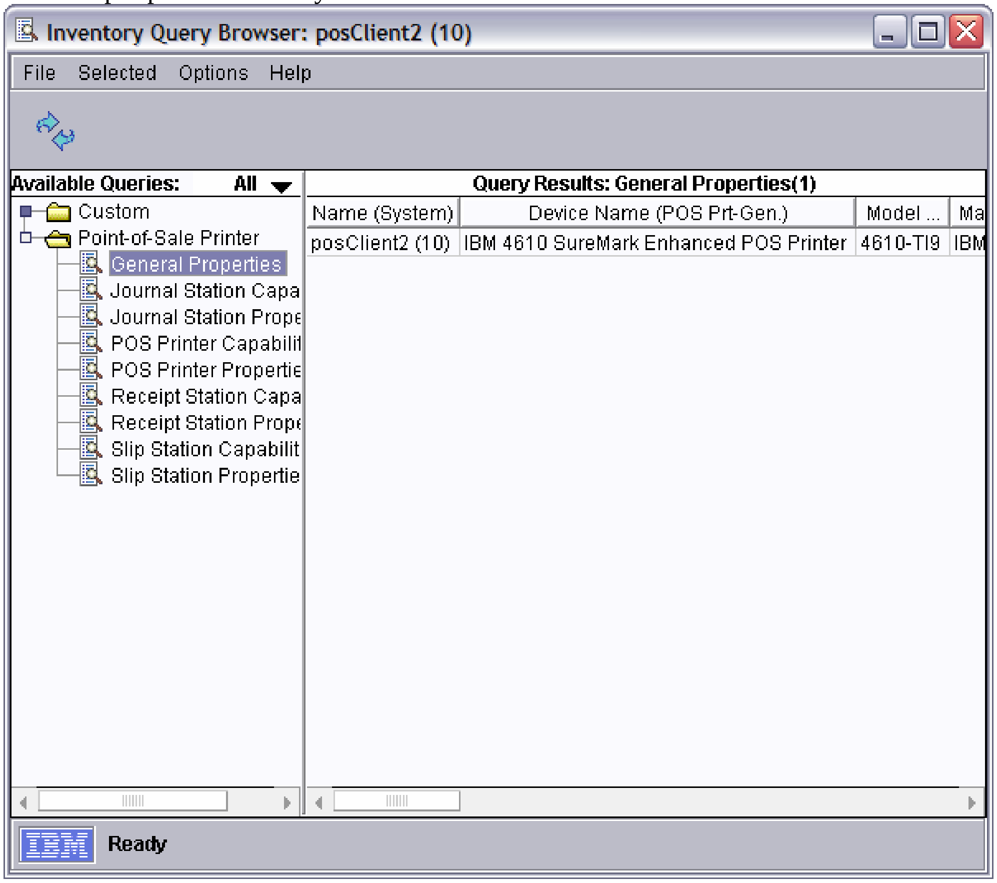
c. If you want to show the peripherals in software inventory, you can collect inventory to pull this information into the Director database. (Note: If the inventory does not get the information, this is probably because the CIM classes are not available. Always use the JMX Browser to verify directly whether the CIM classes are available.)



Select a device type (for example: “Point-of-Sale Printer”):



Drag the “Inventory” task to a system (or multiple selected systems) to view the peripheral inventory:



Name (System)	Device Name (POS Prt-Gen.)	Model ...	Ma
posClient2 (10)	IBM 4610 SureMark Enhanced POS Printer	4610-TI9	IBM

10. After you’ve verified that all the MBeans look correct for the IRES clients within the JMX Browser, you’re now ready to begin using all the other features of RMA and IBM Director to manage your IRES environment – such as inventory, resource monitoring, software distribution, power management, etc. (For help, please refer to the other chapters of this cookbook, the RMA user’s guide, and the IBM Director documentation.)

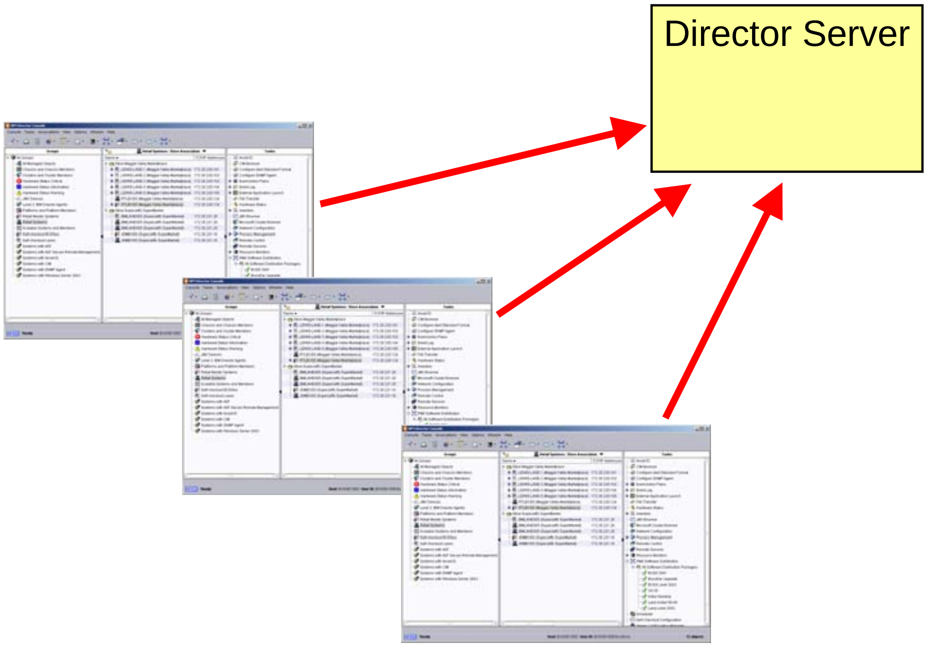
Chapter 5 – RMA/Director Basics

Comment:
Add chapter in the future: Advanced Setup Topics
Coming later … silent deployment, setting up Director Server on Linux, uninstalling, additional Director Consoles, masterhealth, using a NAT, configuring networking equipment (including BladeCenter switches), firewall configuration, Director databases, large # of stores for discovery, user administration, editing RMA config file (e.g. to change store number or network interface), etc.

This chapter should help you learn the “basics” of the Director console’s user interface, along with some of the core features of RMA/Director that will be used throughout the rest of this book. For example, we introduce core concepts such as “managed objects” and “groups”, and we discuss how to use Director’s “inventory” features to track the assets in your retail environment.

Introduction to RMA/Director Basics

The Director Console provides a user interface for the Director Server. You can install multiple instances of the Director Console to allow multiple I/T staff members to interact with the same Director Server. You can also configure the levels of permission for each console user, using the “User Administration” settings for Director Server. Each user of the Director Console must have a unique user ID on the Director Server.



The Director Console doesn’t need to be installed on the same system as the Director Server – as the diagram above shows, the Director Console can run on separate systems (for example, on a laptop with remote access to the Director Server). However, by default, when you install the Director Server, a local instance of the Director Console is also installed for convenience.

When the Director Console is installed on additional systems, please note that it also requires the installation of all applicable extensions (i.e. each console installation must include all the same "extra" installation packages, such as any Director service updates, retail extensions to enable RMA support, and other extensions as needed).

Resources

Although this chapter of the cookbook will give you "survival skills" in using the Director user interface and RMA, it is by no means a replacement for the existing documentation for RMA and Director.

For more comprehensive information, please refer to the IBM Director documentation – particularly the Redbook for IBM Director, which is found at the following URL: http://www.redbooks.ibm.com/abstracts/sg246188.html

You should also refer to the RMA user's guide:
http://www2.clearlake.ibm.com/store/support/html/pubs.html#RMA

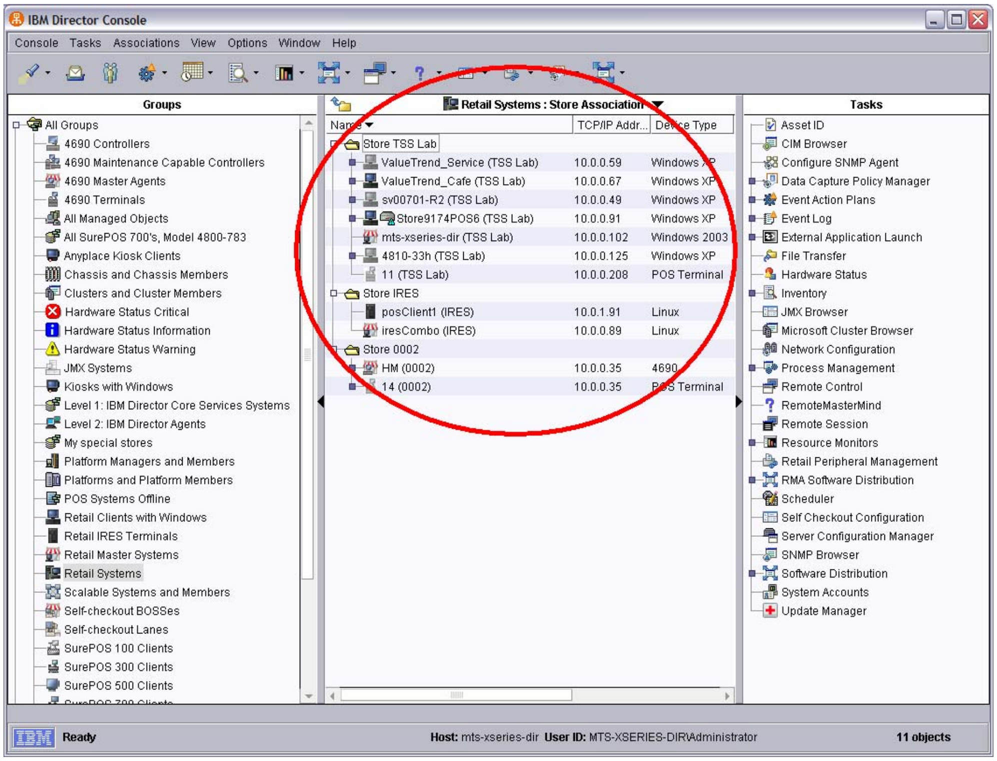
Using the Director Console

The main screen for the Director Console is divided into three panes – the groups pane, the center pane (which shows the sub-groups or managed objects within the currently selected group), and the tasks pane. (You can show or hide each of these panes using the "View" menu.)

What is a managed object?

A "managed object" (MO) is a Director object that represents a remote manageable entity – for retail systems, each MO is an instance of the RMA general agent (or master agent) running on a remote retail POS system.

If you click on "Retail Systems" in the groups pane, the center pane will display all the MO's (i.e. RMA agents) in your retail POS enterprise:



Name	TCP/IP Addr...	Device Type
Store TSS Lab		
ValueTrend_Service (TSS Lab)	10.0.0.59	Windows XP
ValueTrend_Cafe (TSS Lab)	10.0.0.67	Windows XP
sv00701-R2 (TSS Lab)	10.0.0.49	Windows XP
Store9174POS6 (TSS Lab)	10.0.0.91	Windows XP
mts-xseries-dir (TSS Lab)	10.0.0.102	Windows 2003
4810-33h (TSS Lab)	10.0.0.125	Windows XP
11 (TSS Lab)	10.0.0.208	POS Terminal
Store IRES		
posClient1 (IRES)	10.0.1.91	Linux
iresCombo (IRES)	10.0.0.89	Linux
Store 0002		
HM (0002)	10.0.0.35	4690
14 (0002)	10.0.0.35	POS Terminal

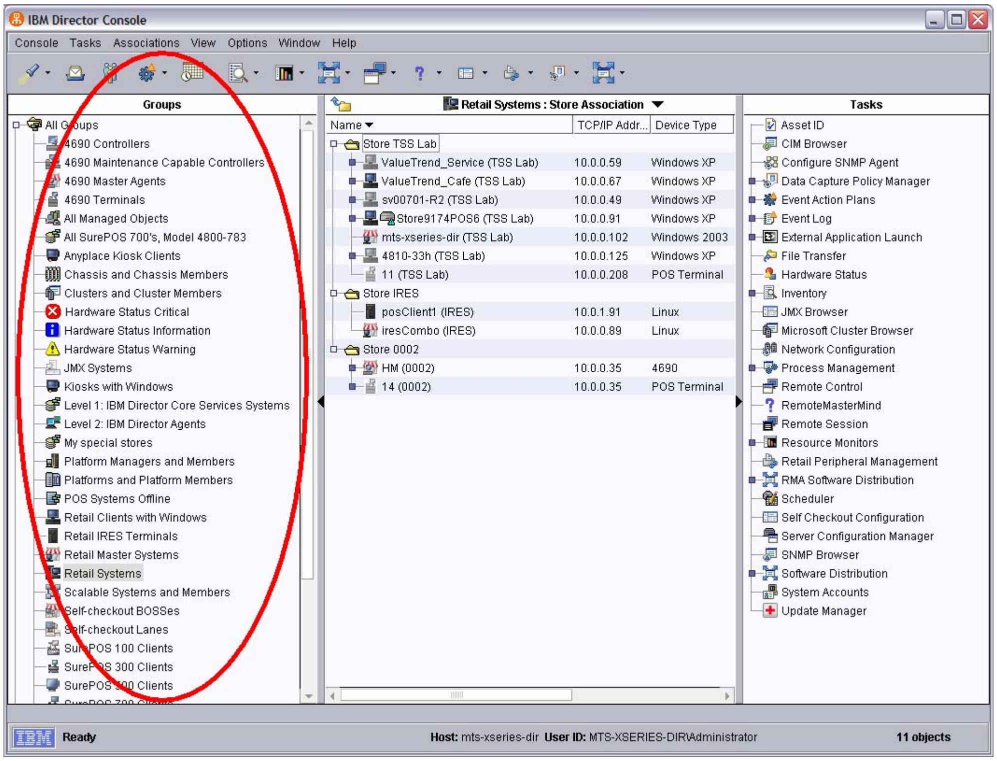
Host: mts-xseries-dir **User ID:** MTS-XSERIES-DIR\Administrator **11 objects**

Usually, each retail MO displayed in Director represents a single remote POS system that is running either an RMA master or general agent.

(However, if there are multiple instances of RMA running on a single machine, there could be multiple MO's for that machine in Director. For example, sometimes a java application such as IBM's "Store Integrator GUI" will instantiate an additional RMA agent on the system. This would cause the same system to appear as 2 different MO's in the console.)

What is a group?

When you select a group in the groups pane on the left, the center pane shows all the members of that group, usually a list of all the "managed objects" in the group, as shown below:



Name	TCP/IP Addr...	Device Type
Store TSS Lab		
ValueTrend_Service (TSS Lab)	10.0.0.59	Windows XP
ValueTrend_Cafe (TSS Lab)	10.0.0.67	Windows XP
sv00701-R2 (TSS Lab)	10.0.0.49	Windows XP
Store9174POS6 (TSS Lab)	10.0.0.91	Windows XP
mts-xseries-dir (TSS Lab)	10.0.0.102	Windows 2003
4810-33h (TSS Lab)	10.0.0.125	Windows XP
11 (TSS Lab)	10.0.0.208	POS Terminal
Store IRES		
posClient1 (IRES)	10.0.1.91	Linux
iresCombo (IRES)	10.0.0.89	Linux
Store 0002		
HM (0002)	10.0.0.35	4690
14 (0002)	10.0.0.35	POS Terminal

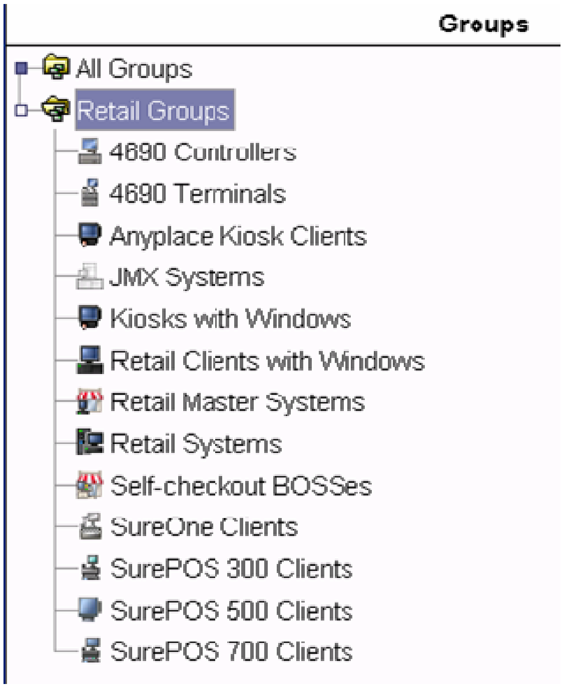
Ready Host: mts-xseries-dir User ID: MTS-XSERIES-DIR\Administrator 11 objects

Note: Some of the items in the groups pane are “groups of groups”. If you select one of these groups (e.g. “All Groups” or “Retail Groups”), then the center pane will display all the groups that are members of the selected group, rather than a list of managed objects in the group.

There are two kinds of groups that are important for our purposes:

- Static groups. The members of the group must be explicitly added or removed from the group
- Dynamic groups. Group membership is based on configurable criteria. Managed objects are automatically added to dynamic groups if their inventory data meets the defined criteria.

When RMA agents are discovered by Director, a number of pre-installed dynamic groups become visible in the Director Console. These are known as “Retail Groups”, as shown below:

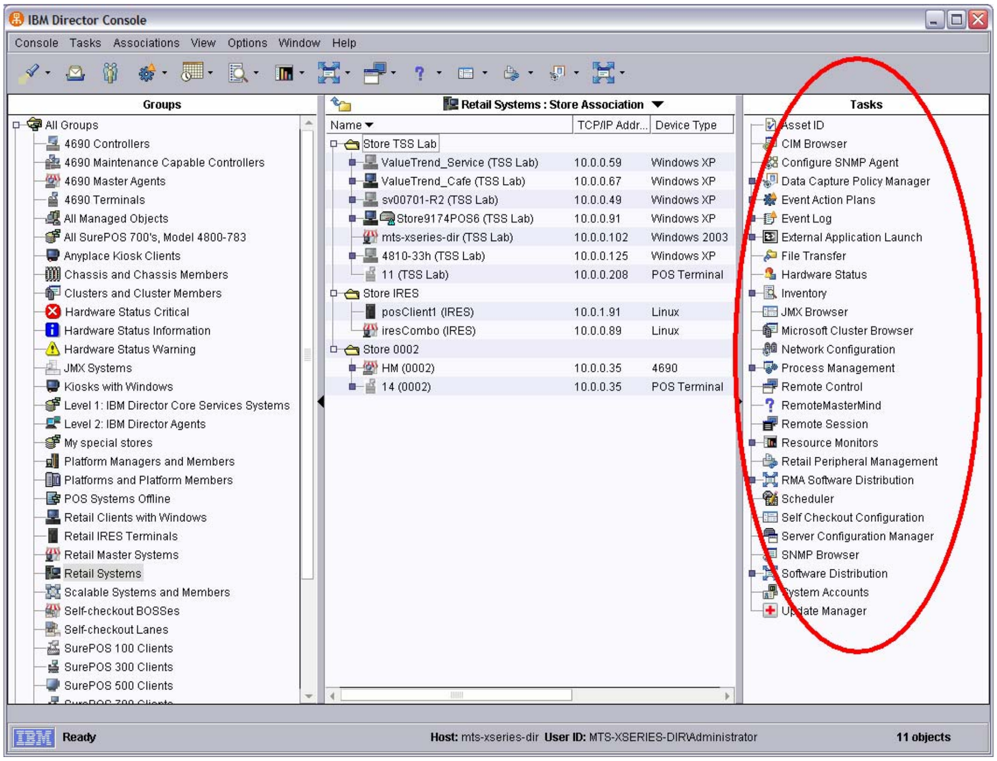


Groups

- All Groups
- Retail Groups
  - 4690 Controllers
  - 4690 Terminals
  - Anyplace Kiosk Clients
  - JMX Systems
  - Kiosks with Windows
  - Retail Clients with Windows
  - Retail Master Systems
  - Retail Systems
  - Self-checkout BOSSes
  - SureOne Clients
  - SurePOS 300 Clients
  - SurePOS 500 Clients
  - SurePOS 700 Clients

What is a task?

A "task" is an operation that can be performed on managed object(s), or on groups of managed objects. The tasks pane shows all the tasks that are available to be used with the managed objects in your environment. Not every task is applicable to every MO (for example, the "Microsoft Cluster Browser" is not supported for use with RMA MO's).



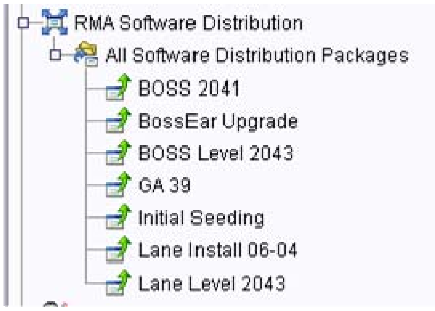
Name	TCP/IP Addr...	Device Type
Store TSS Lab		
ValueTrend_Service (TSS Lab)	10.0.0.59	Windows XP
ValueTrend_Cafe (TSS Lab)	10.0.0.67	Windows XP
sv00701-R2 (TSS Lab)	10.0.0.49	Windows XP
Store9174POS6 (TSS Lab)	10.0.0.91	Windows XP
mts-xseries-dir (TSS Lab)	10.0.0.102	Windows 2003
4810-33h (TSS Lab)	10.0.0.125	Windows XP
11 (TSS Lab)	10.0.0.208	POS Terminal
Store IRES		
posClient1 (IRES)	10.0.1.91	Linux
iresCombo (IRES)	10.0.0.89	Linux
Store 0002		
HM (0002)	10.0.0.35	4690
14 (0002)	10.0.0.35	POS Terminal

Host: mts-xseries-dir **User ID:** MTS-XSERIES-DIR\Administrator **11 objects**

Most tasks can be invoked in many different ways:

- Drag task to a single managed object
- Drag task to a selection of multiple objects (using the CTRL key to select multiple MO's)
- Drag task to a group
- Schedule task using the "Scheduler"
- Invoke task in reaction to an event – i.e. as part of an event action plan
- Invoke task "stand-alone" (i.e. not targeted to any MO's)
- Using menus, context menus, and/or toolbar icons

Many tasks can be "customized" – this allows you to configure the task and save it as a sub-task before applying the task to any MO's. For example, the "RMA Software Distribution" task allows you to create individual software distribution packages that are shown as sub-tasks in the Director Tasks pane. Example:



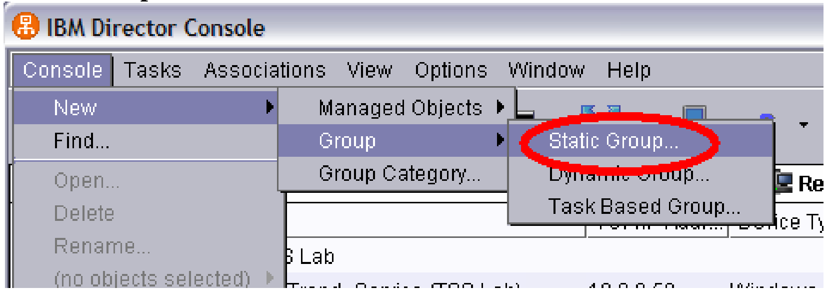
RMA Software Distribution
All Software Distribution Packages
BOSS 2041
BossEar Upgrade
BOSS Level 2043
GA 39
Initial Seeding
Lane Install 06-04
Lane Level 2043

Custom groups – dynamic and static

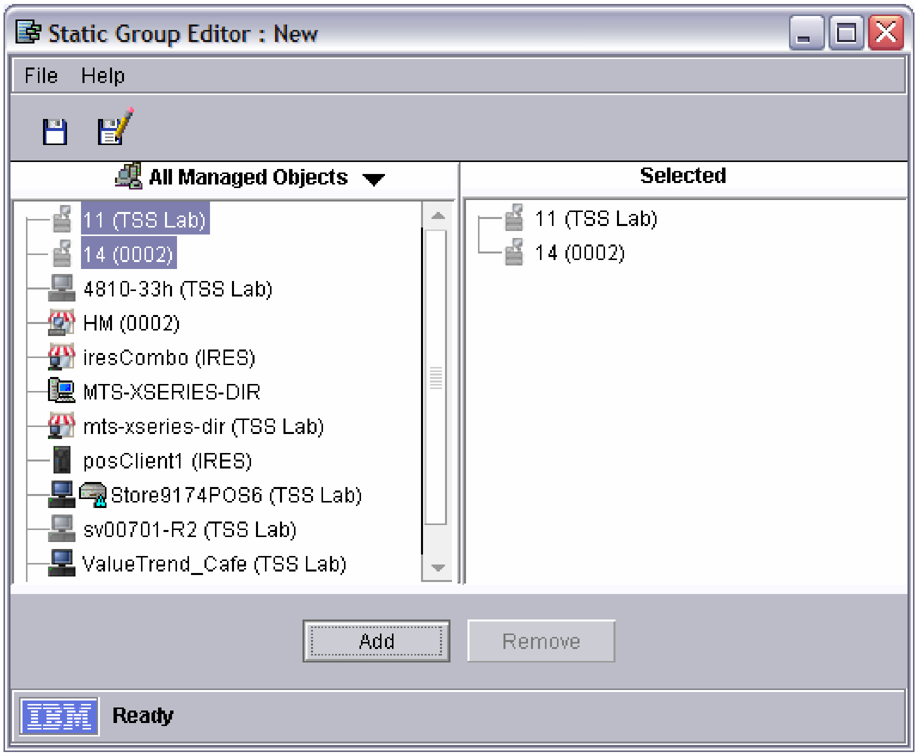
In addition to the pre-defined groups that are available for you to use, you can also create your own custom groups. These can be either “dynamic” or “static”.

A “static” group consists of a static selection of managed objects. See the following example for creating a static group:

- To create a new static group, use the “Console” menu to select “**New / Group / Static Group**”.

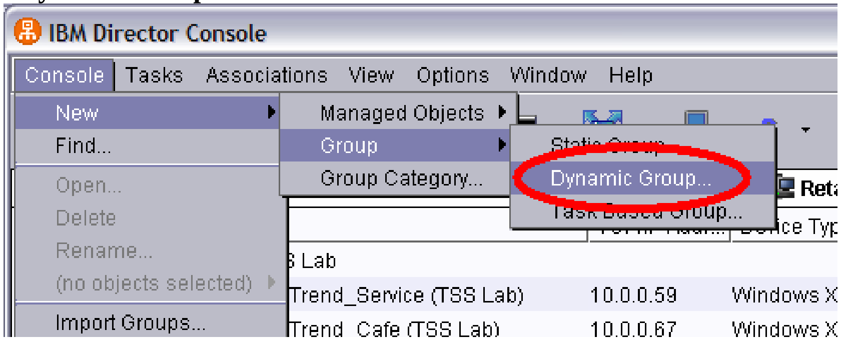


- Next, select the specific MO’s that will belong to the static group:

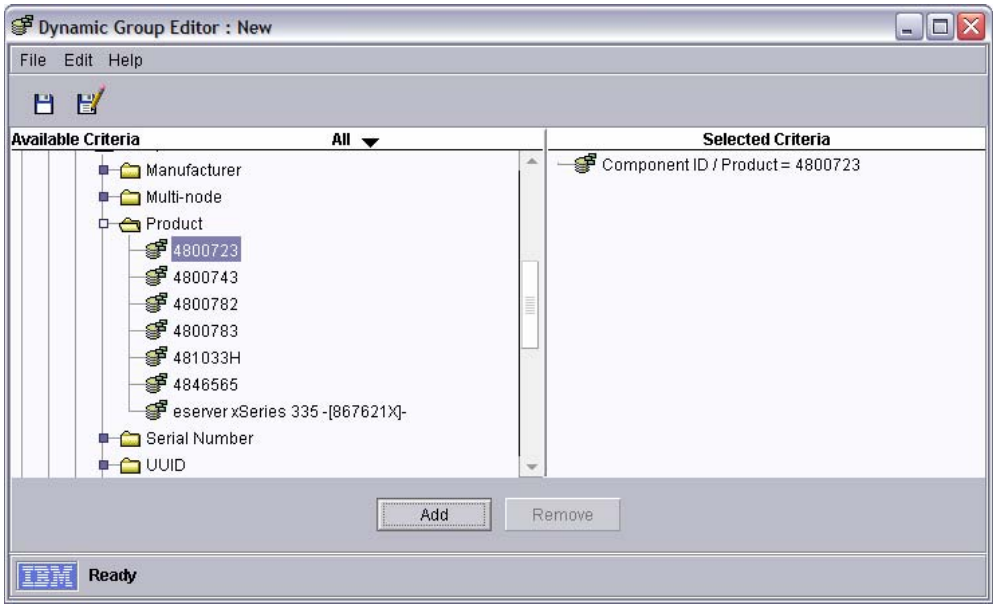


A “dynamic” group is a group that is defined based on rules about the inventory data or attributes for the MO. See the following example of a dynamic group:

- To create a new dynamic group, use the “Console” menu to select “**New / Group / Dynamic Group**”.



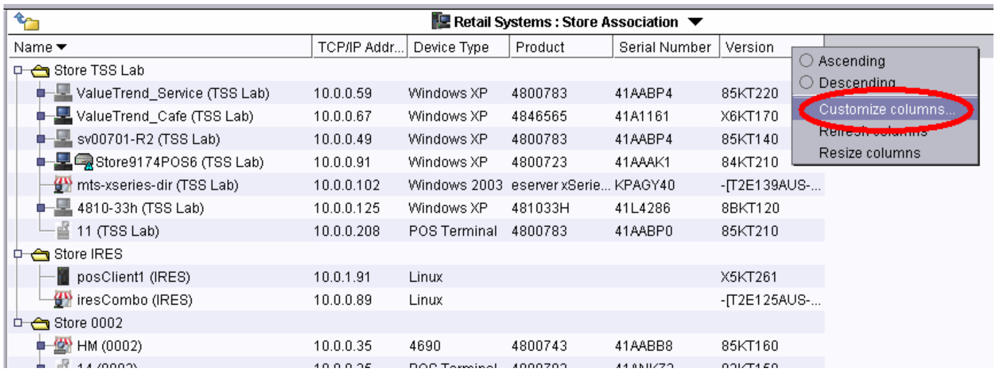
- Next, select the inventory or attribute criteria for your dynamic group. Director will automatically display all the MO’s in your environment that meet the criteria. When a new MO is discovered by Director, it will be added to any matching dynamic groups.



Customizing columns

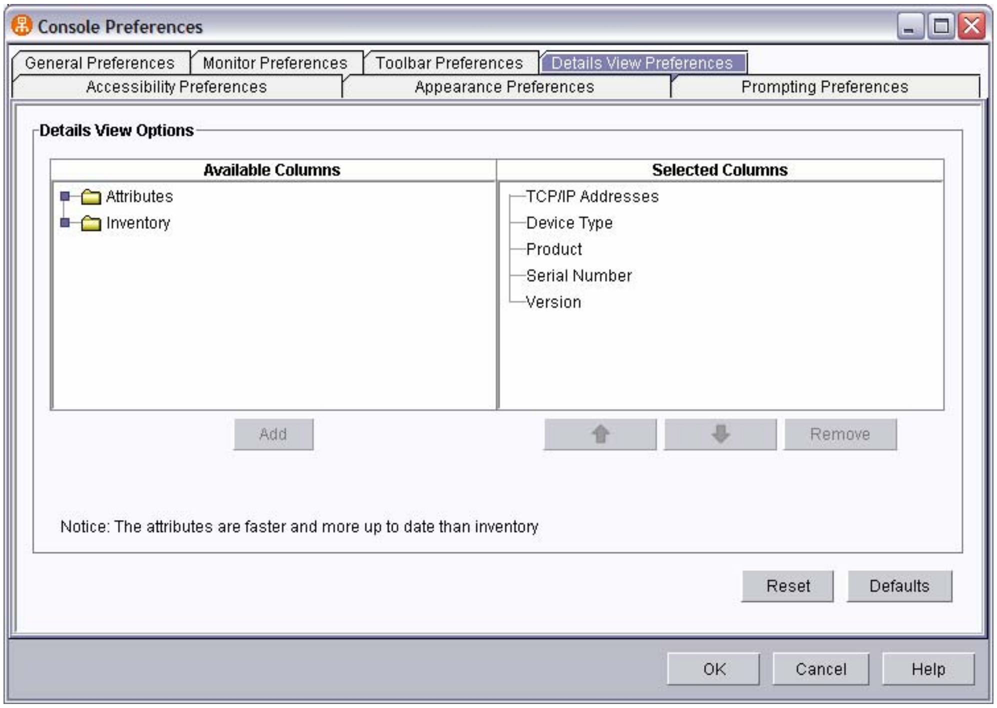
The default columns shown in the center pane of the Director Console are of limited usefulness. Fortunately, you can customize these columns to add retail-specific information about the MO's from inventory or MO attributes.

- To customize, right-click on one of the column headers and select "Customize columns":



Name	TCP/IP Addr...	Device Type	Product	Serial Number	Version
Store TSS Lab					
ValueTrend_Service (TSS Lab)	10.0.0.59	Windows XP	4800783	41AABP4	85KT220
ValueTrend_Cafe (TSS Lab)	10.0.0.67	Windows XP	4846565	41A1161	X6KT170
sv00701-R2 (TSS Lab)	10.0.0.49	Windows XP	4800783	41AABP4	85KT140
Store9174POS6 (TSS Lab)	10.0.0.91	Windows XP	4800723	41AAAK1	84KT210
mts-xseries-dir (TSS Lab)	10.0.0.102	Windows 2003	eserver xSerie...	KPAGY40	-[T2E139AUS-...
4810-33h (TSS Lab)	10.0.0.125	Windows XP	481033H	41L4286	8BKT120
11 (TSS Lab)	10.0.0.208	POS Terminal	4800783	41AABP0	85KT210
Store IRES					
posClient1 (IRES)	10.0.1.91	Linux			X5KT261
iresCombo (IRES)	10.0.0.89	Linux			-[T2E125AUS-...
Store 0002					
HM (0002)	10.0.0.35	4690	4800743	41AABB8	85KT160

- Next, select the inventory data or MO attributes to be shown in the center pane of the console:



Console Preferences

Details View Options

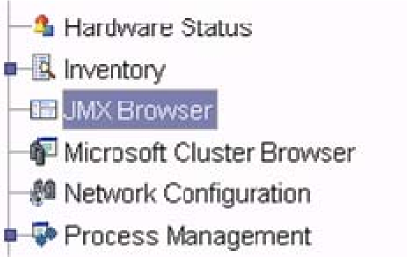
Available Columns	Selected Columns
Attributes	TCP/IP Addresses
Inventory	Device Type
	Product
	Serial Number
	Version

Notice: The attributes are faster and more up to date than inventory

Using the JMX Browser

For advanced users, the “JMX Browser” task allows viewing and manipulating of the raw “MBeans” that are exposed by RMA. These MBeans together comprise all the instrumentation that is available to Director for a particular MO. The JMX Browser is a wonderful tool for troubleshooting or understanding the internal workings of RMA.

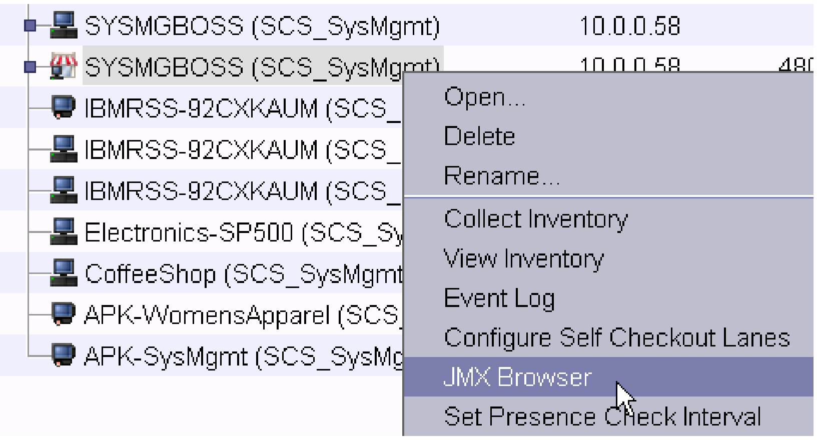
The JMX Browser task appears in the tasks pane of the console:



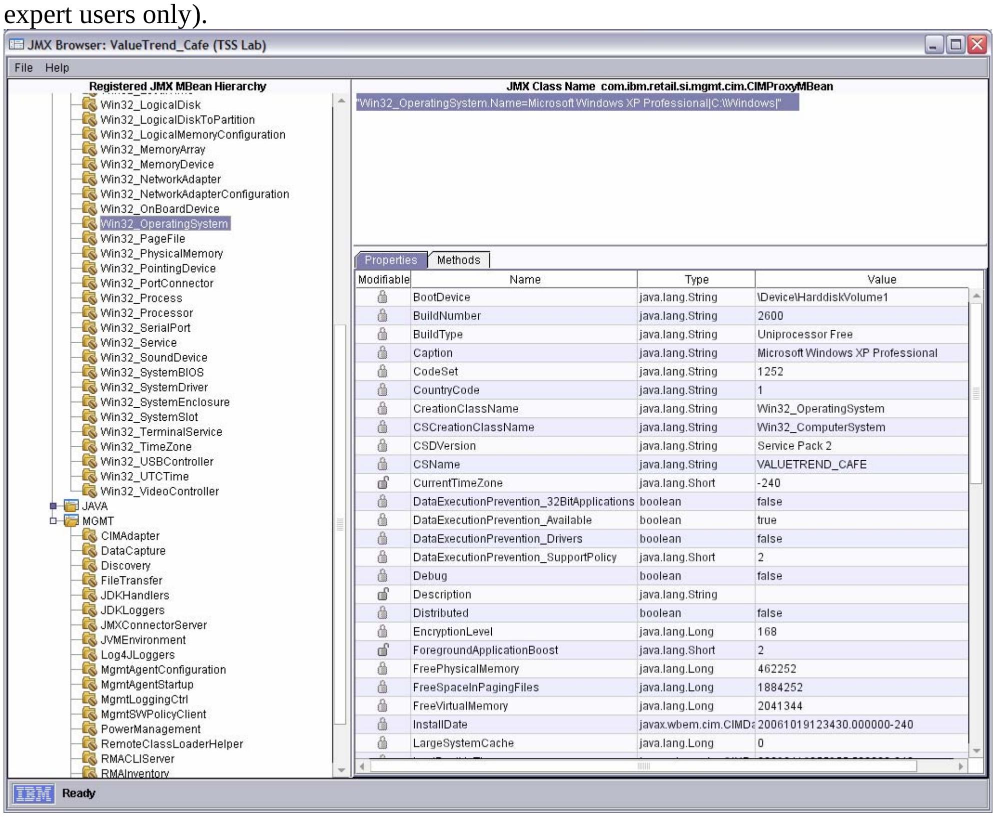
The JMX Browser allows you to do the following:

- Allows viewing of hundreds of properties of the remote system
- Allows you to invoke methods remotely on the MBeans

To launch the JMX Browser, you can drag-and-drop the task, or you can right-click the system and select “JMX Browser” from the context menu.



Within the JMX Browser, you can navigate all the MBean classes and their instances, and view the properties and methods for those MBeans. You can also execute methods (for expert users only).



JMX Class Name com.ibm.retail.si.mgmt.cim.CIMProxyMBean

"Win32_OperatingSystem.Name=Microsoft Windows XP Professional|C:\WINDOWS|"

Modifiable	Name	Type	Value
🔒	BootDevice	java.lang.String	\Device\HarddiskVolume1
🔒	BuildNumber	java.lang.String	2600
🔒	BuildType	java.lang.String	Uniprocessor Free
🔒	Caption	java.lang.String	Microsoft Windows XP Professional
🔒	CodeSet	java.lang.String	1252
🔒	CountryCode	java.lang.String	1
🔒	CreationClassName	java.lang.String	Win32_OperatingSystem
🔒	CSCreationClassName	java.lang.String	Win32_ComputerSystem
🔒	CSDVersion	java.lang.String	Service Pack 2
🔒	CSName	java.lang.String	VALUETREND_CAFE
🔓	CurrentTimeZone	java.lang.Short	-240
🔒	DataExecutionPrevention_32BitApplications	boolean	false
🔒	DataExecutionPrevention_Available	boolean	true
🔒	DataExecutionPrevention_Drivers	boolean	false
🔒	DataExecutionPrevention_SupportPolicy	java.lang.Short	2
🔒	Debug	boolean	false
🔓	Description	java.lang.String	
🔒	Distributed	boolean	false
🔒	EncryptionLevel	java.lang.Long	168
🔓	ForegroundApplicationBoost	java.lang.Short	2
🔒	FreePhysicalMemory	java.lang.Long	462252
🔒	FreeSpaceInPagingFiles	java.lang.Long	1884252
🔒	FreeVirtualMemory	java.lang.Long	2041344
🔒	InstallDate	javax.wbem.cim.CIMDa	20061019123430.000000-240
🔒	LargeSystemCache	java.lang.Long	0

Using Inventory

By default, when Director discovers a new RMA MO, it automatically collects “inventory” information for the remote system.

Inventory data is a collection of (mostly static) information about the remote system, including hardware and software information.

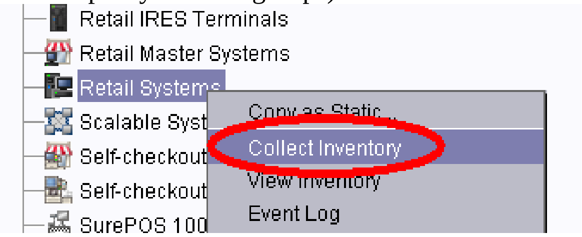
Some examples of inventory data:

- Serial number, manufacturer, model
- BIOS version
- Memory and hard drives installed/capacity
- CPU type, other device drivers
- Operating system type, version
- Networking settings, IP address
- Installed software packages (only available with RMA 2.5 and higher)

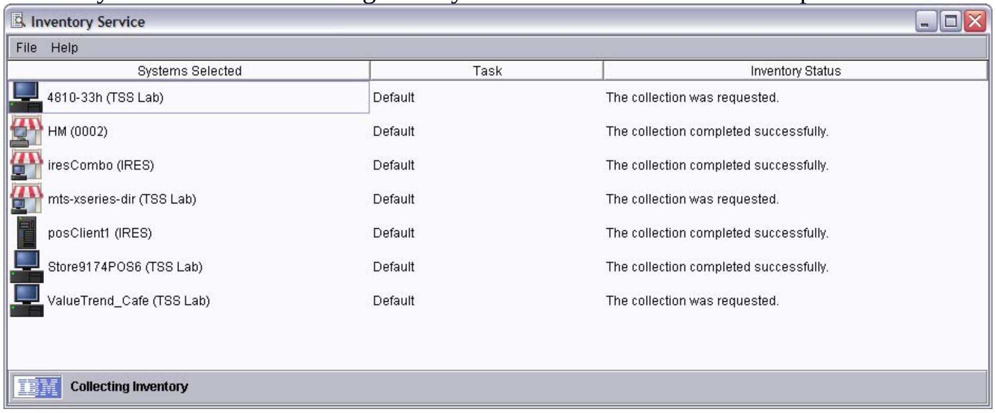
Inventory is collected and stored in a local database on the Director Server, which allows inventory information to be viewed and manipulated even when the remote systems are offline.

Basic collection and viewing

To collect inventory manually (one time), you can right-click any system (or a selection of multiple systems or groups) and select “Collect Inventory” from the context menu.



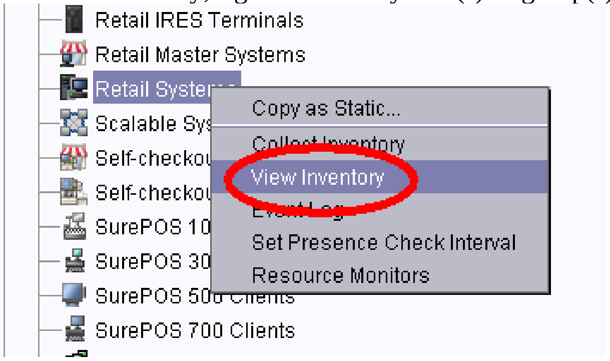
Inventory collection will then begin and you will see the status as it completes:



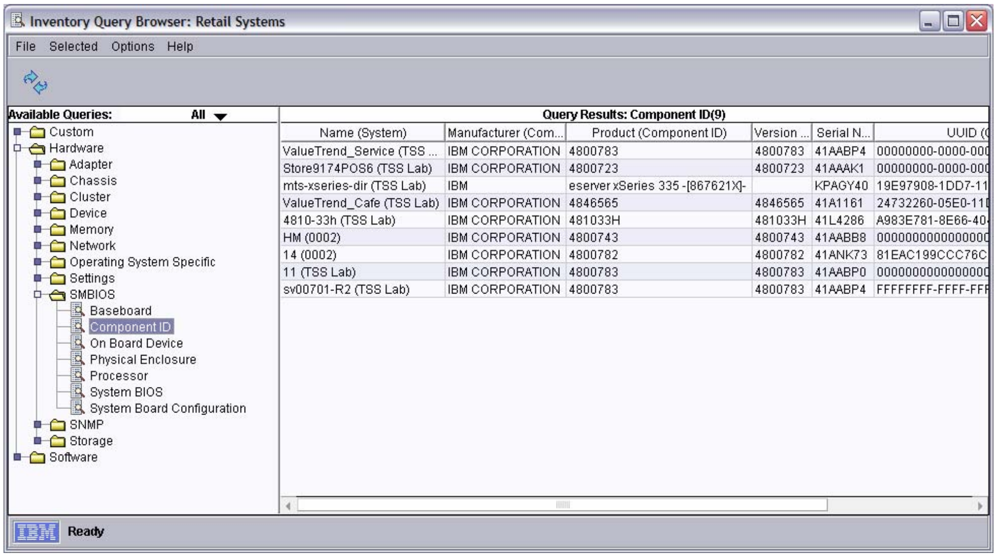
Systems Selected	Task	Inventory Status
4810-33h (TSS Lab)	Default	The collection was requested.
HM (0002)	Default	The collection completed successfully.
iresCombo (IRES)	Default	The collection completed successfully.
mts-xseries-dir (TSS Lab)	Default	The collection was requested.
posClient1 (IRES)	Default	The collection completed successfully.
Store9174POS6 (TSS Lab)	Default	The collection completed successfully.
ValueTrend_Cafe (TSS Lab)	Default	The collection was requested.

Collecting Inventory

To view inventory, right-click the system(s) or group(s) and select “View Inventory”.



You can then use the inventory query browser to browse through the available pre-defined inventory queries. This information is stored in a local database on the Director Server:

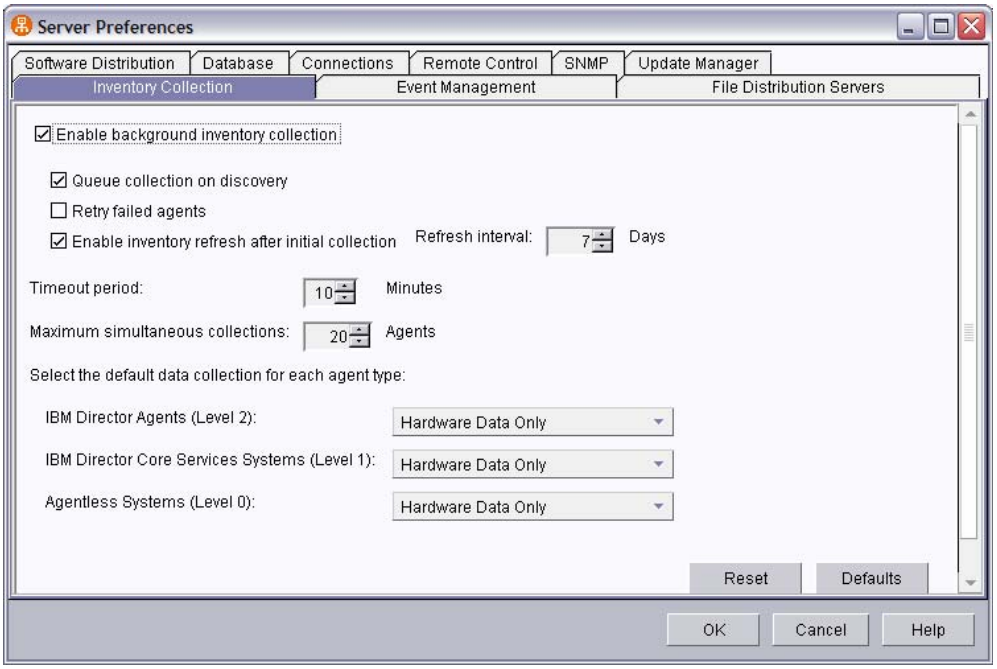


Query Results: Component ID(9)

Name (System)	Manufacturer (Com...	Product (Component ID)	Version ...	Serial N...	UUID (
ValueTrend_Service (TSS ...	IBM CORPORATION	4800783	4800783	41AABP4	00000000-0000-000
Store9174POS6 (TSS Lab)	IBM CORPORATION	4800723	4800723	41AAAK1	00000000-0000-000
mts-xseries-dir (TSS Lab)	IBM	eserver xSeries 335 -[867621X]-		KPAGY40	19E97908-1DD7-11
ValueTrend_Cafe (TSS Lab)	IBM CORPORATION	4846565	4846565	41A1161	24732260-05E0-11
4810-33h (TSS Lab)	IBM CORPORATION	481033H	481033H	41L4286	A983E781-8E66-40
HM (0002)	IBM CORPORATION	4800743	4800743	41AABB8	0000000000000000
14 (0002)	IBM CORPORATION	4800782	4800782	41ANK73	81EAC199CCC76C
11 (TSS Lab)	IBM CORPORATION	4800783	4800783	41AABP0	0000000000000000
sv00701-R2 (TSS Lab)	IBM CORPORATION	4800783	4800783	41AABP4	FFFFFFFF-FFFF-FFF

Configuring inventory collection

By default, inventory collection occurs on a revolving basis. The default values can be configured using the “**Options / Server Preferences**” console menu as shown below:



☑ Enable background inventory collection

☑ Queue collection on discovery

☐ Retry failed agents

☑ Enable inventory refresh after initial collection   Refresh interval: 7 Days

Timeout period: 10 Minutes

Maximum simultaneous collections: 20 Agents

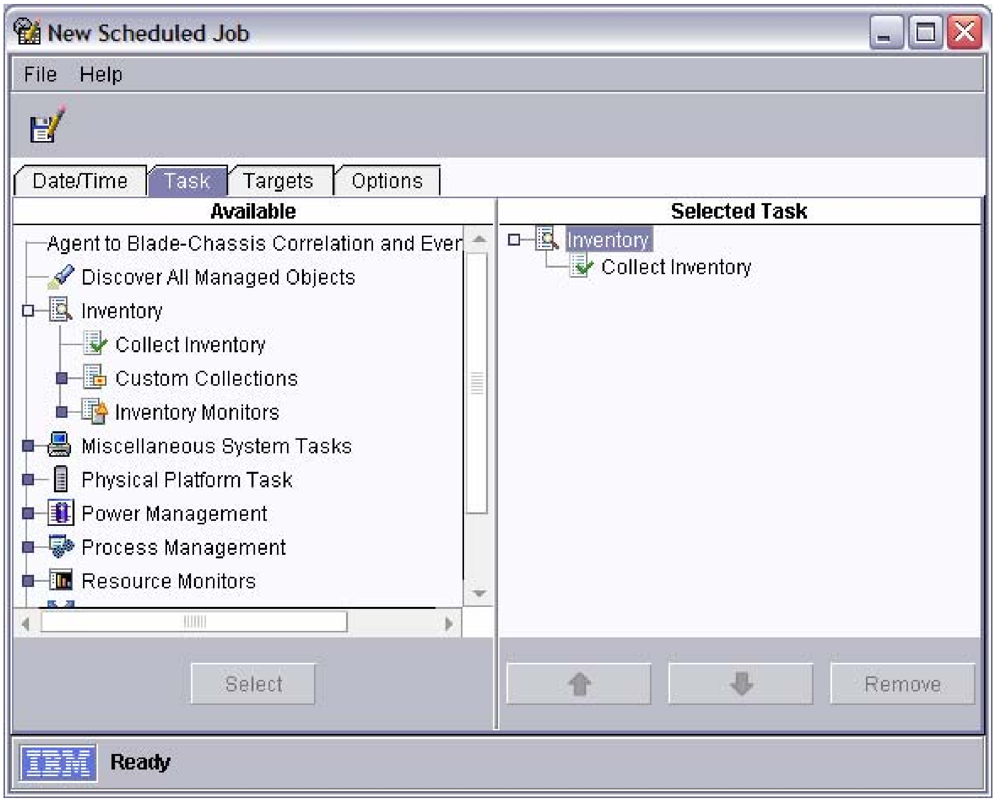
Select the default data collection for each agent type:

IBM Director Agents (Level 2): Hardware Data Only

IBM Director Core Services Systems (Level 1): Hardware Data Only

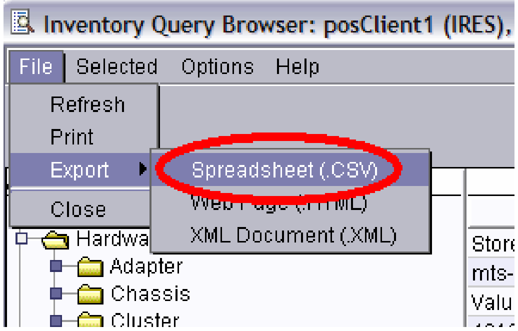
Agentless Systems (Level 0): Hardware Data Only

It is also possible to define your own schedule for inventory collection (i.e. to force inventory collection to take place during off-peak hours in your store). To do so, use the Director "Scheduler" task to schedule the "Collect Inventory" task:



Exporting

Inventory can be exported using the menu within the inventory query browser:

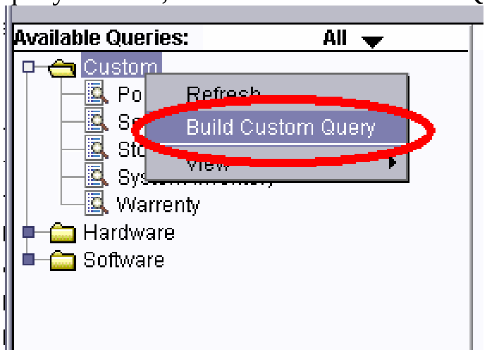


You can export to a spreadsheet (CSV file), web page (HTML), or to a structured XML document.

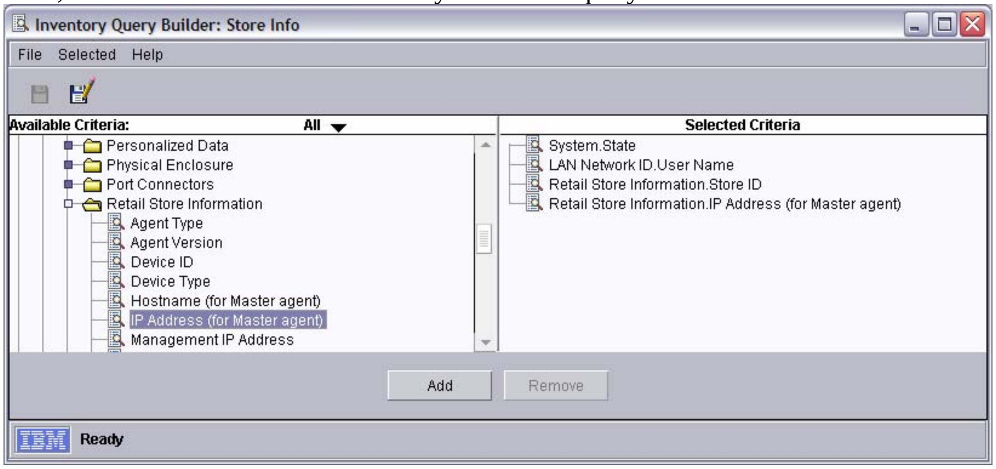
Custom Queries

To create a special/custom view of the inventory information, you can build “custom” inventory queries. This allows you to select the inventory attributes to display in your custom query.

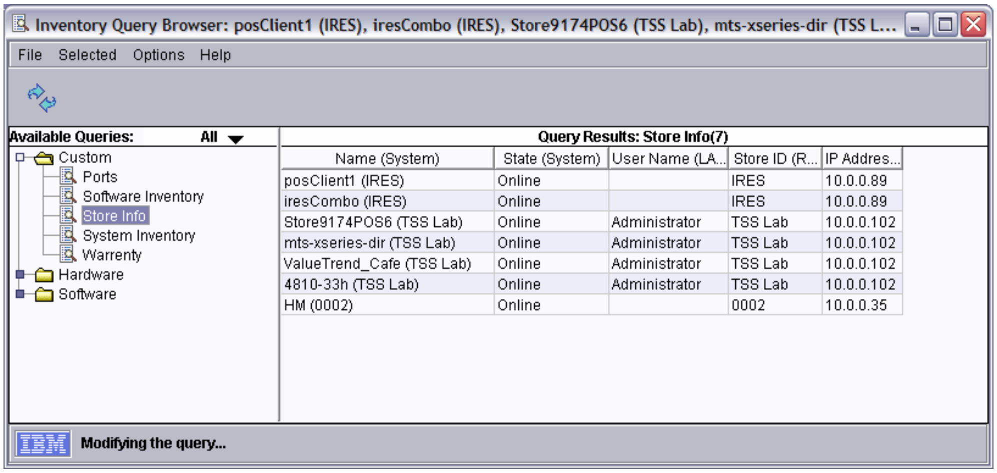
To start building a custom query, right-click the “Custom” category within the inventory query browser, and select “Build Custom Query” from the context menu:



Next, select the attributes to include in your custom query:



Your custom query will then be available within the inventory query browser, allowing you to quickly display the information you selected to include in your custom view:



Query Results: Store Info(7)

Name (System)	State (System)	User Name (LA...	Store ID (R...	IP Addres...
posClient1 (IRES)	Online		IRES	10.0.0.89
iresCombo (IRES)	Online		IRES	10.0.0.89
Store9174POS6 (TSS Lab)	Online	Administrator	TSS Lab	10.0.0.102
mts-xseries-dir (TSS Lab)	Online	Administrator	TSS Lab	10.0.0.102
ValueTrend_Cafe (TSS Lab)	Online	Administrator	TSS Lab	10.0.0.102
4810-33h (TSS Lab)	Online	Administrator	TSS Lab	10.0.0.102
HM (0002)	Online		0002	10.0.0.35

Stopping and Starting RMA and Director

When you install RMA and/or IBM Director, they will each be automatically configured to start automatically when the system boots. However, sometimes you need to be able to temporarily stop, start, or restart these services.

To stop RMA on Windows (or use the Services window):

```
net stop remotemgmtagent
```

To start RMA on Windows (or use the Services window):

```
net start remotemgmtagent
```

To stop and then restart IBM Director on Windows (or use the Services window):

```
net stop twgserver
net stop twgipc
net start twgipc (note: this also causes twgserver to start)
```

To stop RMA on 4690:

```
adxssp01 RMA -C
```

To start RMA on 4690:

```
adxssp01 RMA -R
```

To query the status of RMA on 4690:

```
adxssp01 RMA -Q
```

To stop RMA on Linux:

```
/etc/init.d/rmsvc-ga stop
```

To start RMA on Linux:

```
    /etc/init.d/rmsvc-ga start
```

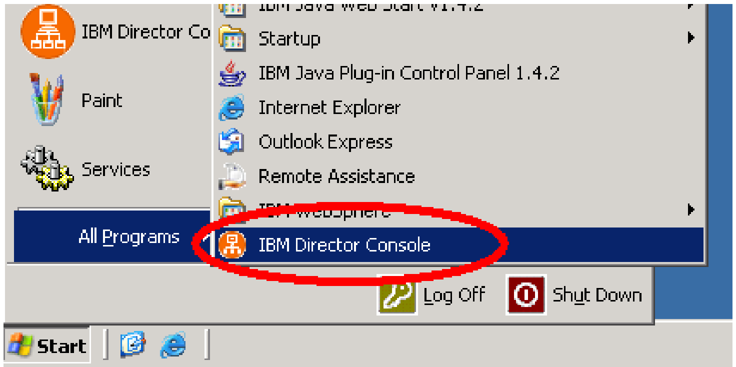
To query the status of RMA on Linux:

```
    /etc/init.d/rmsvc-ga status
```

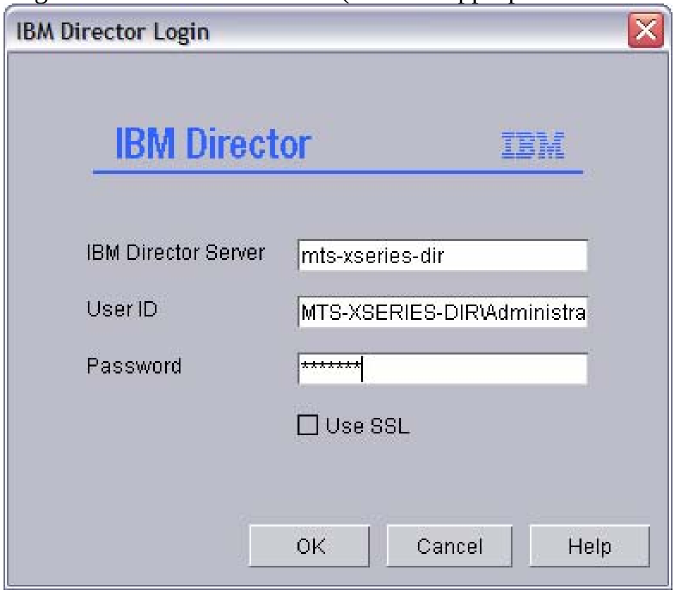
Example: Getting Oriented in Director (Exercise)

This example is an “exercise” to help you get familiar with the basics of using IBM Director and RMA. It assumes you’ve already successfully installed RMA and Director and have already discovered your managed objects, including at least one RMA master agent.

1. Launch the IBM Director Console from the start menu.



2. Log into the Director Console (with the appropriate user name and password).



IBM Director Login

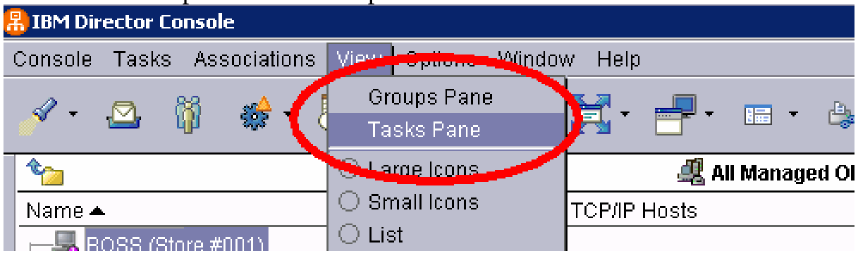
IBM Director Server: mts-xseries-dir

User ID: MTS-XSERIES-DIR\Administra

Password: *******

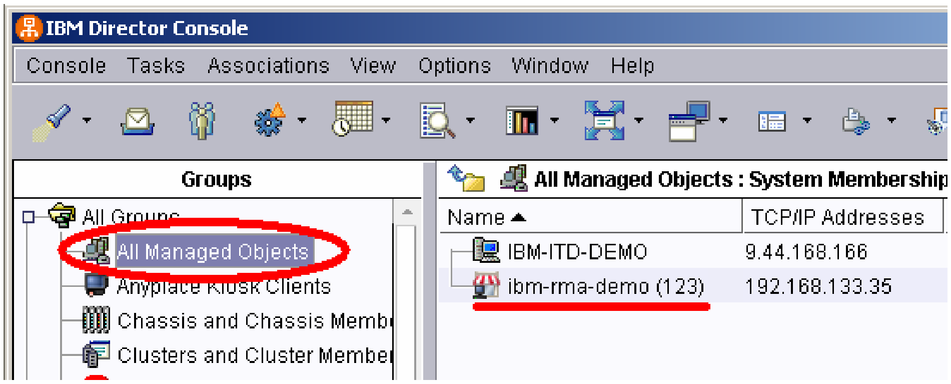
□ Use SSL

3. Show the “Groups” and “Tasks” panes.



Verify that the Director Console is now divided into 3 panes – Groups on the left, group members in the center, and tasks on the right.

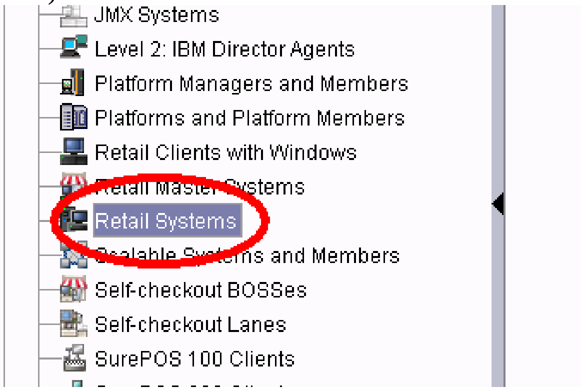
4. On the left, click on the “All Managed Objects” group. Verify that the RMA master agent is visible in the center pane. (The icon looks like a storefront, with red and white stripes on the canopy.) Make sure the icon is not grayed out (which would indicate that the master agent is offline).



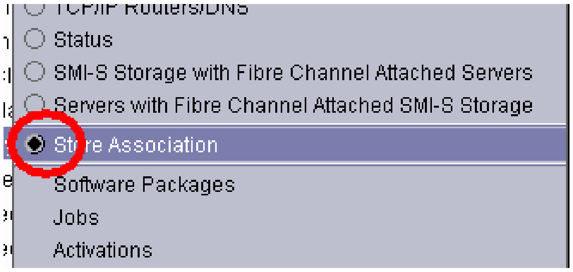
Name ▲	TCP/IP Addresses
IBM-ITD-DEMO	9.44.168.166
ibm-rma-demo (123)	192.168.133.35

5. View the properties for each of the managed objects (MO's) that appear in the console, by double-clicking on each one in turn.
   - Which MO represents the master agent / general agents?
   - Which MO represents the Director agent?
   - Which TCP/IP port is being used for each of these managed objects?

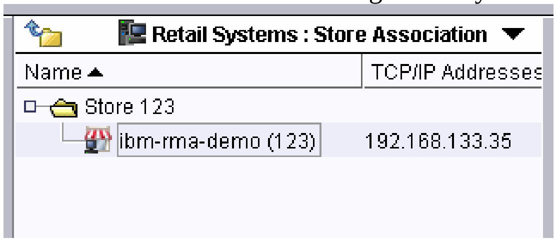
6. Select the "**Retail Systems**" group in the groups pane. You should now see only the RMA systems. (The Director Agent is no longer visible, since it is not a retail MO.)


JMX Systems
Level 2: IBM Director Agents
Platform Managers and Members
Platforms and Platform Members
Retail Clients with Windows
Retail Master Systems
Retail Systems
Scalable Systems and Members
Self-checkout BOSSes
Self-checkout Lanes
SurePOS 100 Clients

7. Make sure that "**Store Association**" is checked in the "**Associations**" menu of the Director Console.


○ TCP/IP Routers/DNS
○ Status
○ SMI-S Storage with Fibre Channel Attached Servers
○ Servers with Fibre Channel Attached SMI-S Storage
● Store Association
Software Packages
Jobs
Activations

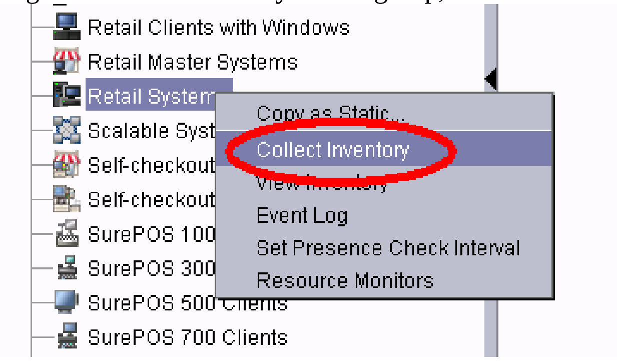
8. You should now see the MO’s organized by store:



Retail Systems : Store Association

Name	TCP/IP Addresses
Store 123	
ibm-rma-demo (123)	192.168.133.35

9. Collect inventory for all the retail systems.
    - Right-click the “**Retail Systems**” group, and select “**Collect Inventory**”.



    - Watch the status of the inventory collection as it completes.

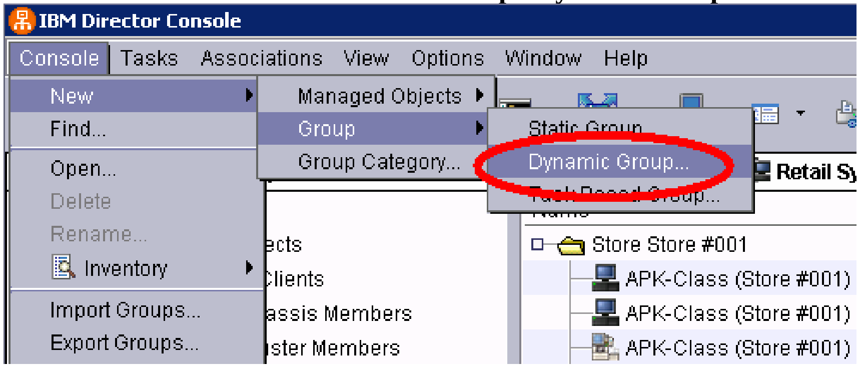
10. After inventory collection is complete, view the inventory by right-clicking “**Retail Systems**” and selecting “**View Inventory**”. Explore the inventory information that is available using the inventory query browser that appears.

    Try to find the following information in the inventory:
    - RMA software version
    - MAC address of the network adapter
    - Amount of physical memory installed on the virtual machine
    - BIOS version

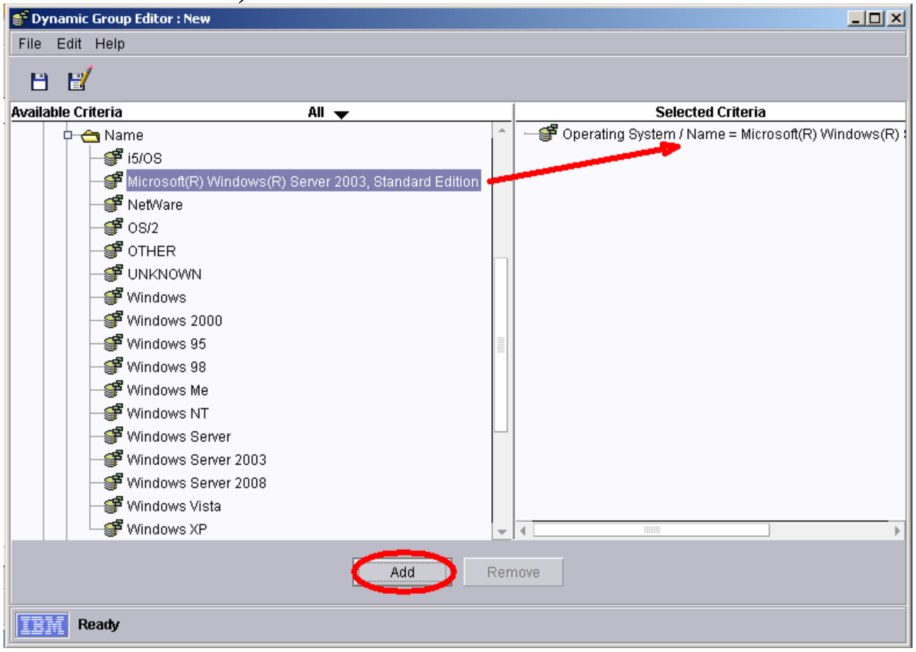
Example: Creating a Dynamic Group based on Software Versions

In this example, we’ll create a dynamic group to contain all RMA agents that are running on **Windows 2003 Server, Standard Edition,** build number **3790.**

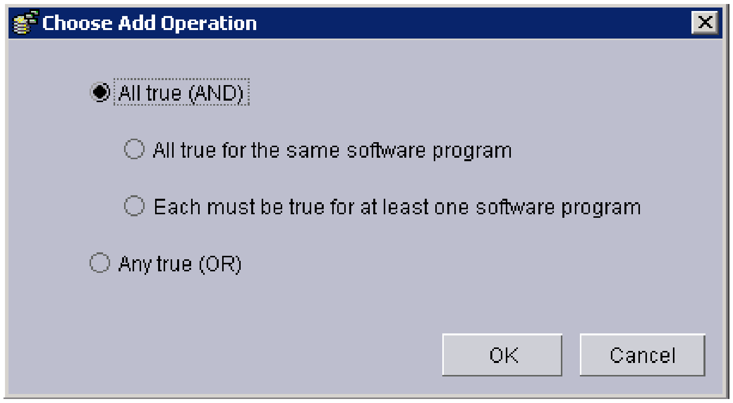
1. Use the console menu to select "**New / Group / Dynamic Group**".



2. First, expand the tree to "**Software / Operating System / Name**" and select "Microsoft(R) Windows(R) Server 2003, Standard Edition" (click "**Add**" to add it to the selected critera):



3. Next, expand the tree to "**Software / Operating System / Version**" and select the "5.2.3790" version. Click "**Add**", then select "**All true (AND)**" in the window that appears.



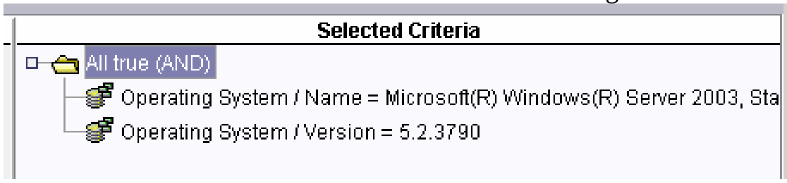
● All true (AND)

○ All true for the same software program

○ Each must be true for at least one software program

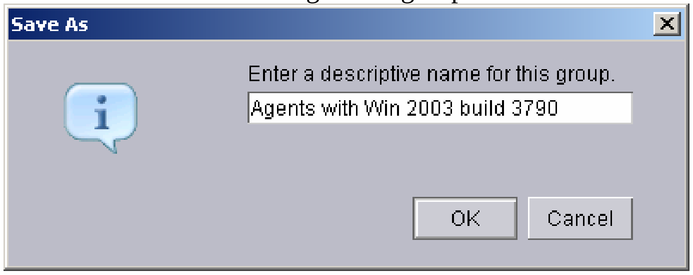
○ Any true (OR)

4. The selected criteria should now look like the following:



All true (AND)
- Operating System / Name = Microsoft(R) Windows(R) Server 2003, Sta
- Operating System / Version = 5.2.3790

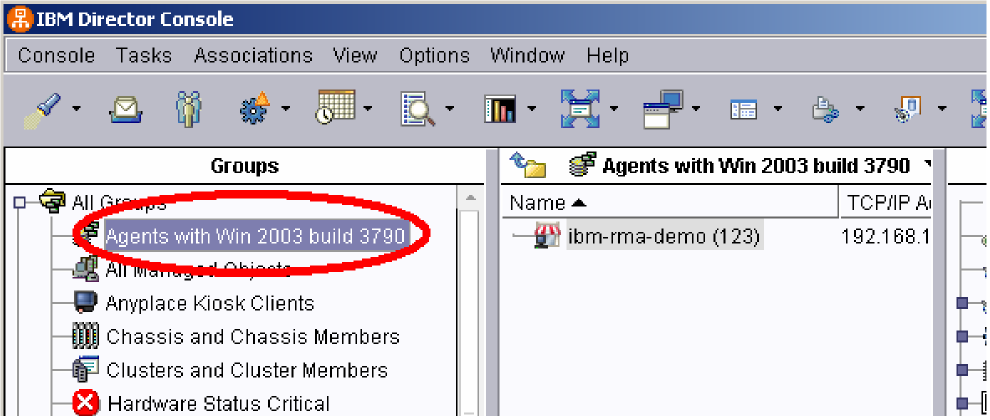
5. Click “**File / Save As**” and give the group a name.



Enter a descriptive name for this group.

Agents with Win 2003 build 3790

6. You should now see your group in the main Director Console’s groups pane:



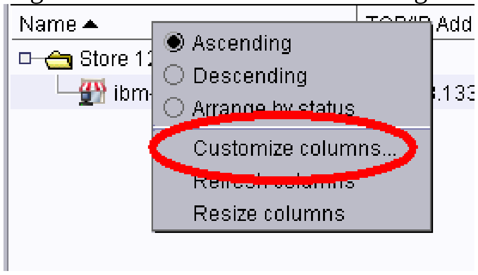
All Groups
- Agents with Win 2003 build 3790
- All Managed Objects
- Anyplace Kiosk Clients
- Chassis and Chassis Members
- Clusters and Cluster Members
- Hardware Status Critical

Name	TCP/IP A
ibm-rma-demo (123)	192.168.1

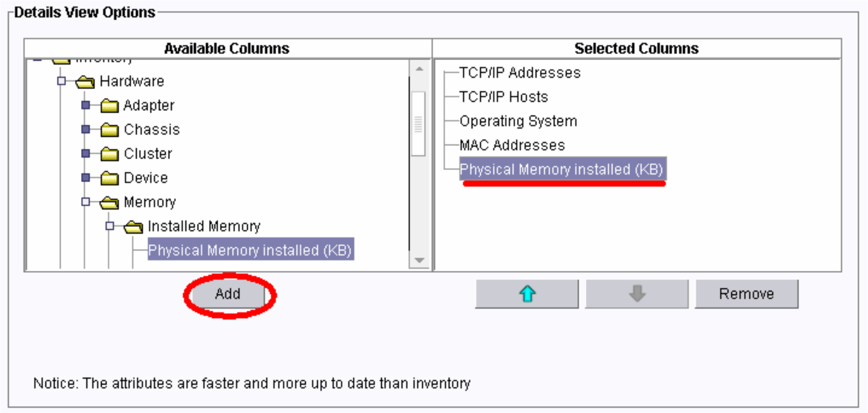
Example: Display Memory Installed in the Director Console

Add the “Physical Memory Installed (KB)” inventory attribute as a column in the center pane of the Console.

1. Right-click one of the column headings and select “Customize Columns”.



2. Add the attribute to the list, then click OK.

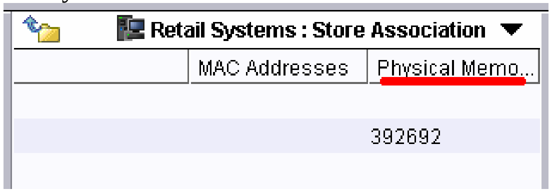


Selected Columns

- TCP/IP Addresses
- TCP/IP Hosts
- Operating System
- MAC Addresses
- Physical Memory installed (KB)

Notice: The attributes are faster and more up to date than inventory

3. Verify the new column in the Console



392692

Chapter 6 – Event Management

This chapter gives a basic introduction to the event management capabilities of RMA and IBM Director, along with examples of using event management with RMA/Director in an IBM POS environment.

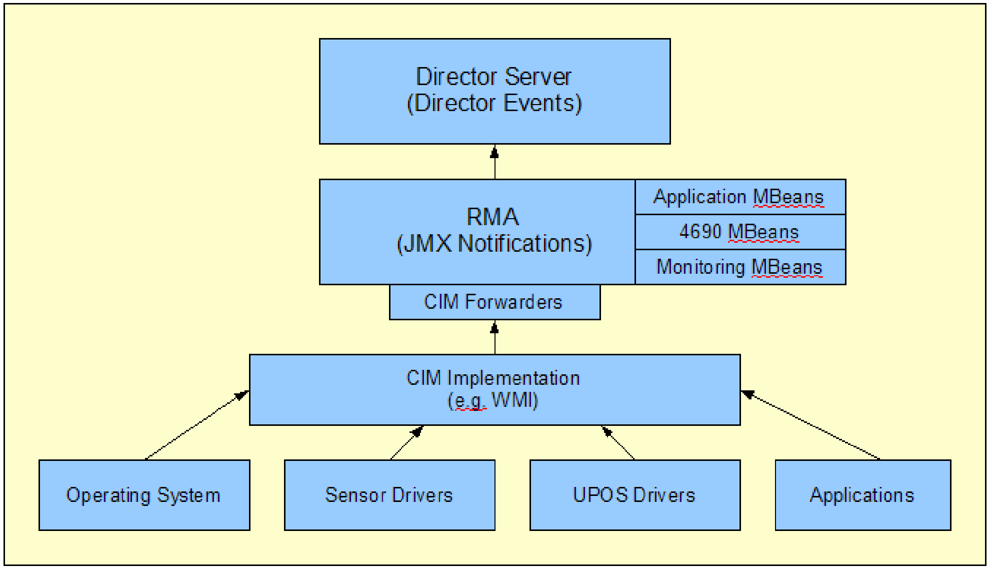
Introduction to Event Management

In the RMA/Director solution, "events" represent alerts that are forwarded from RMA to IBM Director, and can be handled by Director in a variety of ways. Events sometimes originate within RMA itself (e.g. resource monitoring thresholds trigger events internally within RMA), but usually the source of the event is external to RMA.

For example, many events on a Windows system are forwarded to RMA via the WMI event forwarders within the RMA agent. On 4690, events are created by MBeans that are monitoring the 4690 event logs.

When an event is created in RMA, the event becomes a "JMX Notification", which is ultimately forwarded to IBM Director and converted into a Director Event. RMA ensures that these events are never lost – i.e. if the master agent or the Director Server is offline, then the events will be saved locally to make sure they are saved until the upstream systems are back online (this feature is called "store and forward").

The following diagram illustrates the flow of events from CIM to RMA to Director:



There are many sources of events in IBM POS solutions. Here are a few examples:

- UPOS events – on Windows and Linux, all UPOS status update events are forwarded from CIM to RMA to IBM Director. This allows such events as “receipt near end” (i.e. the paper-low sensor for the 4610-2CR/2NR printers) to be handled by Director. For more information, see “**Chapter 9 – Retail Peripheral Management**”.

- Sensor driver events – on Windows only, for systems with sensor drivers and light-path management via the service processor, the status of the LED lights is forwarded from CIM to RMA to IBM Director. This allows management of these LED status lights from the enterprise.

- SMART events – on Windows, selected additional CIM events, such as SMART events (i.e. predicting hard drive failure) are also forwarded from CIM to RMA to IBM Director.

- Resource monitoring events – on all operating systems, RMA’s support for resource monitoring allows events to be generated when the monitored values meet the configured threshold conditions. These events are forwarded from RMA to Director. For more information, see “**Chapter 7 – Resource Monitoring**”.

- Inventory alerts – these are generated within IBM Director in response to inventory alerts that have been configured. For more information, see “**Chapter 5 – RMA/Director Basics**”.

- Director status events – these events don’t really originate from RMA. They are created at the Director Server – for example, RMA agent online/offline.

- 4690 event logs – in a 4690 environment, the MBeans for 4690 monitor the 4690 event logs, and forward these events to RMA (and ultimately to Director). This allows remote management of the 4690 system and application event logs.

- Windows event logs – on Windows, RMA has the ability to forward events from the Windows Event Logs (Application, System, and Security events) to IBM Director. To configure which events will get forwarded you need to set up the “Win32EventLogConfig.xml” found in “C:\Program Files\IBM\StoreIntegrator\user\rma\config\events”. See below for more details.

- Application-specific events – for example, the IBM CHEC self-checkout software automatically forwards a number of events to RMA. In the case of CHEC, it is done via application-specific MBeans within RMA, but it’s also possible to send application events via CIM forwarding.

Resources

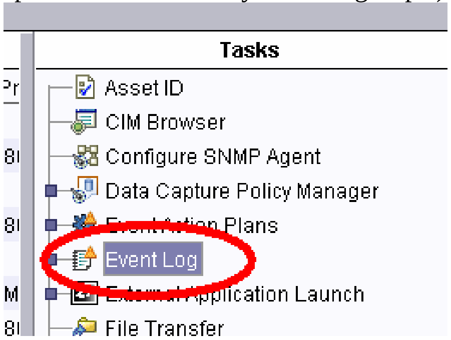
Event management within IBM Director is a large topic. This chapter of the cookbook only gives you the minimal information needed to begin working with events via RMA.

For a more thorough discussion of event management within Director, please refer to the IBM Director documentation – particularly the Redbook for IBM Director, which is found at the following URL:
http://www.redbooks.ibm.com/abstracts/sg246188.html

You should also refer to the RMA user's guide for more information on event handling within RMA:
http://www2.clearlake.ibm.com/store/support/html/pubs.html#RMA

Using the Director Event Log

The "Event Log" is a task within IBM Director. It displays all of the events for the selected system(s). (i.e. You can view ALL events, or you can view the events for a specific selection of systems or groups.)

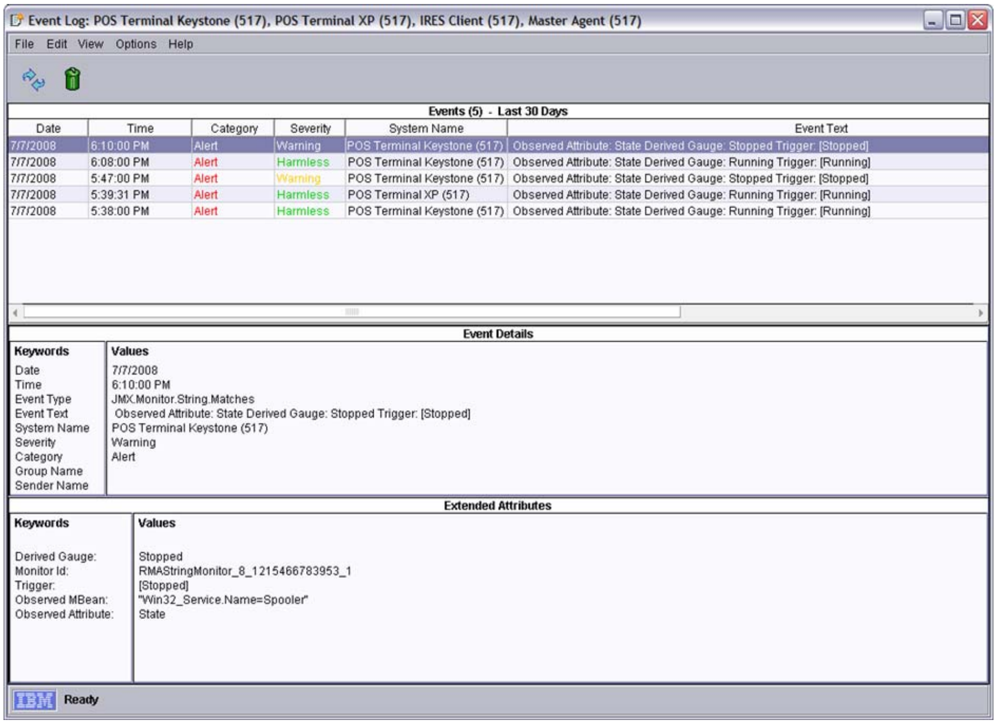


Event Log Viewer

There are several ways to launch the event log task:

1. Drag and drop (to a group, a single object, or a selection of multiple managed objects)
2. Select group or managed object(s), then:
   a. Right-click and use the drop-down context menu
   b. Use the "Tasks" menu to launch the event log
   c. Use the toolbar icon to launch the event log
3. You can also launch the event log without a selection of groups or managed objects – this will display events from all systems.

When you launch the event log, you will bring up the "Event Log Viewer". Each line in the viewer represents an event. You can click any line to show the details for that event.


Event Log: POS Terminal Keystone (517), POS Terminal XP (517), IRES Client (517), Master Agent (517)
File Edit View Options Help
IBM
Ready

Events (5) - Last 30 Days

Date	Time	Category	Severity	System Name	Event Text
7/7/2008	6:10:00 PM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: State Derived Gauge: Stopped Trigger: [Stopped]
7/7/2008	6:08:00 PM	Alert	Harmless	POS Terminal Keystone (517)	Observed Attribute: State Derived Gauge: Running Trigger: [Running]
7/7/2008	5:47:00 PM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: State Derived Gauge: Stopped Trigger: [Stopped]
7/7/2008	5:39:31 PM	Alert	Harmless	POS Terminal XP (517)	Observed Attribute: State Derived Gauge: Running Trigger: [Running]
7/7/2008	5:38:00 PM	Alert	Harmless	POS Terminal Keystone (517)	Observed Attribute: State Derived Gauge: Running Trigger: [Running]

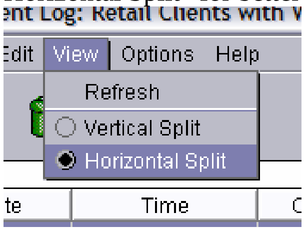
Event Details

Keywords	Values
Date	7/7/2008
Time	6:10:00 PM
Event Type	JMX.Monitor.String.Matches
Event Text	Observed Attribute: State Derived Gauge: Stopped Trigger: [Stopped]
System Name	POS Terminal Keystone (517)
Severity	Warning
Category	Alert
Group Name	
Sender Name	

Extended Attributes

Keywords	Values
Derived Gauge:	Stopped
Monitor Id:	RMAStringMonitor_8_1215466783953_1
Trigger:	[Stopped]
Observed MBean:	"Win32_Service.Name=Spooler"
Observed Attribute:	State

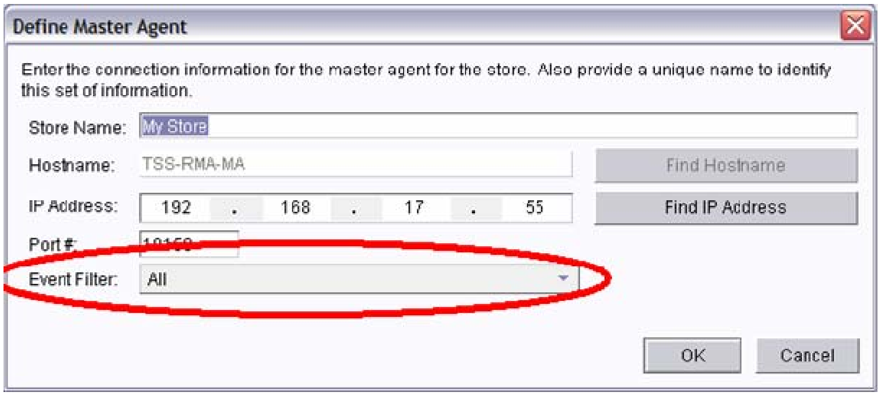
When working with the event log viewer, it’s sometimes a good idea to select “View / Horizontal Split” for better readability.



Configuring the Event Log

There are a number of configuration settings that have an impact on what events are collected, and what events are displayed in the event log viewer.

1. Discovery Preferences – The event filter field (in discovery preferences) controls which events are forwarded from RMA to IBM Director. If you are experiencing too many events at the Director Server, you might consider changing this setting in discover preferences. (In the main Director console, go to “Options / Discovery Preferences / Retail Store Devices / Edit”.)



Enter the connection information for the master agent for the store. Also provide a unique name to identify this set of information.

Store Name: My Store

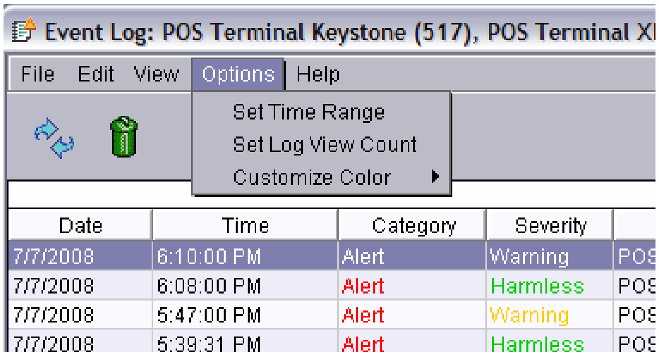
Hostname: TSS-RMA-MA

IP Address: 192 . 168 . 17 . 55

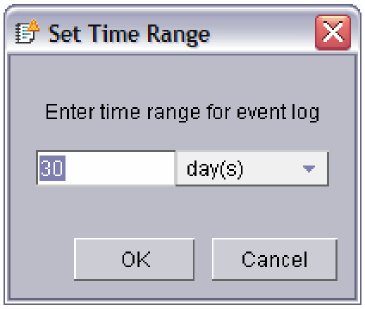
Port #: 10160

Event Filter: All

2. Event Log Viewer Options – Use “Options / Set Time Range” and “Options / Set Log View Count” in the Event Log menu. This changes the number of events that are displayed in the viewer, but it has no effect on the events that are actually stored on the server.

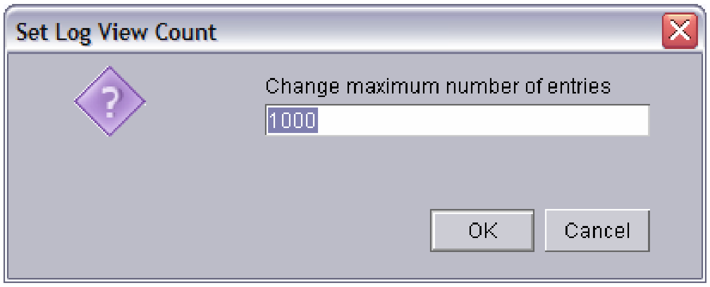


Date	Time	Category	Severity	
7/7/2008	6:10:00 PM	Alert	Warning	POS
7/7/2008	6:08:00 PM	Alert	Harmless	POS
7/7/2008	5:47:00 PM	Alert	Warning	POS
7/7/2008	5:39:31 PM	Alert	Harmless	POS



Enter time range for event log

30 day(s)

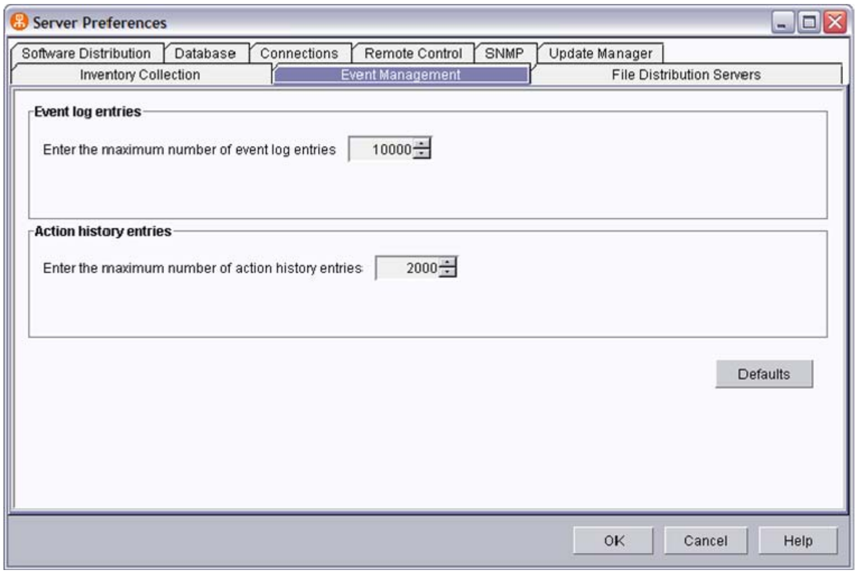


Set Log View Count

Change maximum number of entries

1000

3. Server Preferences – In the main Director console, go to “Options / Server Preferences / Event Management”. This allows you to configure the maximum number of events to store on the Director Server.



Event log entries

Enter the maximum number of event log entries 10000

Action history entries

Enter the maximum number of action history entries 2000

Event Filters

Event filters allow you to sift through the events in the event log, selecting only the events that meet your criteria. (Note that this is different from the discovery preferences event filter.) Event filters are most useful in event action plans (they allow you to select which events will trigger the actions in your event action plan).

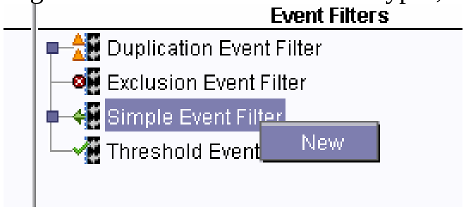
There are 2 ways to create an event filter:

- The hard way – creating an event filter from scratch
- The easy way – creating an event filter using an existing event as a template

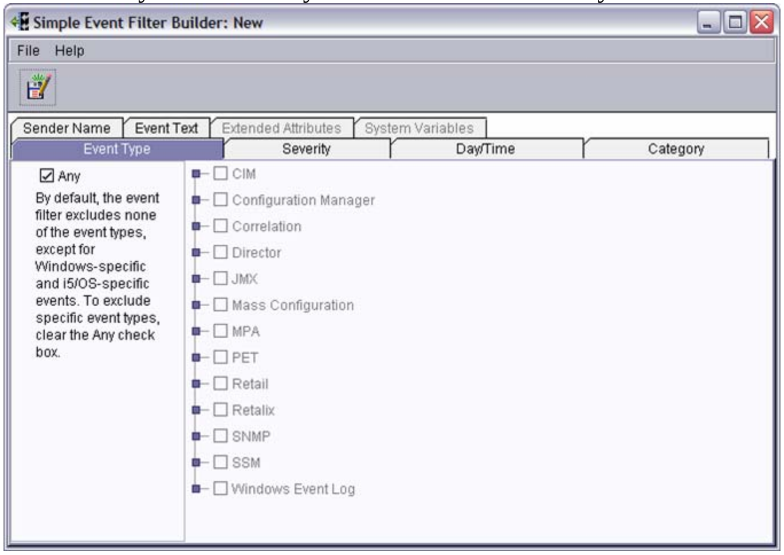
The Hard Way – creating an event filter from scratch

1. Double-click “Event Action Plans” in the tasks pane.

2. Right-click one of the event filter types, and select "New".



3. This allows you to manually define all the criteria for your event filter.

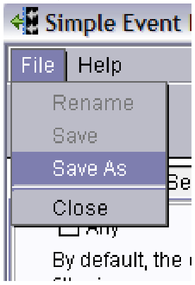


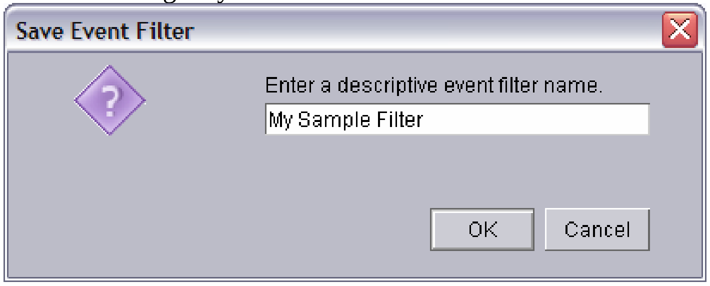
☑ Any

By default, the event filter excludes none of the event types, except for Windows-specific and i5/OS-specific events. To exclude specific event types, clear the Any check box.

□ CIM
□ Configuration Manager
□ Correlation
□ Director
□ JMX
□ Mass Configuration
□ MPA
□ PET
□ Retail
□ Retalix
□ SNMP
□ SSM
□ Windows Event Log

4. When you're done editing all the fields and selecting the criteria for your event filter, click "File / Save As" and give your filter a name.

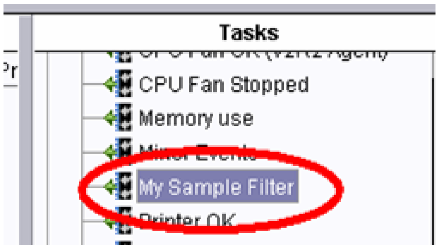




Enter a descriptive event filter name.

My Sample Filter

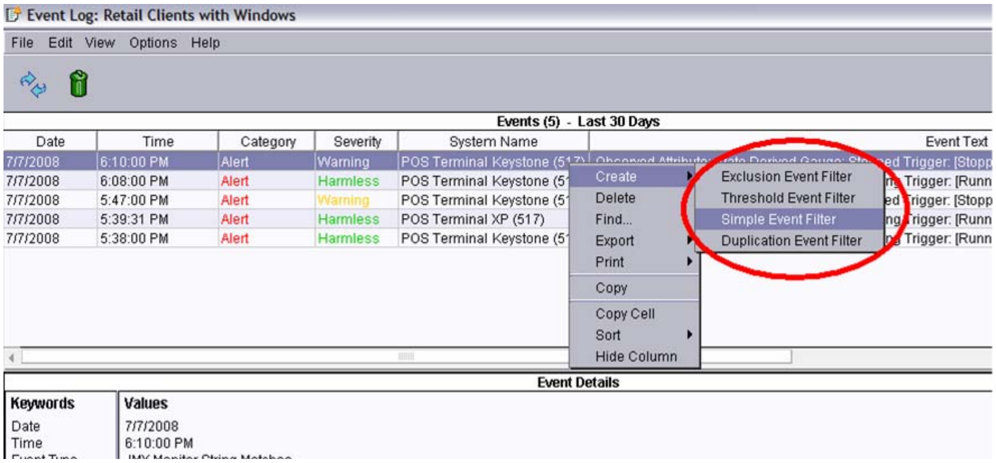
5. You will now see your event filter in the main Director console, under "Event Log".



6. You can drag-and-drop your new filter to a group, a managed object, or a selection of objects – this will display only the events that match your filter.

The Easy Way – creating an event filter using an existing event as a template

If you have an example of an event, you can right-click that event in the Event Log, and select "Create" to create a filter based on that event.



Events (5) - Last 30 Days

Date	Time	Category	Severity	System Name	Event Text
7/7/2008	6:10:00 PM	Alert	Warning	POS Terminal Keystone (517)	ed Trigger: [Stopp
7/7/2008	6:08:00 PM	Alert	Harmless	POS Terminal Keystone (51	Trigger: [Runn
7/7/2008	5:47:00 PM	Alert	Warning	POS Terminal Keystone (51	ed Trigger: [Stopp
7/7/2008	5:39:31 PM	Alert	Harmless	POS Terminal XP (517)	ng Trigger: [Runn
7/7/2008	5:38:00 PM	Alert	Harmless	POS Terminal Keystone (51	Trigger: [Runn

Event Details

Keywords	Values
Date	7/7/2008
Time	6:10:00 PM

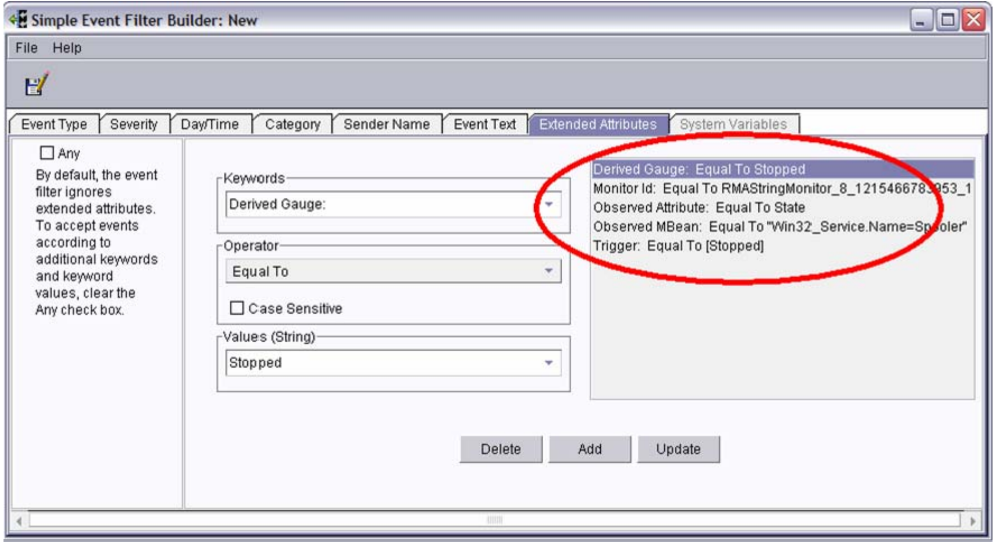
Types of Event Filters

- *Simple Event Filter* – Allows you to specify which events match the filter based on any event attributes (type, severity, text, etc). All other events are filtered out (i.e. ignored). This forms the basis for the other filter types.
- *Exclusion Event Filter* – Allows you to specify additional event types to exclude from your filter
- *Duplication Event Filter* – Allows you to ignore duplicate events (within a specified period of time)
- *Threshold Event Filter* – Allows you to require a certain number of duplicates before matching (within a specified period of time)

Event Filter Extended Attributes

Some events contain “extended attributes”, and you should always examine the extended attributes when editing your event filter.

Usually, you will want to remove any of the extended attributes that are highly specific (i.e. the “Monitor Id” is usually too specific for an event filter, so it should be removed).



☐ Any

By default, the event filter ignores extended attributes. To accept events according to additional keywords and keyword values, clear the Any check box.

Keywords: Derived Gauge:

Operator: Equal To

☐ Case Sensitive

Values (String): Stopped

Derived Gauge: Equal To Stopped
Monitor Id: Equal To RMAStringMonitor_8_1215466783953_1
Observed Attribute: Equal To State
Observed MBean: Equal To "Win32_Service.Name=Spooler"
Trigger: Equal To [Stopped]

Warning: It is very important to carefully examine the extended attributes for an event filter, and “Delete” any of the attributes that will prevent your filter from working in a more general case across many stores and managed objects.

Event Action Plans

The “Event Action Plans” task allows you to define how Director will react to events

To define an event action plan:

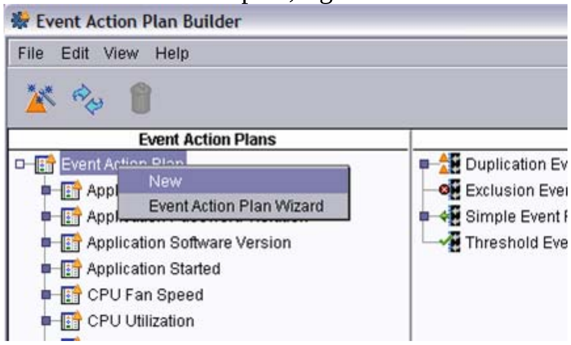
- First, define an event filter that matches the events you want to react to. You can test your event filter independently before creating the event action plan.
- Second, choose (and customize) the actions you want to execute in response to the event.
- Third, drag-and-drop to build your plan.

Event Action Plan Builder

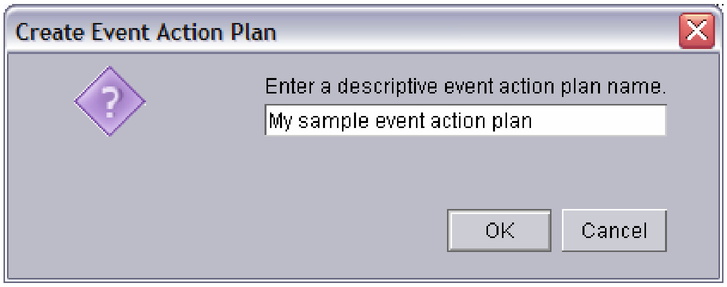
To build a new event action plan, use the event action plan builder as follows:

1. Launch the Event Action Plan builder by double-clicking on “Event Action Plans” in the Director tasks pane.

2. To start a new action plan, right-click “Event Action Plan” and select “New”.



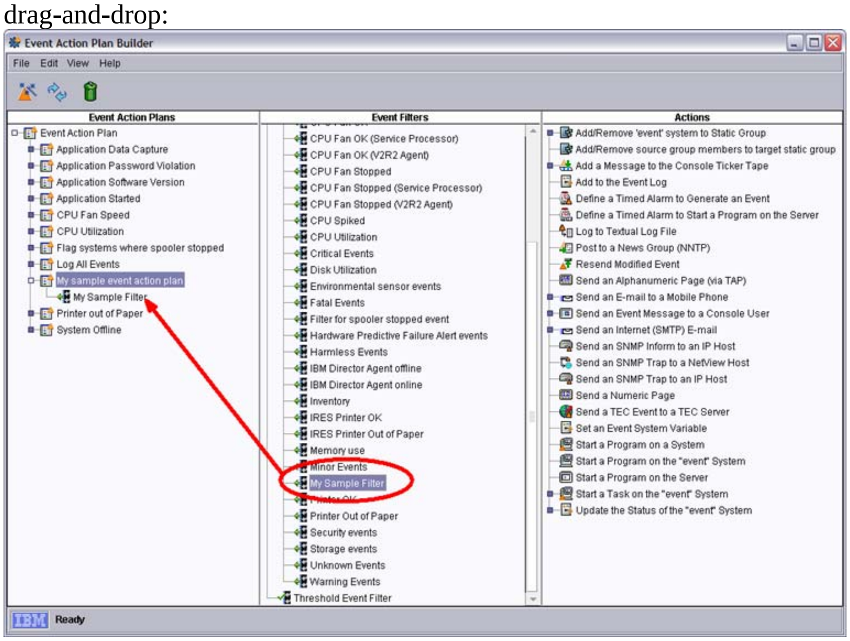
3. Give it a name and click OK.



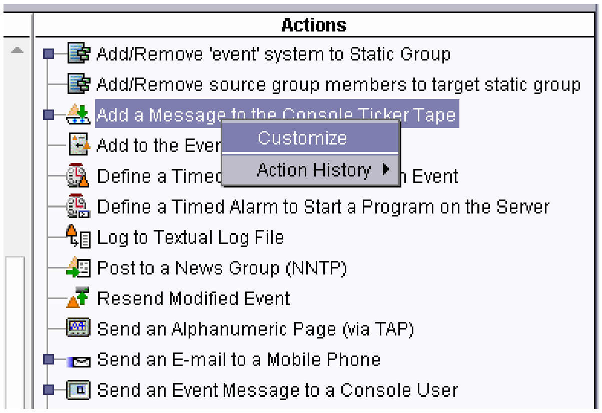
Enter a descriptive event action plan name.

My sample event action plan

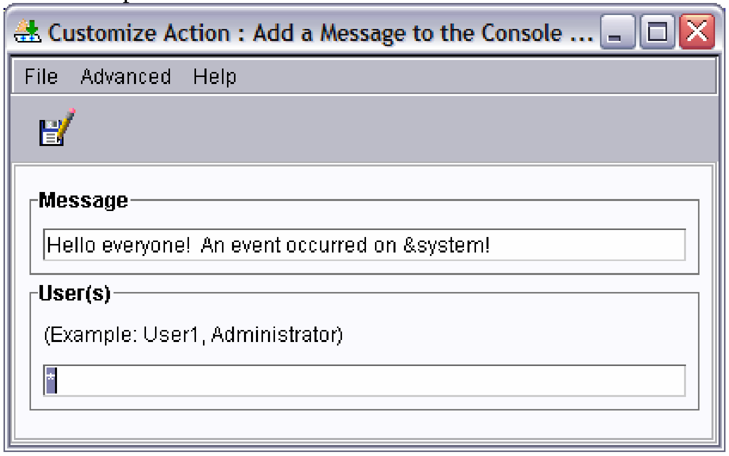
4. The next step is to add your event filter to the event action plan. To do that, just drag-and-drop:


Event Action Plan Builder
File Edit View Help
Event Action Plans
Event Action Plan
Application Data Capture
Application Password Violation
Application Software Version
Application Started
CPU Fan Speed
CPU Utilization
Flag systems where spooler stopped
Log All Events
My sample event action plan
My Sample Filter
Printer out of Paper
System Offline
Event Filters
CPU Fan OK (Service Processor)
CPU Fan OK (V2R2 Agent)
CPU Fan Stopped
CPU Fan Stopped (Service Processor)
CPU Fan Stopped (V2R2 Agent)
CPU Spiked
CPU Utilization
Critical Events
Disk Utilization
Environmental sensor events
Fatal Events
Filter for spooler stopped event
Hardware Predictive Failure Alert events
Harmless Events
IBM Director Agent offline
IBM Director Agent online
Inventory
IRES Printer OK
IRES Printer Out of Paper
Memory use
Minor Events
My Sample Filter
Printer OK
Printer Out of Paper
Security events
Storage events
Unknown Events
Warning Events
Threshold Event Filter
Actions
Add/Remove 'event' system to Static Group
Add/Remove source group members to target static group
Add a Message to the Console Ticker Tape
Add to the Event Log
Define a Timed Alarm to Generate an Event
Define a Timed Alarm to Start a Program on the Server
Log to Textual Log File
Post to a News Group (NNTP)
Resend Modified Event
Send an Alphanumeric Page (via TAP)
Send an E-mail to a Mobile Phone
Send an Event Message to a Console User
Send an Internet (SMTP) E-mail
Send an SNMP Inform to an IP Host
Send an SNMP Trap to a NetView Host
Send an SNMP Trap to an IP Host
Send a Numeric Page
Send a TEC Event to a TEC Server
Set an Event System Variable
Start a Program on a System
Start a Program on the "event" System
Start a Program on the Server
Start a Task on the "event" System
Update the Status of the "event" System
IBM
Ready

5. Next, choose an action from the list of actions on the right. Right-click the action and select “Customize”.


Actions
Add/Remove 'event' system to Static Group
Add/Remove source group members to target static group
Add a Message to the Console Ticker Tape
Add to the Even
Define a Timed
Event
Define a Timed Alarm to Start a Program on the Server
Log to Textual Log File
Post to a News Group (NNTP)
Resend Modified Event
Send an Alphanumeric Page (via TAP)
Send an E-mail to a Mobile Phone
Send an Event Message to a Console User
Customize
Action History

6. Edit the action parameters (see example screenshot below) – each action type will have different required parameters. Refer to the IBM Director redbook for help with these parameters.



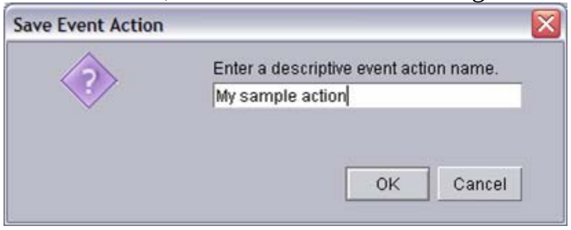
Message

Hello everyone! An event occurred on &system!

User(s)

(Example: User1, Administrator)

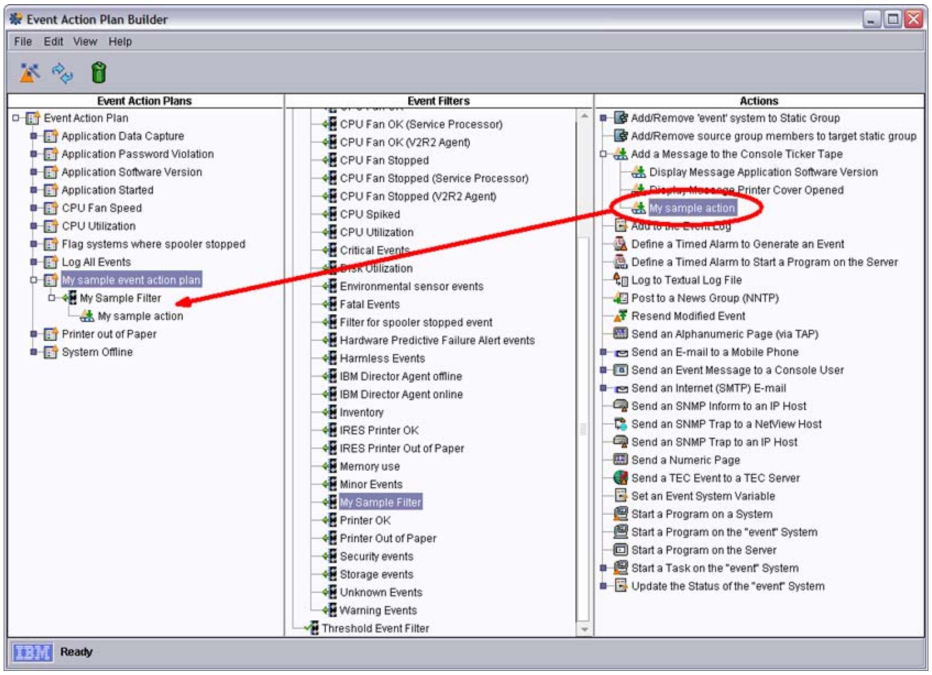
7. When finished, click “File / Save As” and give it a name.



Enter a descriptive event action name.

My sample action

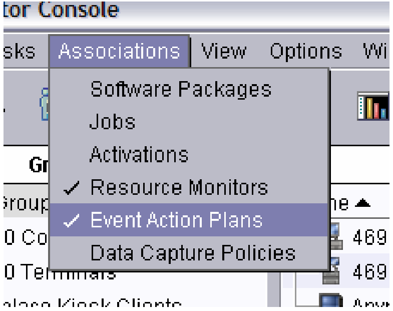
8. Finally, drag-and-drop your new action to the event action plan


Event Action Plan Builder
File Edit View Help
Event Action Plans
Event Action Plan
Application Data Capture
Application Password Violation
Application Software Version
Application Started
CPU Fan Speed
CPU Utilization
Flag systems where spooler stopped
Log All Events
My sample event action plan
My Sample Filter
My sample action
Printer out of Paper
System Offline
Event Filters
CPU Fan OK (Service Processor)
CPU Fan OK (V2R2 Agent)
CPU Fan Stopped
CPU Fan Stopped (Service Processor)
CPU Fan Stopped (V2R2 Agent)
CPU Spiked
CPU Utilization
Critical Events
Disk Utilization
Environmental sensor events
Fatal Events
Filter for spooler stopped event
Hardware Predictive Failure Alert events
Harmless Events
IBM Director Agent offline
IBM Director Agent online
Inventory
IRES Printer OK
IRES Printer Out of Paper
Memory use
Minor Events
My Sample Filter
Printer OK
Printer Out of Paper
Security events
Storage events
Unknown Events
Warning Events
Threshold Event Filter
Actions
Add/Remove 'event' system to Static Group
Add/Remove source group members to target static group
Add a Message to the Console Ticker Tape
Display Message Application Software Version
Display Message Printer Cover Opened
My sample action
Add to the Event Log
Define a Timed Alarm to Generate an Event
Define a Timed Alarm to Start a Program on the Server
Log to Textual Log File
Post to a News Group (NNTP)
Resend Modified Event
Send an Alphanumeric Page (via TAP)
Send an E-mail to a Mobile Phone
Send an Event Message to a Console User
Send an Internet (SMTP) E-mail
Send an SNMP Inform to an IP Host
Send an SNMP Trap to a NetView Host
Send an SNMP Trap to an IP Host
Send a Numeric Page
Send a TEC Event to a TEC Server
Set an Event System Variable
Start a Program on a System
Start a Program on the "event" System
Start a Program on the Server
Start a Task on the "event" System
Update the Status of the "event" System
IBM
Ready

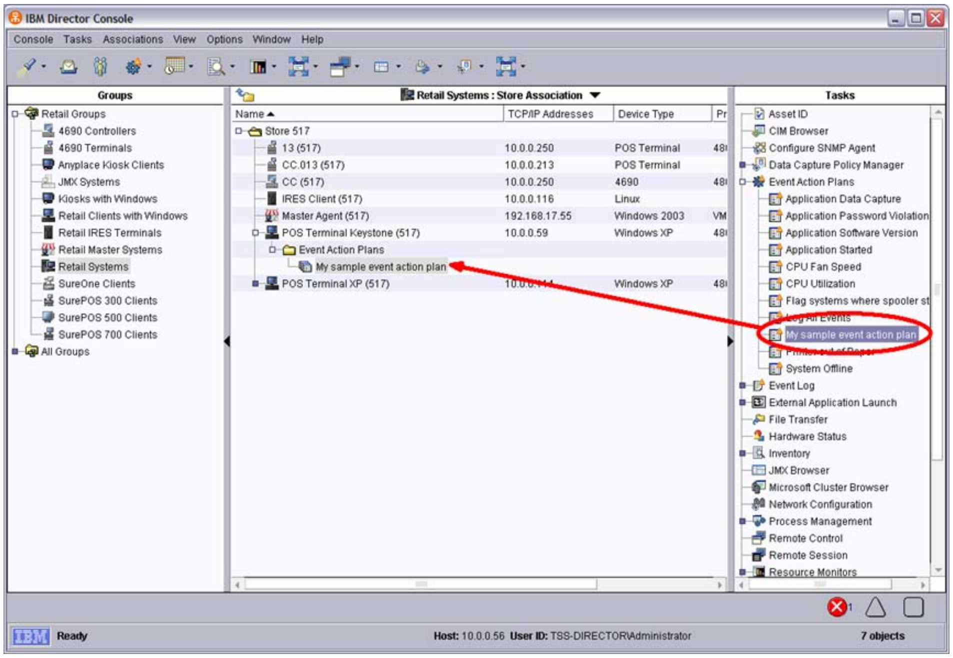
Associating the Event Action Plan

Now that you've created an event action plan, you still need to "associate" it to a group, a managed object, or a selection of managed objects. Do this in the main Director console.

1. First, make sure "Event Action Plans" is checked in the "Associations" menu.



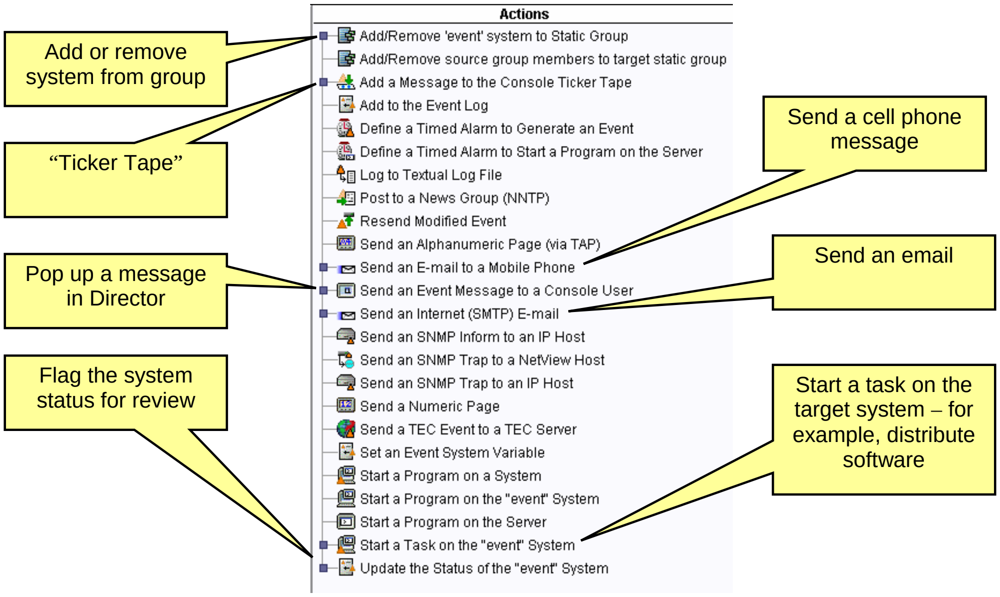
2. Drag-and-drop the event action plan to associate it to a managed object, group, or selection of multiple managed objects or groups.



Name ▲	TCP/IP Addresses	Device Type	Pr
Store 517			
13 (517)	10.0.0.250	POS Terminal	48
CC.013 (517)	10.0.0.213	POS Terminal	
CC (517)	10.0.0.250	4690	48
IRES Client (517)	10.0.0.116	Linux	
Master Agent (517)	192.168.17.55	Windows 2003	VM
POS Terminal Keystone (517)	10.0.0.59	Windows XP	48
Event Action Plans			
My sample event action plan			
POS Terminal XP (517)	10.0.0.144	Windows XP	48

Possible Actions

To get an idea of the actions that are available to be used in your event action plans, you can browse the right-hand side of the event action plan builder, as shown below.



Actions

- Add/Remove 'event' system to Static Group
- Add/Remove source group members to target static group
- Add a Message to the Console Ticker Tape
- Add to the Event Log
- Define a Timed Alarm to Generate an Event
- Define a Timed Alarm to Start a Program on the Server
- Log to Textual Log File
- Post to a News Group (NNTP)
- Resend Modified Event
- Send an Alphanumeric Page (via TAP)
- Send an E-mail to a Mobile Phone
- Send an Event Message to a Console User
- Send an Internet (SMTP) E-mail
- Send an SNMP Inform to an IP Host
- Send an SNMP Trap to a NetView Host
- Send an SNMP Trap to an IP Host
- Send a Numeric Page
- Send a TEC Event to a TEC Server
- Set an Event System Variable
- Start a Program on a System
- Start a Program on the "event" System
- Start a Program on the Server
- Start a Task on the "event" System
- Update the Status of the "event" System

Add or remove system from group

“Ticker Tape”

Pop up a message in Director

Flag the system status for review

Send a cell phone message

Send an email

Start a task on the target system – for example, distribute software

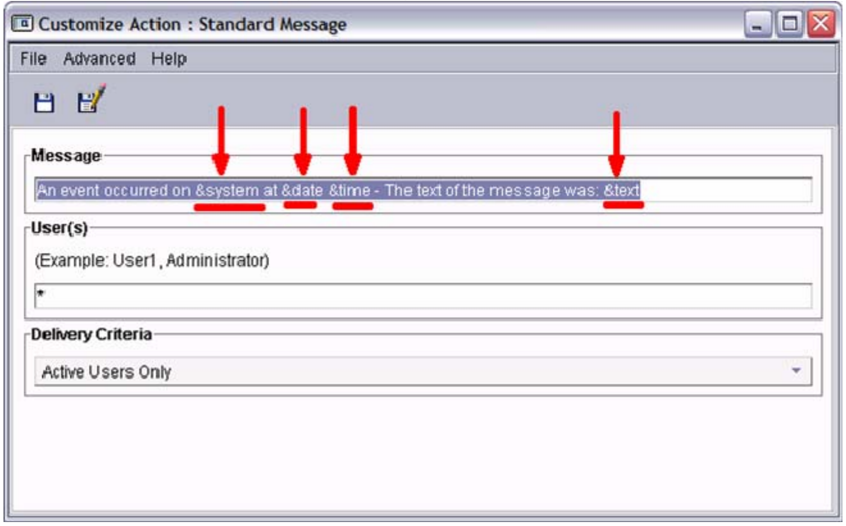
Event Data Substitution Variables

When customizing the actions in an event action plan, you can use variables to represent data from the event that triggered the action.

For example, the text of your email message could be "A severe error occurred on &system". When Director sends your email, it will replace "&system" with the name of the managed object that generated the event. (Note: be careful not to add punctuation marks immediately after a variable substitution.)

For a detailed listing of possible variables, see "event data substitution variables" in the Redbook for IBM Director.

Another example – sending a message to a Director console user:



Message

An event occurred on &system at &date &time - The text of the message was: &text

User(s)

(Example: User1 , Administrator)

*

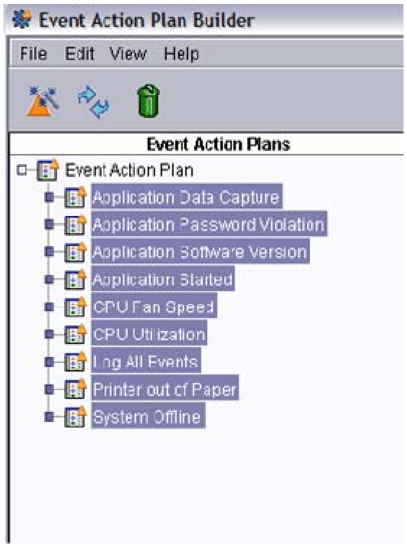
Delivery Criteria

Active Users Only

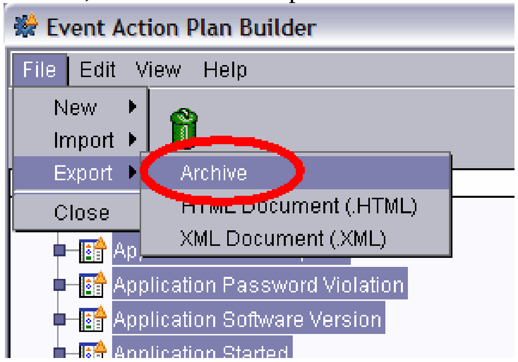
Importing/Exporting Event Action Plans

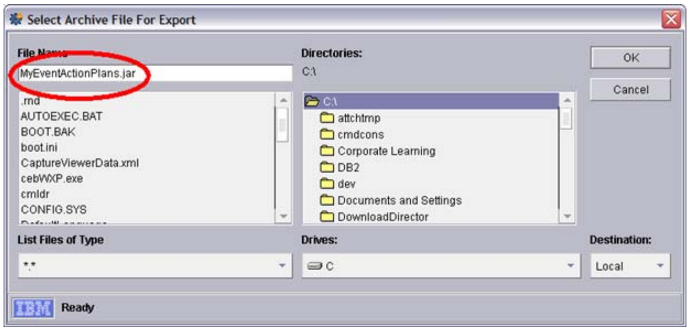
Event action plans can be imported/exported (along with any necessary event filters) using the "File" menu in the Event Action Plan builder. This is useful for saving your work and/or giving your EAP's to a customer or partner to replicate on a different Director Server.

1. First, select the action plans you want to export



2. Second, choose “File / Export / Archive”




Select Archive File For Export

File Name: MyEventActionPlans.jar

Directories: C:\

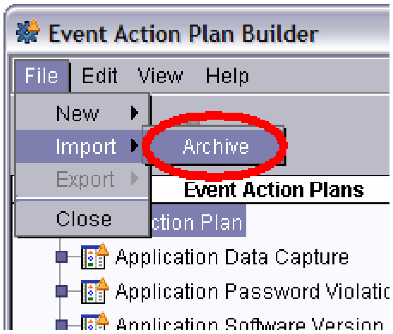
List Files of Type: *.*

Drives: C

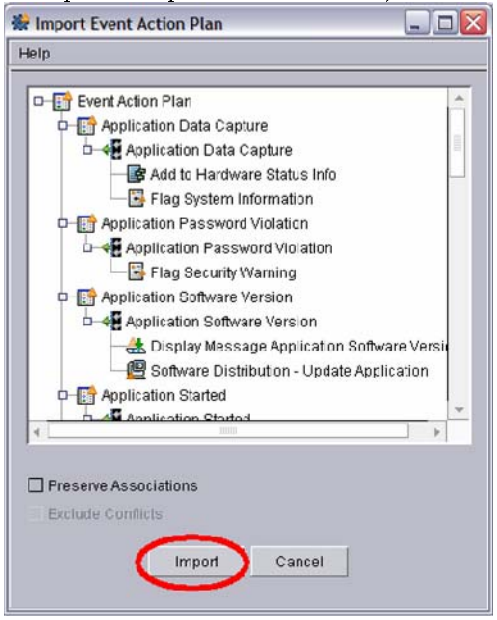
Destination: Local

Ready

3. Later, you can import those event action plans by selecting “File / Import”



4. Sometimes you might need to check "Exclude Conflicts". (Otherwise, you may end up with duplicate event filters.)



Event Management for 4690 OS

Events logged to the 4690 event logs (including system and application events) are forwarded to RMA and are available within the IBM Director Console. You can use event action plans to react to specific events from 4690.

There are many 4690 events of potential interest. The ones most important to a particular retailer vary depending on the 4690 features used and how the stores are operated. The system events that might be logged are listed and described in the "4690 Operating System Messages Guide", which can be found here: http://www2.clearlake.ibm.com/store/support/html/pubs.html#4690v6r1

A review of messages listed in that document might suggest events of particular interest. Examining current 4690 event logs might also identify the types of events experienced in a particular environment. Examination of problem histories might be a good source of events of interest.

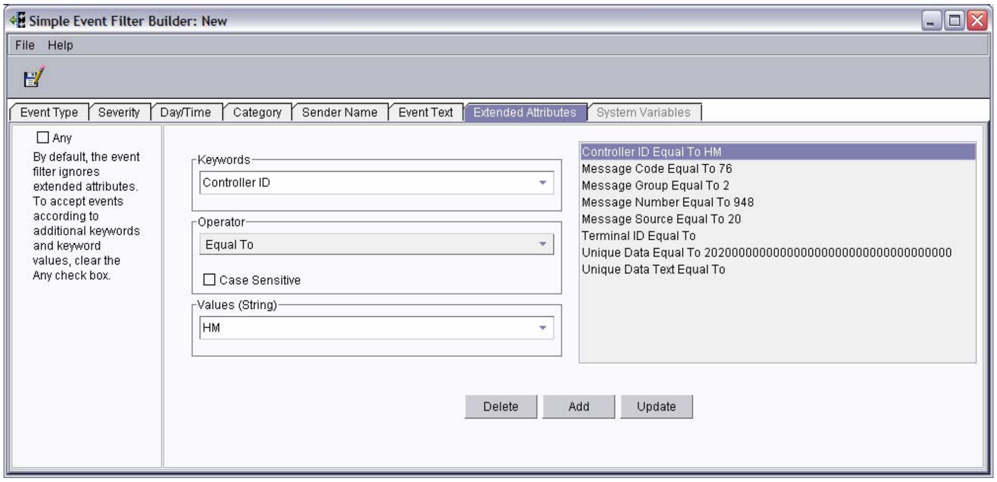
It shouldn't be necessary to have event action plans for all events that suggest a problem. Frequently, problems log multiple events providing different details of what occurred. Create event action plans for events that are representative of the types of problems of interest. Then, you can investigate the event log to get more details for the problem that occurred.

The following is a list of 4690 controller events that might be used to trigger Event Action Plans. Some or all of these might make a good starter set. Add others to suit your particular interests and needs.

Examples:

- W889 FTP connection from 9.44.166.206
- W893 Telnet connection from 9.44.166.206
- W619 PROGRAM COMMAND WAS STARTED
- W312 CHECKOUT SCANNER PROBLEM
- W598 STORE CONTROLLER STORAGE DUMP OCCURRED
- W599 NORMAL STORE CONTROLLER IPL
- W610 PROGRAM CANCELED DUE TO INSUFFICIENT STORAGE
- W619 PROGRAM *xxxxxxxx* WAS STARTED
- W620 PROGRAM *xxxxxxxx* HAS ENDED
- W638 APPLY SOFTWARE MAINTENANCE FAILED
- W650 PROGRAM *xxxxxxxx* HAS ENDED ABNORMALLY
- W762 TERMINAL *xxx* DOES NOT RESPOND
- W806 HOST COMMUNICATIONS PROBLEM ON LINE *xxxxxxxx*
- W901 NO ACTING MASTER CONTROLLER FOUND
- W902 NO ACTING FILE SERVER CONTROLLER FOUND
- W907 UPDATE FROM ACTING FILE SERVER WAS UNSUCCESSFUL
- W947 CONTROLLER *xx* HAS LEFT LAN SYSTEM

On 4690 V6, all events include a number of "extended attributes", as shown in the following example:



□ Any

By default, the event filter ignores extended attributes. To accept events according to additional keywords and keyword values, clear the Any check box.

Keywords: Controller ID

Operator: Equal To

□ Case Sensitive

Values (String): HM

Controller ID Equal To HM
Message Code Equal To 76
Message Group Equal To 2
Message Number Equal To 948
Message Source Equal To 20
Terminal ID Equal To
Unique Data Equal To 2020000000000000000000000000000000000000
Unique Data Text Equal To

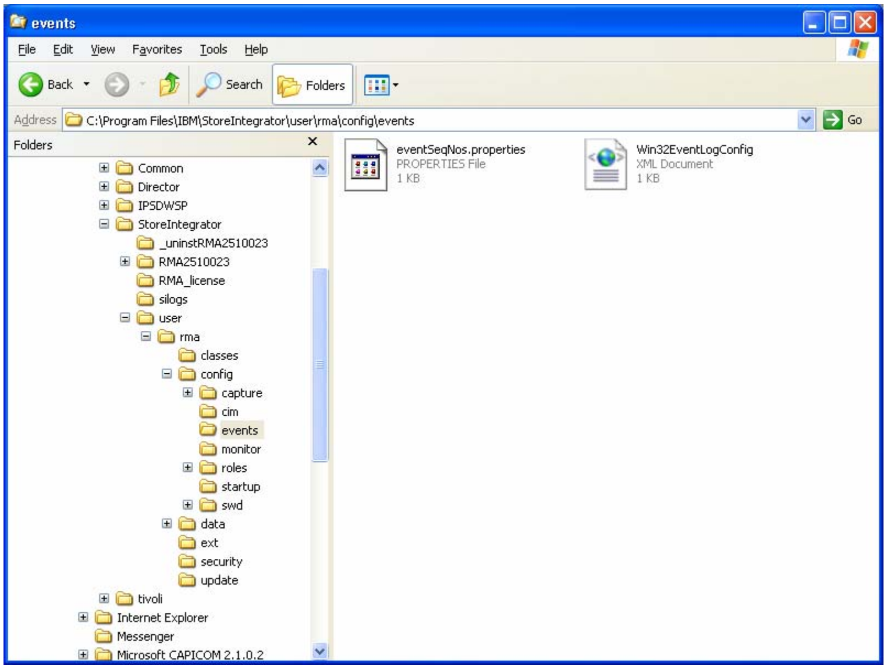
These extended attributes allow you to be **very specific** when creating your event filter – i.e. you can select only events that come from a particular controller ID, or from a particular application (source), from a specific terminal ID, or with a particular message number.

In many cases, you will probably need to "Delete" most of these extended attributes from your event filters – otherwise, your event filters for 4690 will be too specific and will not apply broadly to all the controllers, terminals, and event sources that you want to manage.

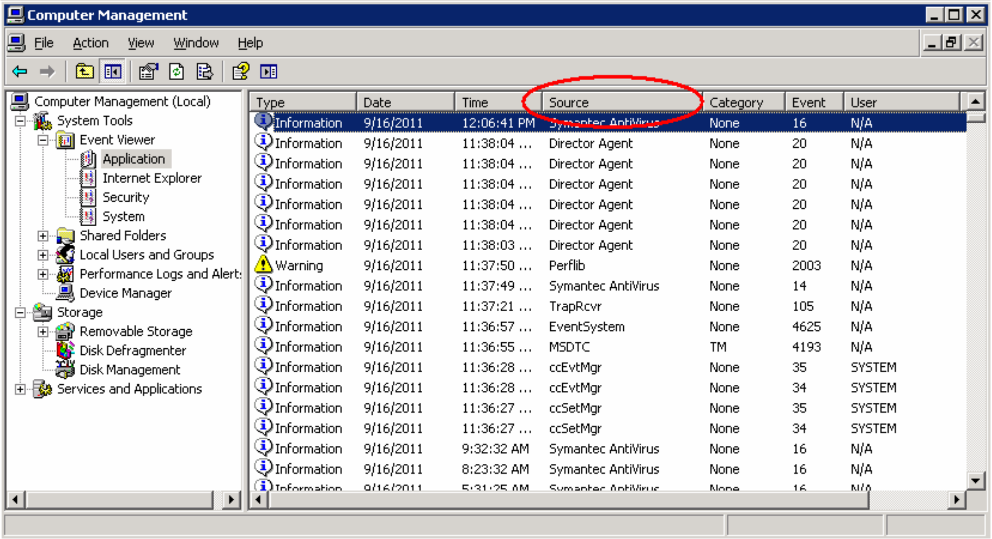
Using the Windows Event Log

RMA has the ability to forward events from any of the Windows Event Logs (Application, Security, or System) up to IBM Director. Due to resource concerns and the high volume of events in the Windows Event Log, the agents must be configured to forward the events you would like to see rather than simply forwarding all events in the logs. Once the events are forwarded you can use event action plans to react to specific events from 4690.

In order to configure which Windows Event Log events will get forwarded through RMA, you need to set up the Win32EventLogConfig.xml in the folder "C:\Program Files\IBM\StoreIntegrator\user\rma\config\events".



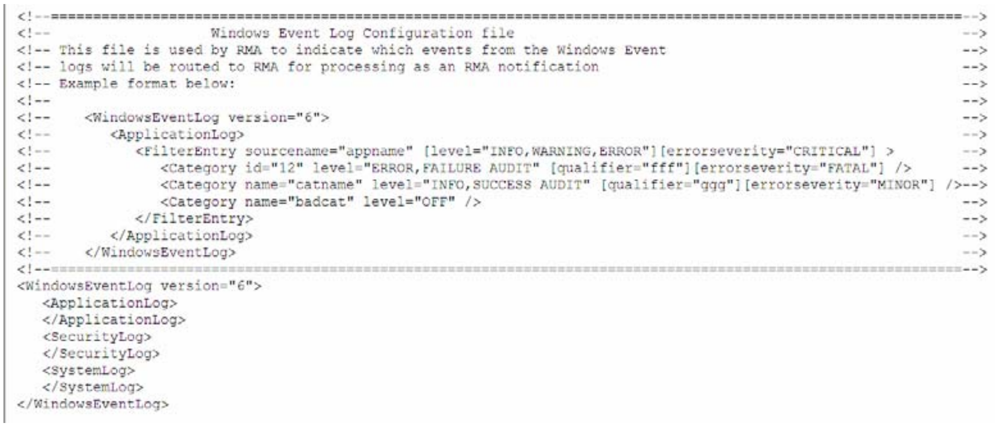
Prior to setting up the Win32EventLogConfig.xml, you should look at the Windows Event Log to determine which events you would like to monitor. Particularly you need to make note of the "Source" of the events in the event log. Other event details such as the "Category" and "Event" can be optionally used to further narrow the events that will be forwarded.



Type	Date	Time	Source	Category	Event	User
Information	9/16/2011	12:06:41 PM	Symantec AntiVirus	None	16	N/A
Information	9/16/2011	11:38:04 ...	Director Agent	None	20	N/A
Information	9/16/2011	11:38:04 ...	Director Agent	None	20	N/A
Information	9/16/2011	11:38:04 ...	Director Agent	None	20	N/A
Information	9/16/2011	11:38:04 ...	Director Agent	None	20	N/A
Information	9/16/2011	11:38:04 ...	Director Agent	None	20	N/A
Information	9/16/2011	11:38:03 ...	Director Agent	None	20	N/A
Warning	9/16/2011	11:37:50 ...	Perflib	None	2003	N/A
Information	9/16/2011	11:37:49 ...	Symantec AntiVirus	None	14	N/A
Information	9/16/2011	11:37:21 ...	TrapRcvr	None	105	N/A
Information	9/16/2011	11:36:57 ...	EventSystem	None	4625	N/A
Information	9/16/2011	11:36:55 ...	MSDTC	TM	4193	N/A
Information	9/16/2011	11:36:28 ...	ccEvtMgr	None	35	SYSTEM
Information	9/16/2011	11:36:28 ...	ccEvtMgr	None	34	SYSTEM
Information	9/16/2011	11:36:27 ...	ccSetMgr	None	35	SYSTEM
Information	9/16/2011	11:36:27 ...	ccSetMgr	None	34	SYSTEM
Information	9/16/2011	9:32:32 AM	Symantec AntiVirus	None	16	N/A
Information	9/16/2011	8:23:32 AM	Symantec AntiVirus	None	16	N/A
Information	9/16/2011	5:31:25 AM	Symantec AntiVirus	None	16	N/A

Once you have identified the events that you wish to forward, open up the Win32EventLogConfig.xml in a text editor.

The default file looks like the following:



```
<!--============================================================================================================-->
<!--                   Windows Event Log Configuration file                                                     -->
<!-- This file is used by RMA to indicate which events from the Windows Event                                   -->
<!-- logs will be routed to RMA for processing as an RMA notification                                           -->
<!-- Example format below:                                                                                      -->
<!--                                                                                                            -->
<!--    <WindowsEventLog version="6">                                                                           -->
<!--       <ApplicationLog>                                                                                     -->
<!--          <FilterEntry sourcename="appname" [level="INFO,WARNING,ERROR"][errorseverity="CRITICAL"] >        -->
<!--             <Category id="12" level="ERROR,FAILURE AUDIT" [qualifier="fff"][errorseverity="FATAL"] />      -->
<!--             <Category name="catname" level="INFO,SUCCESS AUDIT" [qualifier="ggg"][errorseverity="MINOR"] />-->
<!--             <Category name="badcat" level="OFF" />                                                         -->
<!--          </FilterEntry>                                                                                    -->
<!--       </ApplicationLog>                                                                                    -->
<!--    </WindowsEventLog>                                                                                      -->
<!--============================================================================================================-->
<WindowsEventLog version="6">
   <ApplicationLog>
   </ApplicationLog>
   <SecurityLog>
   </SecurityLog>
   <SystemLog>
   </SystemLog>
</WindowsEventLog>
```

Note: This file is **case-sensitive** so be sure to maintain the correct capitalizations when entering the xml tags.

The file definition will always begin with a <WindowEventLog version=”6’> tag, and will always end with the </WindowsEventLog> tag.

In between, you can specify <ApplicationLog>, <SecurityLog>, or <SystemLog> tags in order to declare events from each of the logs.

Under each <xxxxxxxxLog> tag, you declare the specific events that you would like to forward from that log.

Each event type that will be forwarded is declared as a “Filter Entry”. Each Filter Entry must specify a “sourcename” (the “Source” column from the Windows Event Log – this is case sensitive), and can optionally specify a “level” or “error severity.”

The optional “level” tag indicates which specific event severities you would like to forward through the agent. Options for this field are OFF, INFO, WARNING, ERROR, SUCCESS AUDIT, and FAILURE AUDIT.

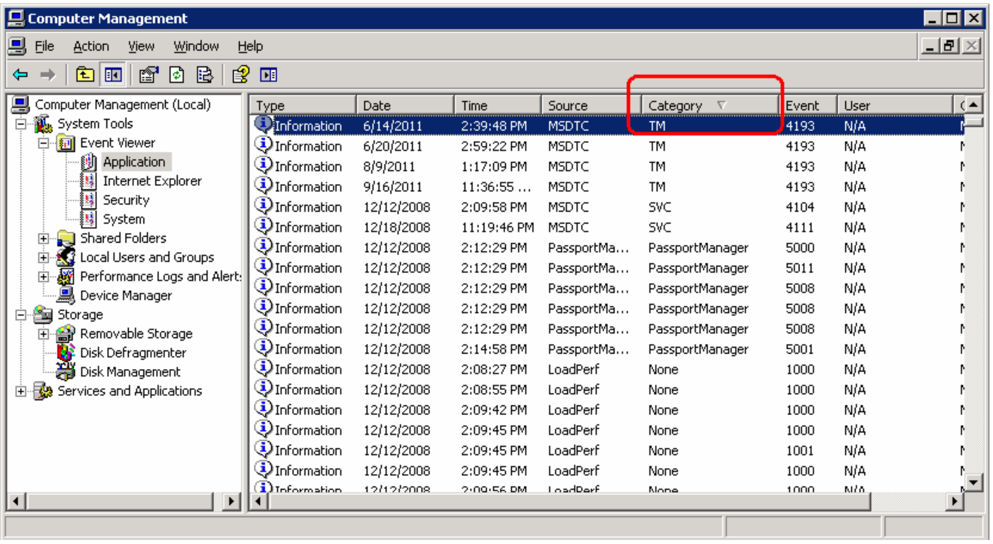
For example, if you only wanted to forward WARNING and ERROR events from the “Symantec Antivirus” source, you would add the following Filter Entry:

```
<FilterEntry sourcename="Symantec Antivirus" level=”WARNING,ERROR” />
```

The optional “error severity” tag specifics what severity you would like the events to show up in IBM Director as. So, even if the event was listed as “INFO” in the Windows

Event Log, you could still have it appear in IBM Director as a “FATAL” error if you wish.

You can also specify an optional “Category” tag if you would like to narrow down the events you are interested in from a particular source. Many applications have several categories of events.



Type	Date	Time	Source	Category	Event	User
Information	6/14/2011	2:39:48 PM	MSDTC	TM	4193	N/A
Information	6/20/2011	2:59:22 PM	MSDTC	TM	4193	N/A
Information	8/9/2011	1:17:09 PM	MSDTC	TM	4193	N/A
Information	9/16/2011	11:36:55 …	MSDTC	TM	4193	N/A
Information	12/12/2008	2:09:58 PM	MSDTC	SVC	4104	N/A
Information	12/18/2008	11:19:46 PM	MSDTC	SVC	4111	N/A
Information	12/12/2008	2:12:29 PM	PassportMa…	PassportManager	5000	N/A
Information	12/12/2008	2:12:29 PM	PassportMa…	PassportManager	5011	N/A
Information	12/12/2008	2:12:29 PM	PassportMa…	PassportManager	5008	N/A
Information	12/12/2008	2:12:29 PM	PassportMa…	PassportManager	5008	N/A
Information	12/12/2008	2:12:29 PM	PassportMa…	PassportManager	5008	N/A
Information	12/12/2008	2:14:58 PM	PassportMa…	PassportManager	5001	N/A
Information	12/12/2008	2:08:27 PM	LoadPerf	None	1000	N/A
Information	12/12/2008	2:08:55 PM	LoadPerf	None	1000	N/A
Information	12/12/2008	2:09:42 PM	LoadPerf	None	1000	N/A
Information	12/12/2008	2:09:45 PM	LoadPerf	None	1000	N/A
Information	12/12/2008	2:09:45 PM	LoadPerf	None	1001	N/A
Information	12/12/2008	2:09:45 PM	LoadPerf	None	1000	N/A
Information	12/12/2008	2:09:56 PM	LoadPerf	None	1000	N/A

Categories in the Windows Event Log can either be specified as String values (ie, “PassportManager” above), or numerical values. If you specify a Category object, you must specify either a “name” tag (for String values) or an “id” tag (for Numerical values) as well as the “level” and “qualifier” tags. Optionally you can also specify an “error severity” tag.

The “level” and “error severity” tags work the same for “Category” declarations as they did for “Event Filter” declarations. The “qualifier” tag can be any text you want and will be used to identify the event type for that specific Category when it reaches IBM Director.

For example, consider the following declarations in the configuration file:

```
<WindowsEventLog>
<ApplicationLog>
            <FilterEntry sourcename="MyRetailApp" level="ERROR" />
                    <Category id="1" qualifier="Printer" level="WARNING,ERROR" errorseverity="CRITICAL" />
            </FilterEntry>
</ApplicationLog>
</WindowsEventLog>
```

That declaration would cause RMA to forward all “ERROR” events from the “MyRetailApp” source and all “WARNING” and “ERROR” events from the “1” category of “MyRetailApp”. Events coming from the “1” category would appear in IBM

Director as “WindowsEventLog.Application.MyRetailApp.Printer” event types and would have CRITICAL error severities.

Example: Create a Custom Group for Agents Offline

There are many scenarios where it is desirable to create a custom group that is automatically populated (i.e. systems are added to and removed from the group automatically). In this example, we’ll create a custom group called “POS Systems Offline”, and we’ll automatically add and remove systems to the group when an online or offline event occurs. This allows the system administrator to go to a single place in the Director UI to determine exactly which systems are currently offline.

This same concept can be applied to many different situations; this is just one example of how a custom group can be used in conjunction with event action plans that add/remove members from the group based on events that occur.

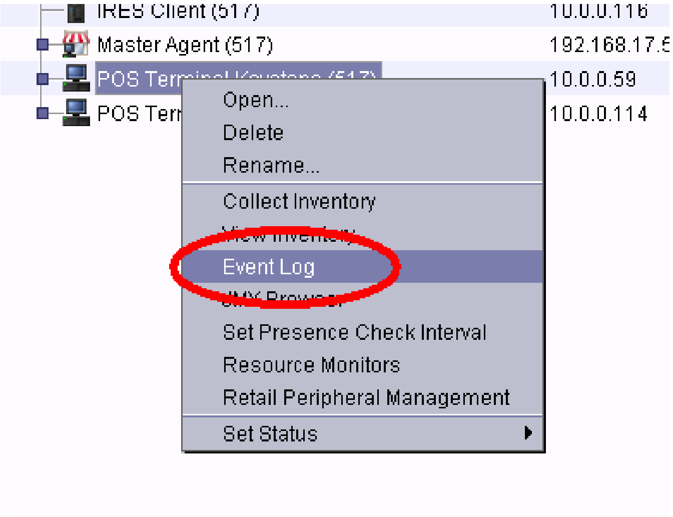
This example demonstrates:

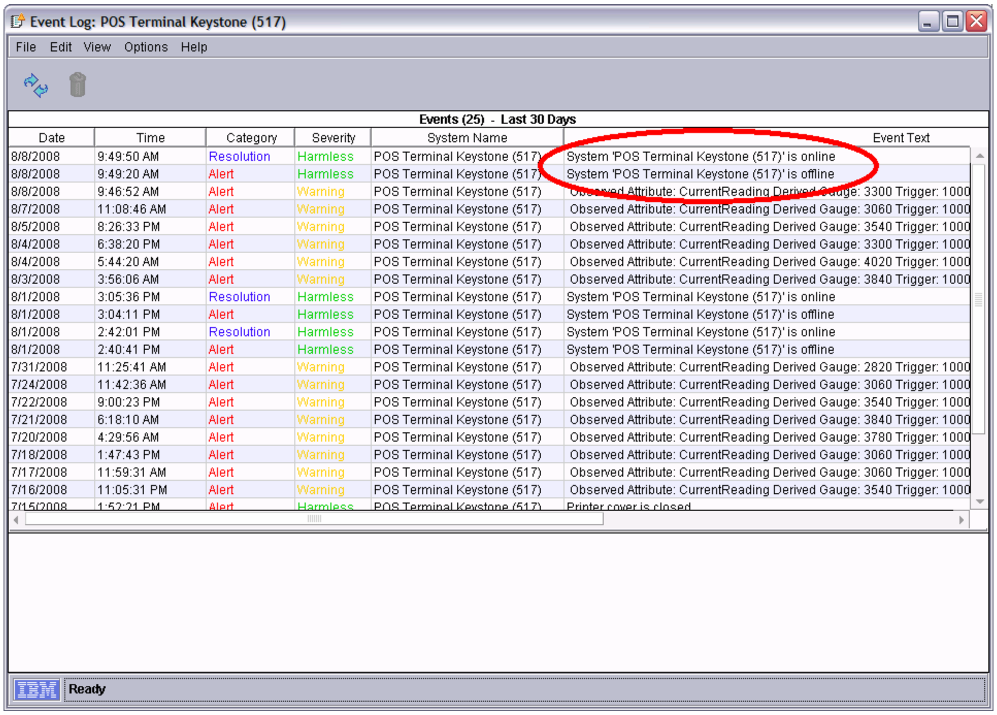
- Static custom groups
- Event filters
- Event action plans

Steps:

1. Since the easiest way to create an event filter is to first find an example of the events you want to filter, start by stopping and restarting an agent to get the offline/online events. To do that:
    - First, stop any general agent using the command “net stop RemoteMgmtAgent” (for Windows).
    - Wait 30 seconds or so, then restart the agent using the command “net start RemoteMgmtAgent”.

2. Right-click the system that went offline, and select “Event Log”. When the event log appears, the most recent 2 events should be offline and online events.

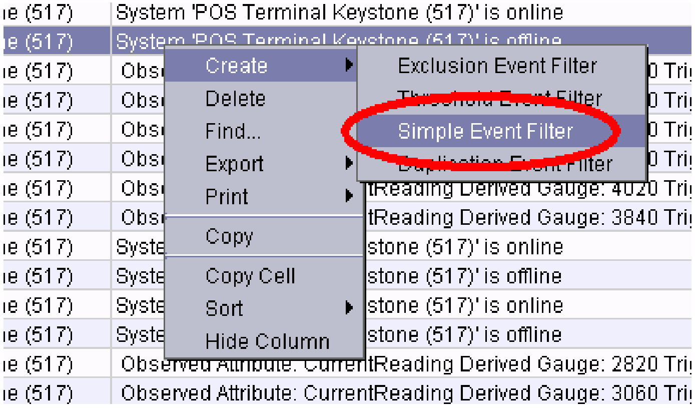




Events (25) - Last 30 Days

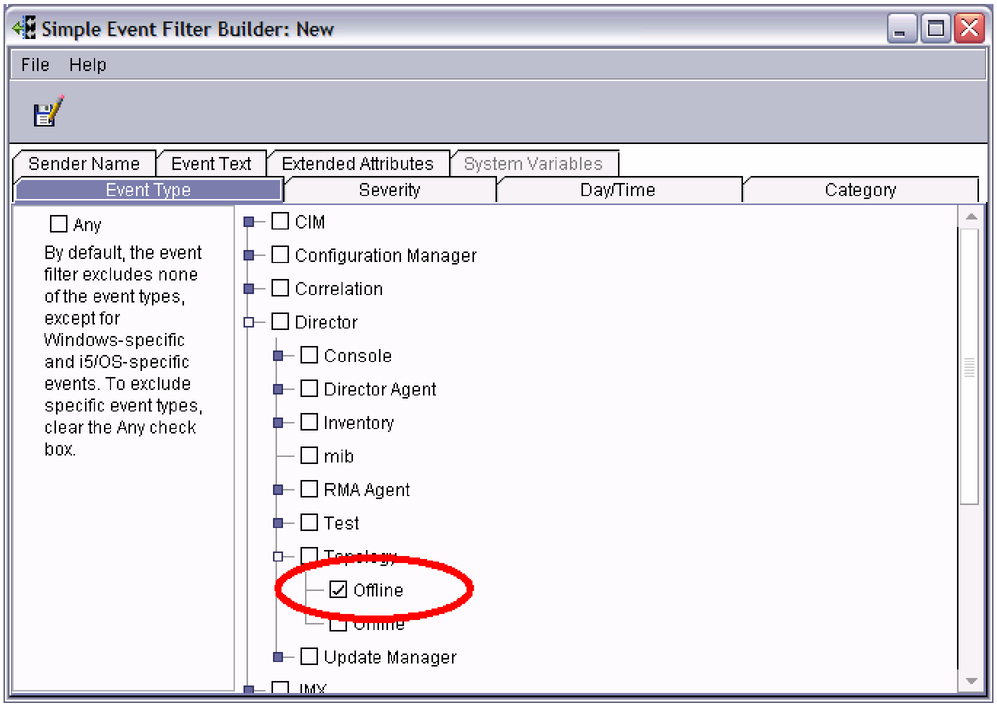
Date	Time	Category	Severity	System Name	Event Text
8/8/2008	9:49:50 AM	Resolution	Harmless	POS Terminal Keystone (517)	System 'POS Terminal Keystone (517)' is online
8/8/2008	9:49:20 AM	Alert	Harmless	POS Terminal Keystone (517)	System 'POS Terminal Keystone (517)' is offline
8/8/2008	9:46:52 AM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: CurrentReading Derived Gauge: 3300 Trigger: 1000
8/7/2008	11:08:46 AM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: CurrentReading Derived Gauge: 3060 Trigger: 1000
8/5/2008	8:26:33 PM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: CurrentReading Derived Gauge: 3540 Trigger: 1000
8/4/2008	6:38:20 PM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: CurrentReading Derived Gauge: 3300 Trigger: 1000
8/4/2008	5:44:20 AM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: CurrentReading Derived Gauge: 4020 Trigger: 1000
8/3/2008	3:56:06 AM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: CurrentReading Derived Gauge: 3840 Trigger: 1000
8/1/2008	3:05:36 PM	Resolution	Harmless	POS Terminal Keystone (517)	System 'POS Terminal Keystone (517)' is online
8/1/2008	3:04:11 PM	Alert	Harmless	POS Terminal Keystone (517)	System 'POS Terminal Keystone (517)' is offline
8/1/2008	2:42:01 PM	Resolution	Harmless	POS Terminal Keystone (517)	System 'POS Terminal Keystone (517)' is online
8/1/2008	2:40:41 PM	Alert	Harmless	POS Terminal Keystone (517)	System 'POS Terminal Keystone (517)' is offline
7/31/2008	11:25:41 AM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: CurrentReading Derived Gauge: 2820 Trigger: 1000
7/24/2008	11:42:36 AM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: CurrentReading Derived Gauge: 3060 Trigger: 1000
7/22/2008	9:00:23 PM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: CurrentReading Derived Gauge: 3540 Trigger: 1000
7/21/2008	6:18:10 AM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: CurrentReading Derived Gauge: 3840 Trigger: 1000
7/20/2008	4:29:56 AM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: CurrentReading Derived Gauge: 3780 Trigger: 1000
7/18/2008	1:47:43 PM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: CurrentReading Derived Gauge: 3060 Trigger: 1000
7/17/2008	11:59:31 AM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: CurrentReading Derived Gauge: 3060 Trigger: 1000
7/16/2008	11:05:31 PM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: CurrentReading Derived Gauge: 3540 Trigger: 1000
7/15/2008	1:52:21 PM	Alert	Harmless	POS Terminal Keystone (517)	Printer cover is closed

3. Now, create an event filter for each of these two events. To do that, start by right-clicking the "offline" event, and select "Create → Simple Event Filter".

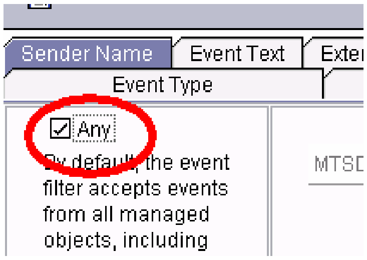


ie (517) | System 'POS Terminal Keystone (517)' is online
e (517) | System 'POS Terminal Keystone (517)' is offline
Create
Delete
Find...
Export
Print
Copy
Copy Cell
Sort
Hide Column
Exclusion Event Filter
Threshold Event Filter
Simple Event Filter
Duplication Event Filter
ie (517) | Observed Attribute: CurrentReading Derived Gauge: 2820 Tri
ie (517) | Observed Attribute: CurrentReading Derived Gauge: 3060 Tri

4. Next, do the following:
   - On the "Event Type" tab, make sure that the correct event type is selected ("Director.Topology.Offline")
   - On the "Sender Name" tab, check "Any".
   - On the "Event Text" tab, check "Any".

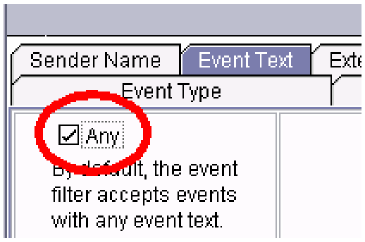


By default, the event filter excludes none of the event types, except for Windows-specific and i5/OS-specific events. To exclude specific event types, clear the Any check box.



☑ Any

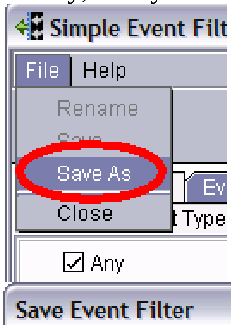
By default, the event filter accepts events from all managed objects, including

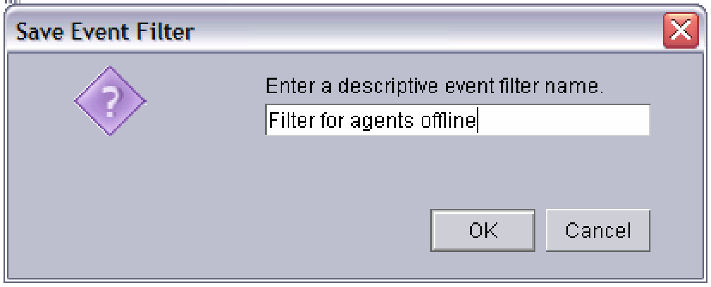


☑ Any

By default, the event filter accepts events with any event text.

5. Finally, save your event filter and give it a name.



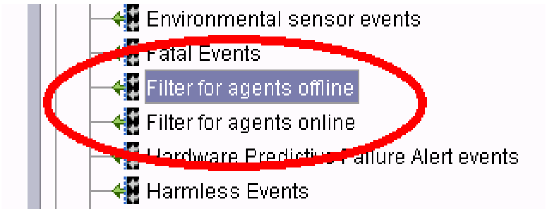


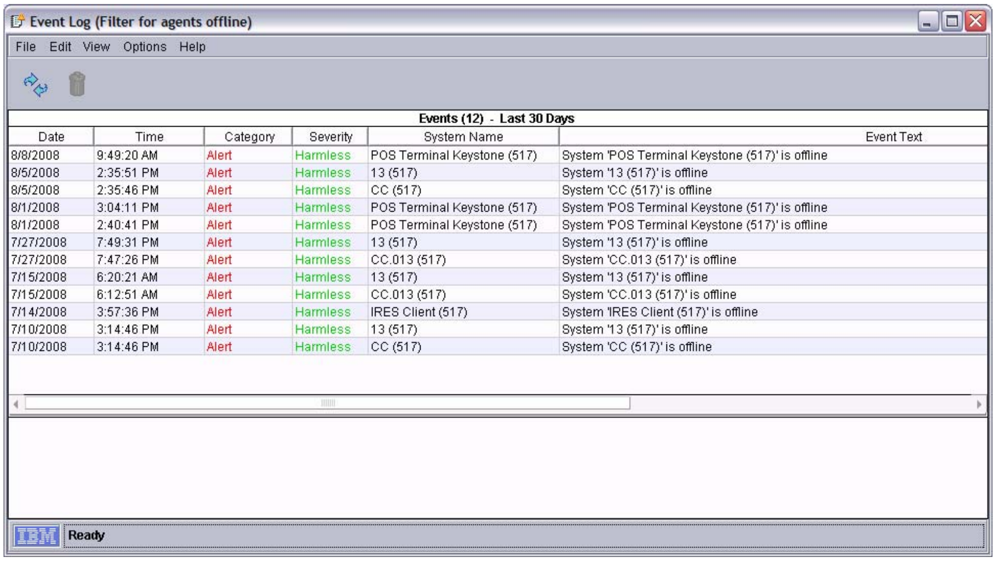
Enter a descriptive event filter name.

Filter for agents offline

6. Do the same thing for the “online” event. The only difference is that you will make sure the event type is “Director.Topology.Online” instead of “Director.Topology.Offline”. Save this filter also and give it an appropriate name.

7. Next, test your event filters by expanding the “Event Log” task in the console’s tasks pane. You should see your new event filters shown in the list of event filters underneath the event log. To test your filter, double-click it and ensure that only the online or offline events appear in the list of events displayed.

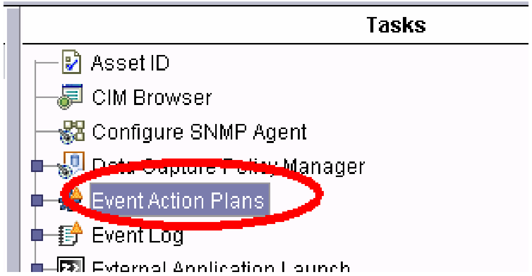

Environmental sensor events
Fatal Events
Filter for agents offline
Filter for agents online
Hardware Predictive Failure Alert events
Harmless Events


Event Log (Filter for agents offline)
File Edit View Options Help
IBM
Ready

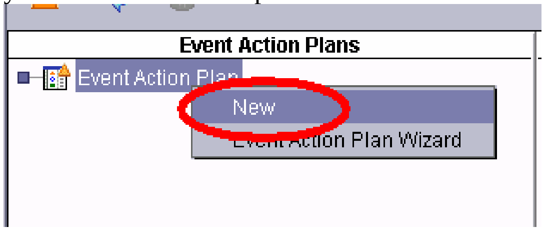
Events (12) - Last 30 Days

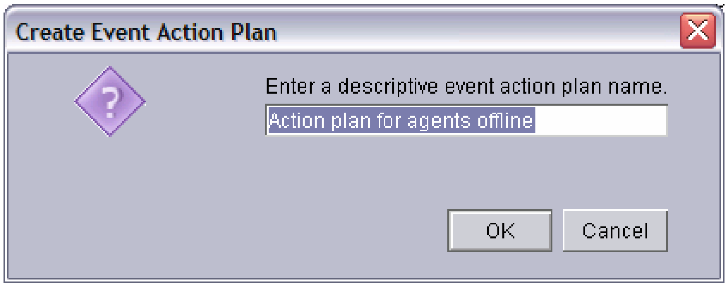
Date	Time	Category	Severity	System Name	Event Text
8/8/2008	9:49:20 AM	Alert	Harmless	POS Terminal Keystone (517)	System 'POS Terminal Keystone (517)' is offline
8/5/2008	2:35:51 PM	Alert	Harmless	13 (517)	System '13 (517)' is offline
8/5/2008	2:35:46 PM	Alert	Harmless	CC (517)	System 'CC (517)' is offline
8/1/2008	3:04:11 PM	Alert	Harmless	POS Terminal Keystone (517)	System 'POS Terminal Keystone (517)' is offline
8/1/2008	2:40:41 PM	Alert	Harmless	POS Terminal Keystone (517)	System 'POS Terminal Keystone (517)' is offline
7/27/2008	7:49:31 PM	Alert	Harmless	13 (517)	System '13 (517)' is offline
7/27/2008	7:47:26 PM	Alert	Harmless	CC.013 (517)	System 'CC.013 (517)' is offline
7/15/2008	6:20:21 AM	Alert	Harmless	13 (517)	System '13 (517)' is offline
7/15/2008	6:12:51 AM	Alert	Harmless	CC.013 (517)	System 'CC.013 (517)' is offline
7/14/2008	3:57:36 PM	Alert	Harmless	IRES Client (517)	System 'IRES Client (517)' is offline
7/10/2008	3:14:46 PM	Alert	Harmless	13 (517)	System '13 (517)' is offline
7/10/2008	3:14:46 PM	Alert	Harmless	CC (517)	System 'CC (517)' is offline

8. Next, double-click the “Event Action Plans” task in the console’s tasks pane.



9. When the event action plans task window appears, you can start a new event action plan by right-clicking “Event Action Plans” and selecting “New”. Give your new event action plan a name and click OK.



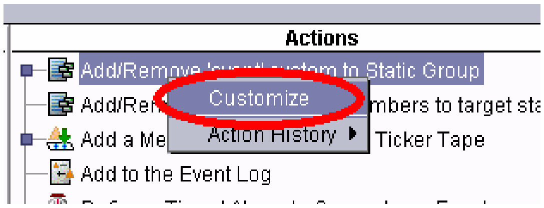


Create Event Action Plan

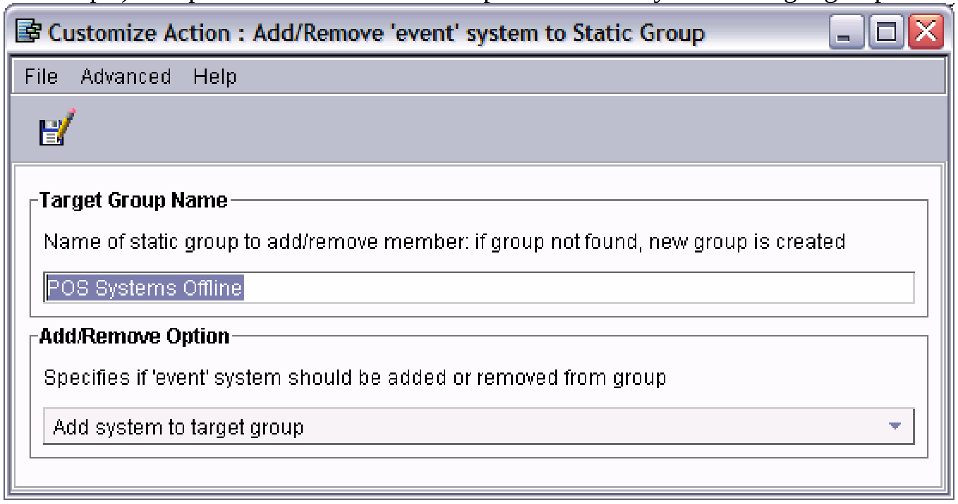
Enter a descriptive event action plan name.

Action plan for agents offline

10. Next, we'll customize an action to add and remove the system from a static group. To do that, right-click "Add/Remove 'event' system to Static Group" and click "Customize".



11. On the next screen that appears, enter the name of a static group (POS Systems Offline). (Note: Don't worry if this group doesn't yet exist – we'll create it in later steps.) Keep the default add/remove option of "Add system to target group."



Customize Action : Add/Remove 'event' system to Static Group

Target Group Name

Name of static group to add/remove member: if group not found, new group is created

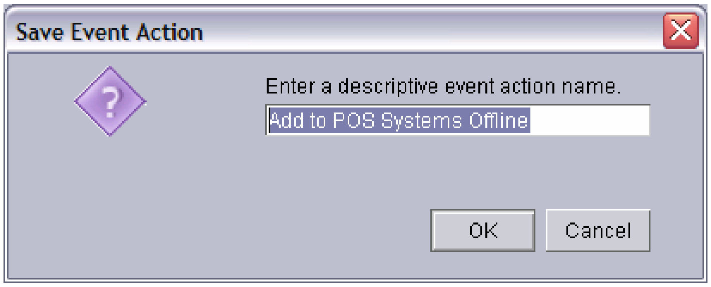
POS Systems Offline

Add/Remove Option

Specifies if 'event' system should be added or removed from group

Add system to target group

12. Select "File → Save As" and give your custom action a name, then click OK.

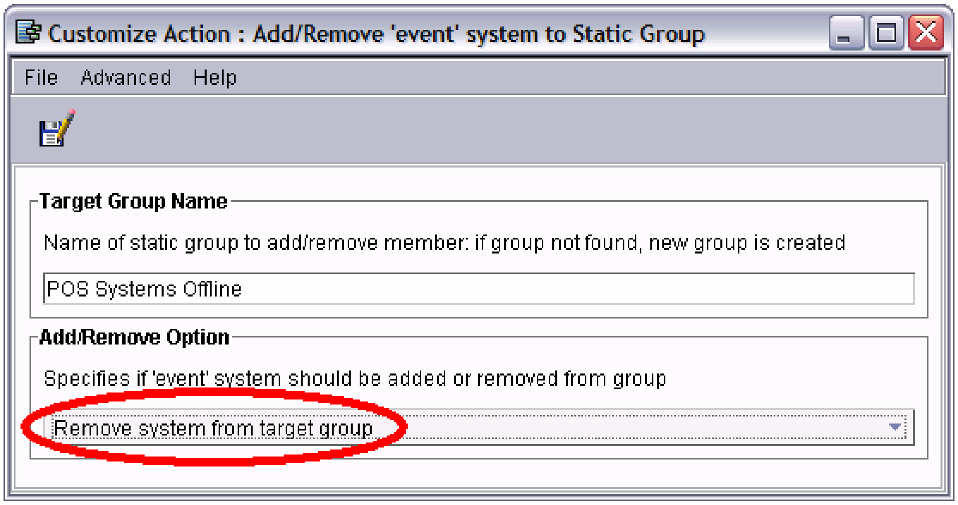


Save Event Action

Enter a descriptive event action name.

Add to POS Systems Offline

13. Customize another action, but this time change the add/remove option to "Remove system from target group". To do that:
    - Right-click "Add/Remove 'event' system to Static Group" and click "Customize".
    - Enter the same name for the static group as before (i.e. "POS Systems Offline").
    - Change the add/remove option to "Remove system from target group".
    - Click "File → Save As" and give your custom action a name, then click OK.



Customize Action : Add/Remove 'event' system to Static Group

Target Group Name

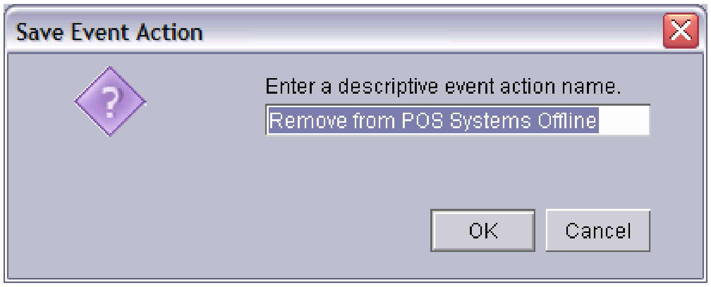
Name of static group to add/remove member: if group not found, new group is created

POS Systems Offline

Add/Remove Option

Specifies if 'event' system should be added or removed from group

Remove system from target group

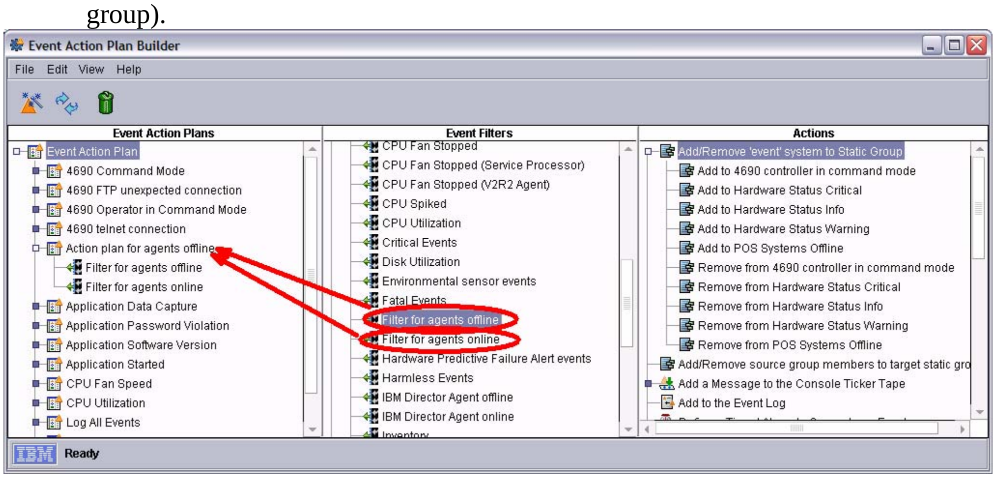


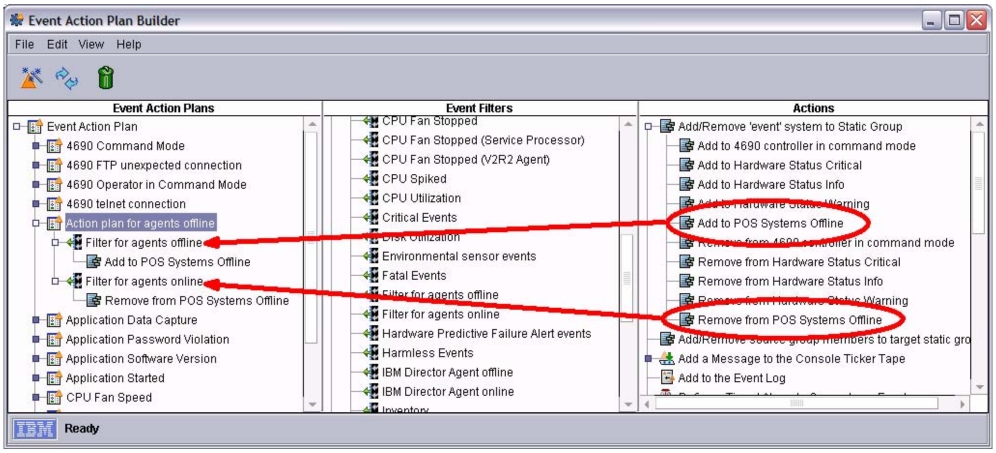
Save Event Action

Enter a descriptive event action name.

Remove from POS Systems Offline

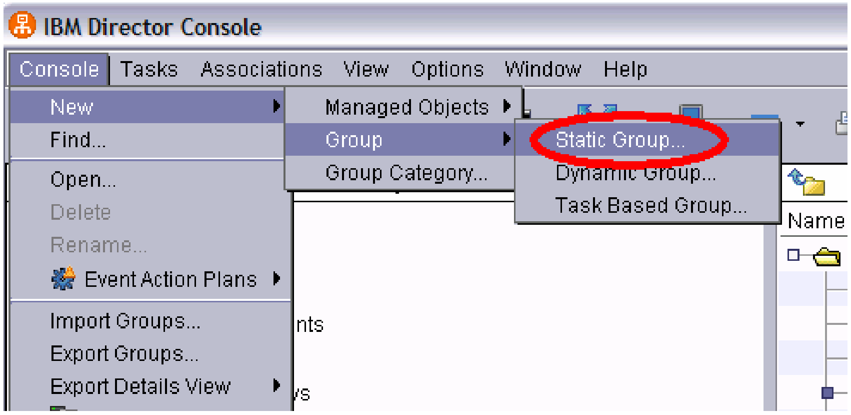
14. Now, drag-and-drop to build your event action plan, as shown below. To do that:
    - First, drag both of your event filters to the event action plan.
    - Next, drag your custom actions to the appropriate filter within the action plan (i.e. for the offline filter, drag the action for adding to the custom group; for the online filter, drag the action for removing from the custom group).

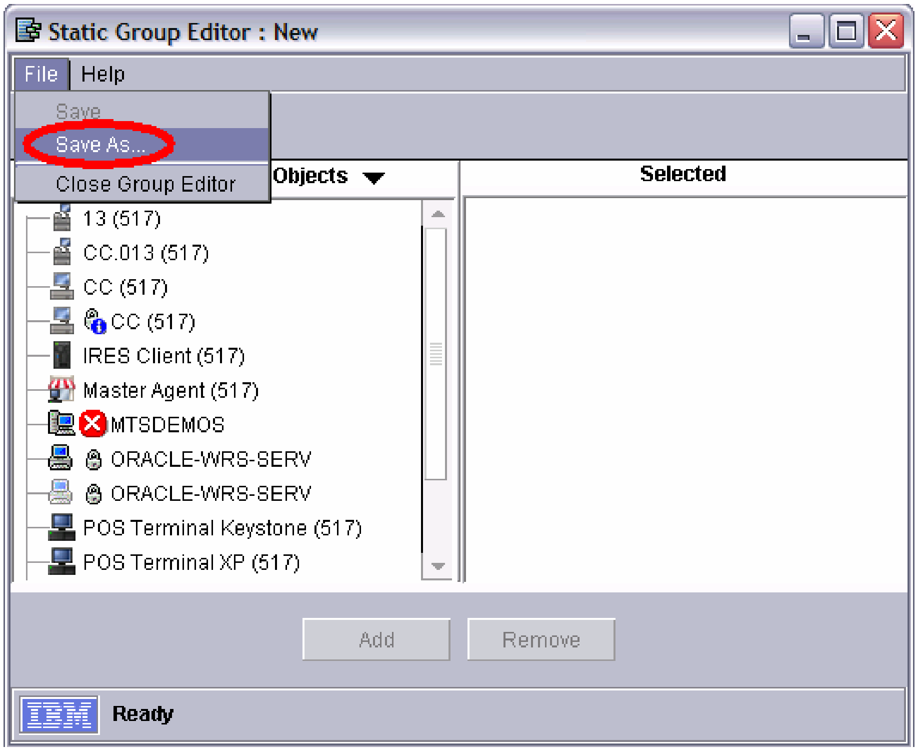

Event Action Plan Builder
File Edit View Help
Event Action Plans
Event Action Plan
4690 Command Mode
4690 FTP unexpected connection
4690 Operator in Command Mode
4690 telnet connection
Action plan for agents offline
Filter for agents offline
Filter for agents online
Application Data Capture
Application Password Violation
Application Software Version
Application Started
CPU Fan Speed
CPU Utilization
Log All Events
Event Filters
CPU Fan Stopped
CPU Fan Stopped (Service Processor)
CPU Fan Stopped (V2R2 Agent)
CPU Spiked
CPU Utilization
Critical Events
Disk Utilization
Environmental sensor events
Fatal Events
Filter for agents offline
Filter for agents online
Hardware Predictive Failure Alert events
Harmless Events
IBM Director Agent offline
IBM Director Agent online
Inventory
Actions
Add/Remove 'event' system to Static Group
Add to 4690 controller in command mode
Add to Hardware Status Critical
Add to Hardware Status Info
Add to Hardware Status Warning
Add to POS Systems Offline
Remove from 4690 controller in command mode
Remove from Hardware Status Critical
Remove from Hardware Status Info
Remove from Hardware Status Warning
Remove from POS Systems Offline
Add/Remove source group members to target static gro
Add a Message to the Console Ticker Tape
Add to the Event Log
IBM
Ready

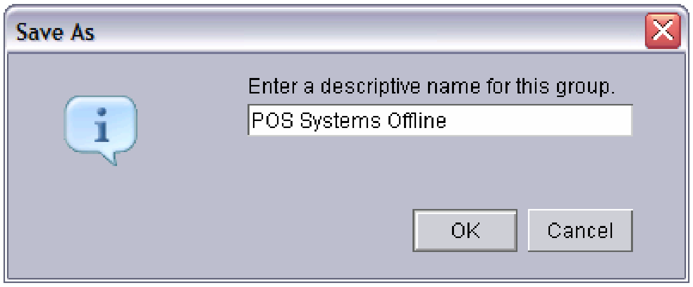

Event Action Plan Builder
File Edit View Help
Event Action Plans
Event Action Plan
4690 Command Mode
4690 FTP unexpected connection
4690 Operator in Command Mode
4690 telnet connection
Action plan for agents offline
Filter for agents offline
Add to POS Systems Offline
Filter for agents online
Remove from POS Systems Offline
Application Data Capture
Application Password Violation
Application Software Version
Application Started
CPU Fan Speed
Event Filters
CPU Fan Stopped
CPU Fan Stopped (Service Processor)
CPU Fan Stopped (V2R2 Agent)
CPU Spiked
CPU Utilization
Critical Events
Disk Utilization
Environmental sensor events
Fatal Events
Filter for agents offline
Filter for agents online
Hardware Predictive Failure Alert events
Harmless Events
IBM Director Agent offline
IBM Director Agent online
Inventory
Actions
Add/Remove 'event' system to Static Group
Add to 4690 controller in command mode
Add to Hardware Status Critical
Add to Hardware Status Info
Add to Hardware Status Warning
Add to POS Systems Offline
Remove from 4690 controller in command mode
Remove from Hardware Status Critical
Remove from Hardware Status Info
Remove from Hardware Status Warning
Remove from POS Systems Offline
Add/Remove source group members to target static gro
Add a Message to the Console Ticker Tape
Add to the Event Log
IBM
Ready

15. Close the event action plan builder screen. In the main Director console, we now need to create a custom group called "POS Systems Offline". To do that:

    - Click "Console → New → Group → Static Group".
    - On the next screen, leave the group members list empty (remember – this group will be populated automatically by the event action plan).
    - Click "File → Save As" an give the group the name "POS Systems Offline" and click OK.
    - Your group will now appear under "All Groups" in the main Director console (in the groups pane).


IBM Director Console
Console
Tasks
Associations
View
Options
Window
Help
New
Find...
Open...
Delete
Rename...
Event Action Plans
Import Groups...
Export Groups...
Export Details View
Managed Objects
Group
Group Category...
Static Group...
Dynamic Group...
Task Based Group...
Name
nts
ys


Static Group Editor : New
File
Help
Save
Save As...
Close Group Editor
Objects
Selected
13 (517)
CC.013 (517)
CC (517)
CC (517)
IRES Client (517)
Master Agent (517)
MTSDEMOS
ORACLE-WRS-SERV
ORACLE-WRS-SERV
POS Terminal Keystone (517)
POS Terminal XP (517)
Add
Remove
IBM
Ready

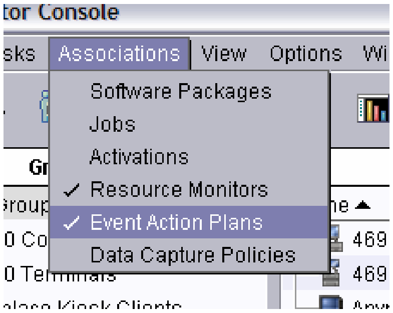


Save As

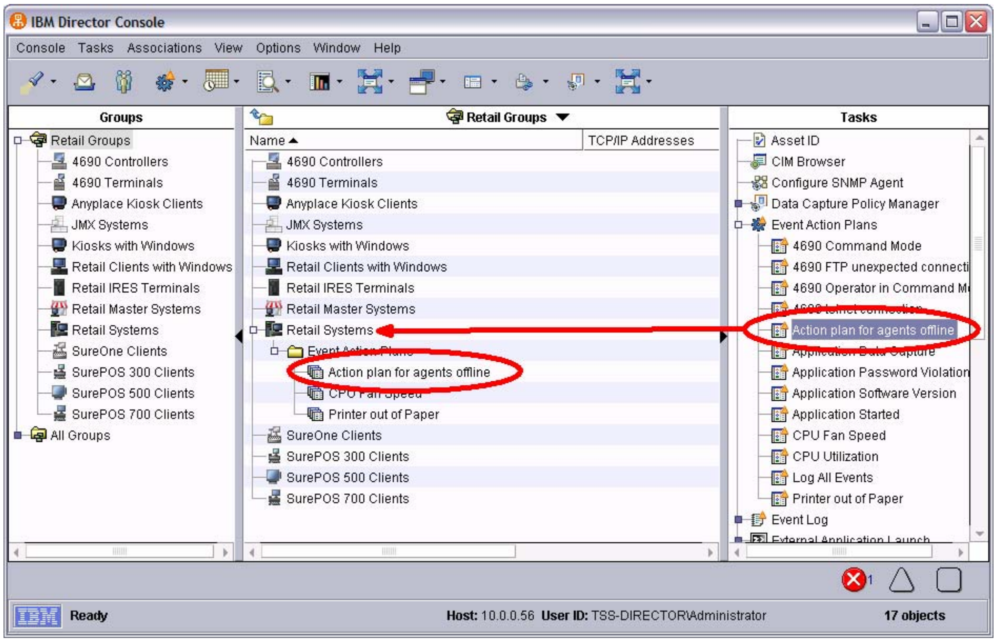
Enter a descriptive name for this group.

POS Systems Offline

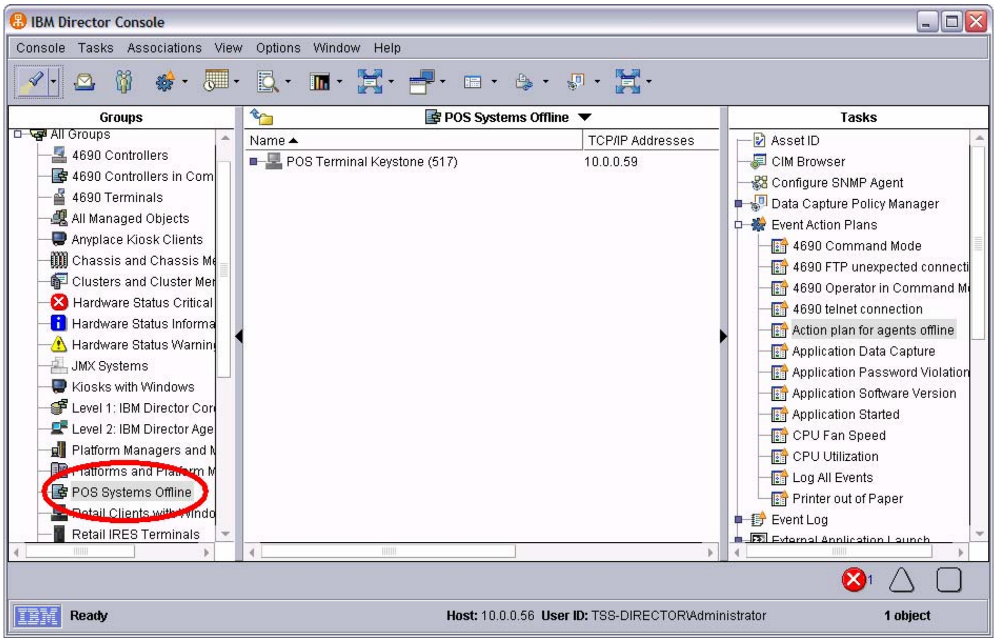
16. Next, make sure the “Event Action Plans” association is checked in the console’s “Associations” menu.



17. Next, we need to associate your event action plan with the systems to which it will apply. To do that:
    - Select “Retail Groups” in the groups pane so that all the retail groups will be shown in the center pane.
    - Drag your event action plan from the tasks pane (underneath “Event Action Plans”) to the group “Retail Systems”.
    - If you expand the tree underneath this group, you should now see your action plan associated to the group “Retail Systems”.



18. Finally, we're ready to test the event action plan. To do that:
    - Select "All Groups → POS Systems Offline" in the groups pane.
    - On a general agent, run the command "net stop RemoteMgmtAgent" to stop the general agent.
    - The system should automatically appear in the center pane after a few seconds.

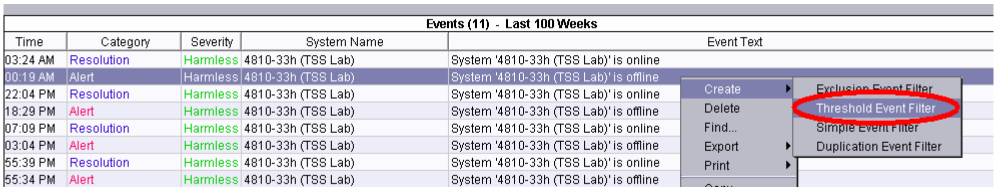


Example: Trigger action only if event occurs 3 times within a 24-hour period

In this scenario, we'll configure the event action plan to display a ticker message if a system goes online/offline *repeatedly* within a single day. If the system goes offline 3 times within a given 24-hour period, the event action plan will trigger.

> **Note**: This example assumes you've already become familiar with the basics of creating an event filter and an event action plan. If not, you should first try "**Example: Create a Custom Group for Agents Offline**", and read the introduction to event management, before proceeding with this example.

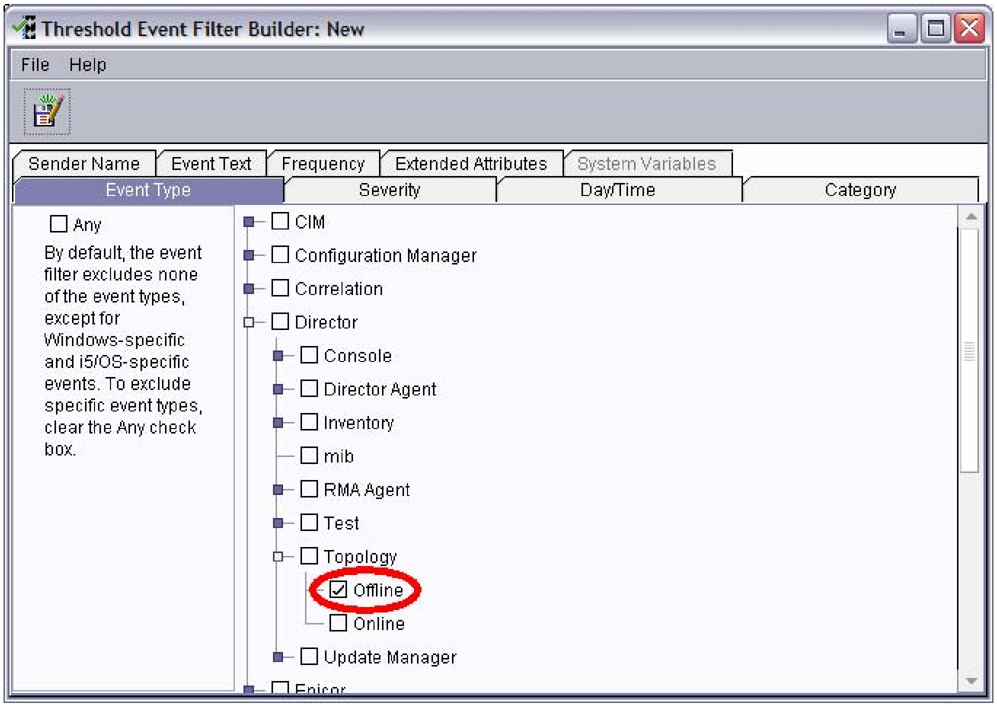
1. Find an example of the offline event in the event log, then right-click and select "**Create / Threshold Event Filter**".



Events (11) - Last 100 Weeks

Time	Category	Severity	System Name	Event Text
03:24 AM	Resolution	Harmless	4810-33h (TSS Lab)	System '4810-33h (TSS Lab)' is online
00:19 AM	Alert	Harmless	4810-33h (TSS Lab)	System '4810-33h (TSS Lab)' is offline
22:04 PM	Resolution	Harmless	4810-33h (TSS Lab)	System '4810-33h (TSS Lab)' is online
18:29 PM	Alert	Harmless	4810-33h (TSS Lab)	System '4810-33h (TSS Lab)' is offline
07:09 PM	Resolution	Harmless	4810-33h (TSS Lab)	System '4810-33h (TSS Lab)' is online
03:04 PM	Alert	Harmless	4810-33h (TSS Lab)	System '4810-33h (TSS Lab)' is offline
55:39 PM	Resolution	Harmless	4810-33h (TSS Lab)	System '4810-33h (TSS Lab)' is online
55:34 PM	Alert	Harmless	4810-33h (TSS Lab)	System '4810-33h (TSS Lab)' is offline

2. When configuring your filter, set the event type to "**Director.Topology.Offline**".

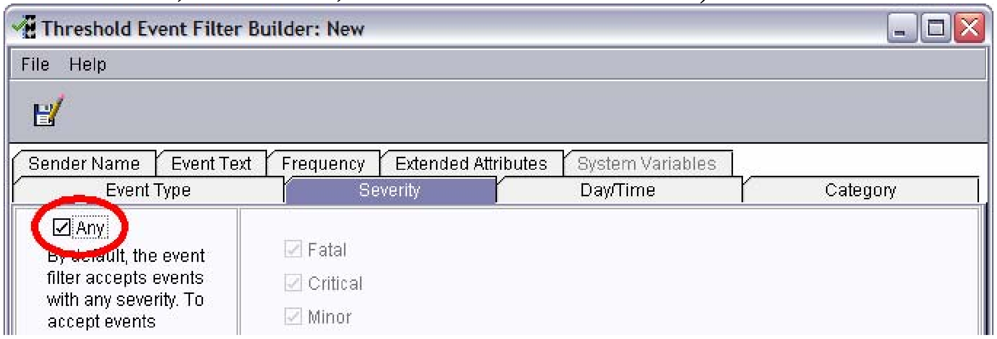


☐ Any

By default, the event filter excludes none of the event types, except for Windows-specific and i5/OS-specific events. To exclude specific event types, clear the Any check box.

- ☐ CIM
- ☐ Configuration Manager
- ☐ Correlation
- ☐ Director
  - ☐ Console
  - ☐ Director Agent
  - ☐ Inventory
  - ☐ mib
  - ☐ RMA Agent
  - ☐ Test
  - ☐ Topology
    - ☑ Offline
    - ☐ Online
  - ☐ Update Manager
- ☐ Enicor

3. For all other tabs (except the "Frequency" tab), select "**Any**". (In this example, you'll check the "**Any**" checkbox for the "Severity", "Day/Time", "Category", "Sender Name", "Event Text", and "Extended Attributes" tabs.)

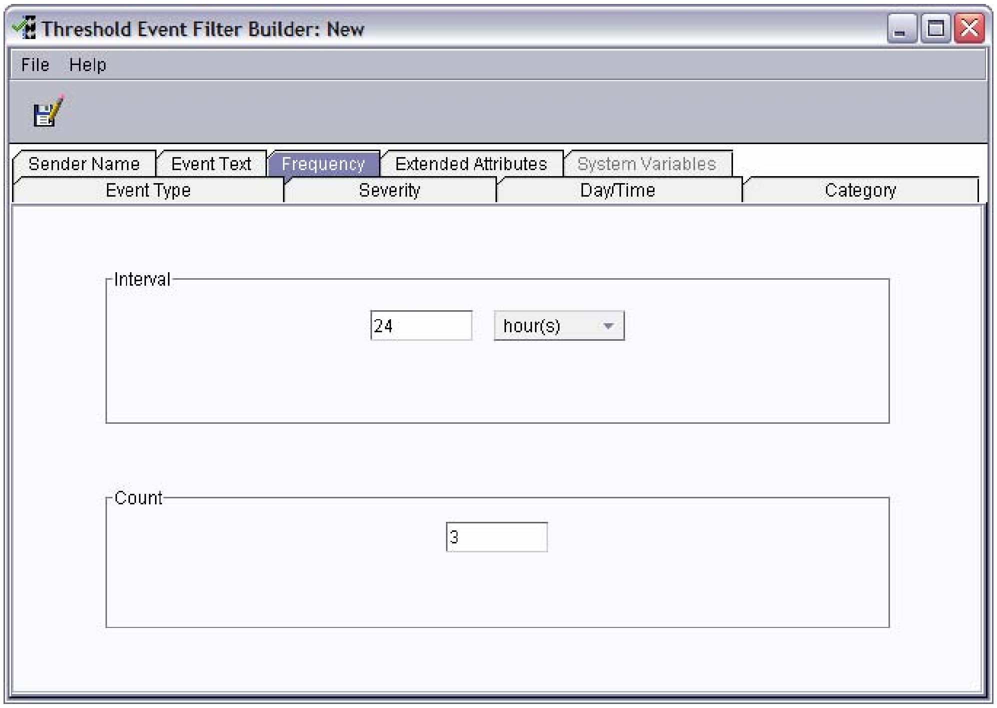


☑ Any

By default, the event filter accepts events with any severity. To accept events

☑ Fatal
☑ Critical
☑ Minor

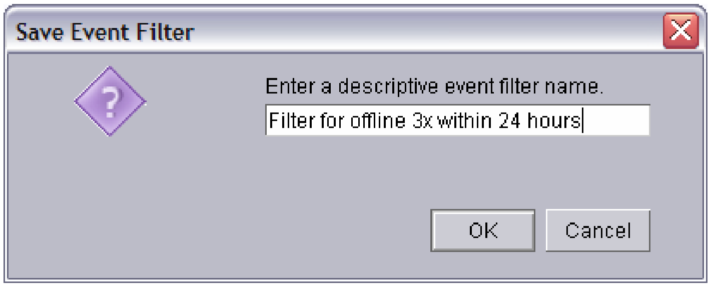
4. At this point, the only tab left to edit is the "Frequency" tab. Set the interval to 24 hours, and the count to 3.



Interval: 24 hour(s)

Count: 3

5. Save the filter.

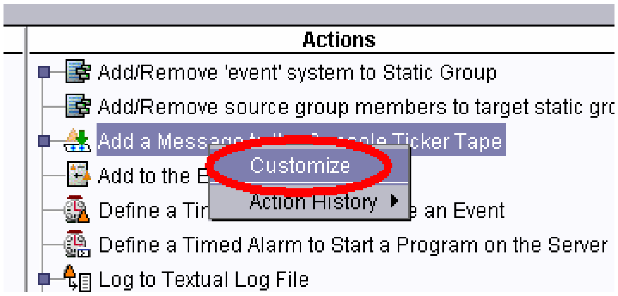


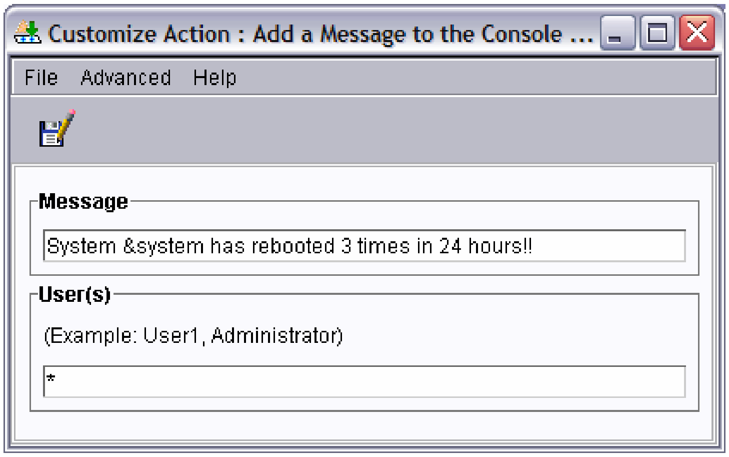
Enter a descriptive event filter name.

Filter for offline 3x within 24 hours

6. Open the event action plans task. If desired, create a new event action plan for your new scenario.

7. Right-click “Add a Message to the Console Ticker Tape” (under Actions within the Event Actions Plan Builder), and enter a message to be displayed.


Actions
Add/Remove 'event' system to Static Group
Add/Remove source group members to target static gro
Add a Messag   ole Ticker Tape
Customize
Action History
Add to the E
Define a Tir   e an Event
Define a Timed Alarm to Start a Program on the Server
Log to Textual Log File



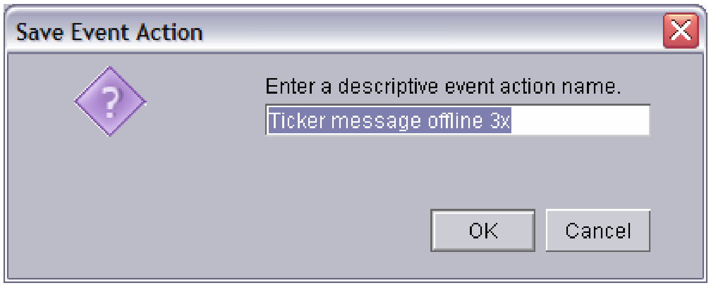
Message

System &system has rebooted 3 times in 24 hours!!

User(s)

(Example: User1, Administrator)

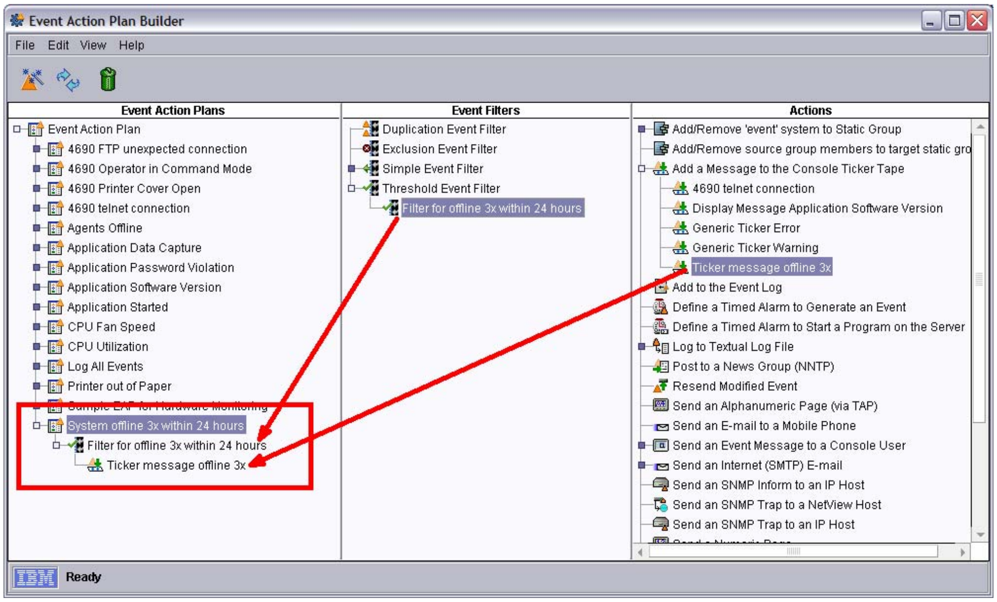
*



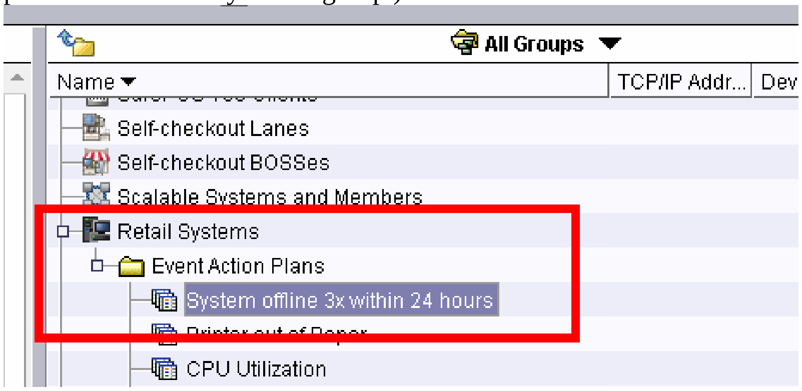
Enter a descriptive event action name.

Ticker message offline 3x

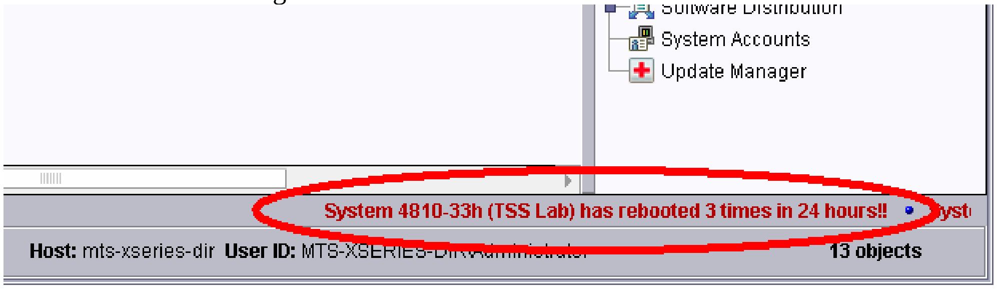
8. Drag-and-drop to build your event action plan.


Event Action Plan Builder
File Edit View Help
Event Action Plans
Event Action Plan
4690 FTP unexpected connection
4690 Operator in Command Mode
4690 Printer Cover Open
4690 telnet connection
Agents Offline
Application Data Capture
Application Password Violation
Application Software Version
Application Started
CPU Fan Speed
CPU Utilization
Log All Events
Printer out of Paper
Sample EAP for Hardware Monitoring
System offline 3x within 24 hours
Filter for offline 3x within 24 hours
Ticker message offline 3x
Event Filters
Duplication Event Filter
Exclusion Event Filter
Simple Event Filter
Threshold Event Filter
Filter for offline 3x within 24 hours
Actions
Add/Remove 'event' system to Static Group
Add/Remove source group members to target static gro
Add a Message to the Console Ticker Tape
4690 telnet connection
Display Message Application Software Version
Generic Ticker Error
Generic Ticker Warning
Ticker message offline 3x
Add to the Event Log
Define a Timed Alarm to Generate an Event
Define a Timed Alarm to Start a Program on the Server
Log to Textual Log File
Post to a News Group (NNTP)
Resend Modified Event
Send an Alphanumeric Page (via TAP)
Send an E-mail to a Mobile Phone
Send an Event Message to a Console User
Send an Internet (SMTP) E-mail
Send an SNMP Inform to an IP Host
Send an SNMP Trap to a NetView Host
Send an SNMP Trap to an IP Host
Send a Numeric Page
IBM Ready

9. In the main Director Console, click on “All Groups”, then associate your event action plan with the group “Retail Systems”. (i.e. Drag-and-drop the event action plan to the “Retail Systems” group.)



10. To test your event action plan, try rebooting any of your systems 3 times, and you will see the ticker message at the bottom of the Director Console.


Software Distribution
System Accounts
Update Manager

System 4810-33h (TSS Lab) has rebooted 3 times in 24 hours!!

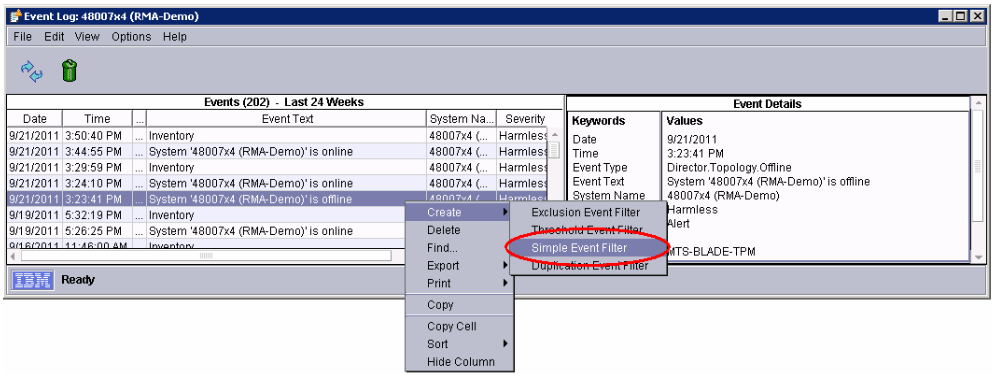
Host: mts-xseries-dir User ID: MTS-XSERIES-DIR\Administrator
13 objects

Example: Trigger action only if system is offline for an extended period of time

In this scenario, we'll configure the event action plan to display a ticker message if a system goes offline and *stays offline without an online event* for an extended period of time.

> **Note**: This example assumes you've already become familiar with the basics of creating an event filter and an event action plan. If not, you should first try "**Example: Create a Custom Group for Agents Offline**", and read the introduction to event management, before proceeding with this example.

1. Find an example of the offline event in the event log, then right-click and create a simple event filter:



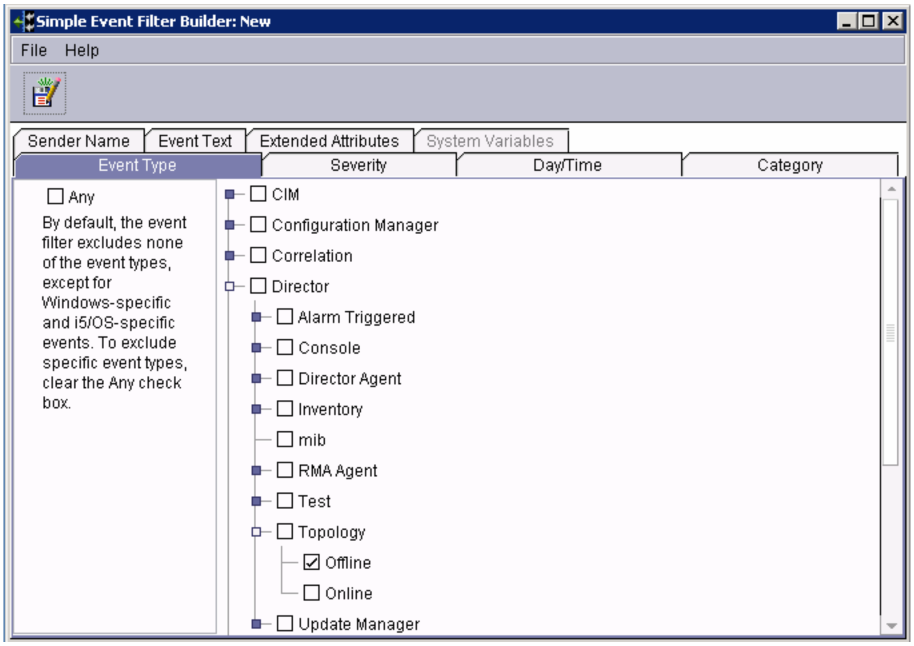
Events (202) - Last 24 Weeks

Date	Time	...	Event Text	System Na...	Severity
9/21/2011	3:50:40 PM	...	Inventory	48007x4 (...	Harmless
9/21/2011	3:44:55 PM	...	System '48007x4 (RMA-Demo)' is online	48007x4 (...	Harmless
9/21/2011	3:29:59 PM	...	Inventory	48007x4 (...	Harmless
9/21/2011	3:24:10 PM	...	System '48007x4 (RMA-Demo)' is online	48007x4 (...	Harmless
9/21/2011	3:23:41 PM	...	System '48007x4 (RMA-Demo)' is offline	48007x4 (...	Harmless
9/19/2011	5:32:19 PM	...	Inventory		
9/19/2011	5:26:25 PM	...	System '48007x4 (RMA-Demo)' is online		
9/16/2011	11:46:00 AM	...	Inventory		

Event Details

Keywords	Values
Date	9/21/2011
Time	3:23:41 PM
Event Type	Director.Topology.Offline
Event Text	System '48007x4 (RMA-Demo)' is offline
System Name	48007x4 (RMA-Demo)
	Harmless
	Alert
	MTS-BLADE-TPM

2. Ensure that the Event Type is set to "**Director.Topology.Offline**"



Simple Event Filter Builder: New

File Help

Sender Name | Event Text | Extended Attributes | System Variables

Event Type | Severity | Day/Time | Category

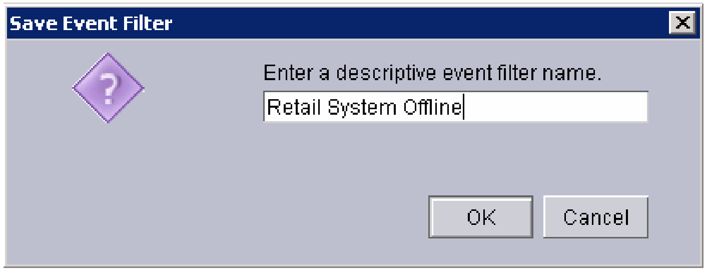
□ Any

By default, the event filter excludes none of the event types, except for Windows-specific and i5/OS-specific events. To exclude specific event types, clear the Any check box.

- □ CIM
- □ Configuration Manager
- □ Correlation
- □ Director
  - □ Alarm Triggered
  - □ Console
  - □ Director Agent
  - □ Inventory
  - □ mib
  - □ RMA Agent
  - □ Test
  - □ Topology
    - ☑ Offline
    - □ Online
  - □ Update Manager

3. For all other tabs, select "**Any**". (In this example, you'll check the "**Any**" checkbox for the "Severity", "Day/Time", "Category", "Sender Name", "Event Text", and "Extended Attributes" tabs.)

4. Save the event filter and give it a descriptive name



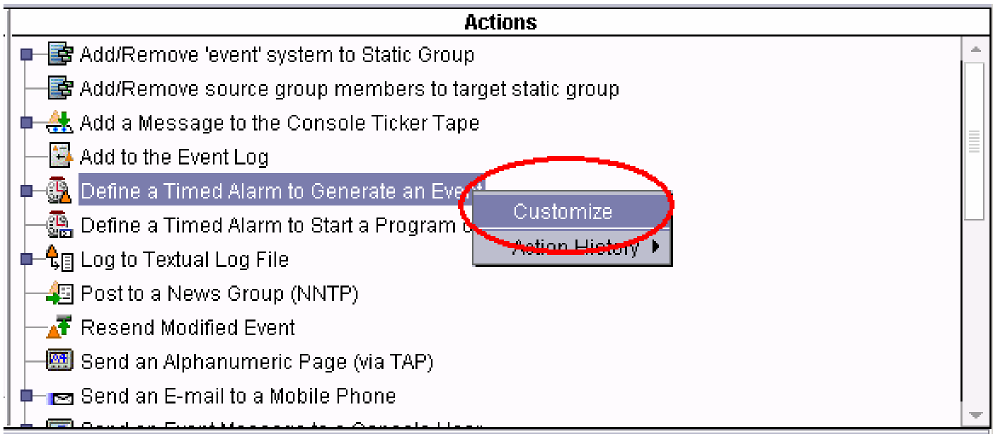
Save Event Filter

Enter a descriptive event filter name.

Retail System Offline

5. Open the event action plans task. If desired, create a new event action plan for your new scenario.

6. In the Event Action Plan Builder, right-click on "Define a Timed Alarm to Generate an Event" and click "Customize".



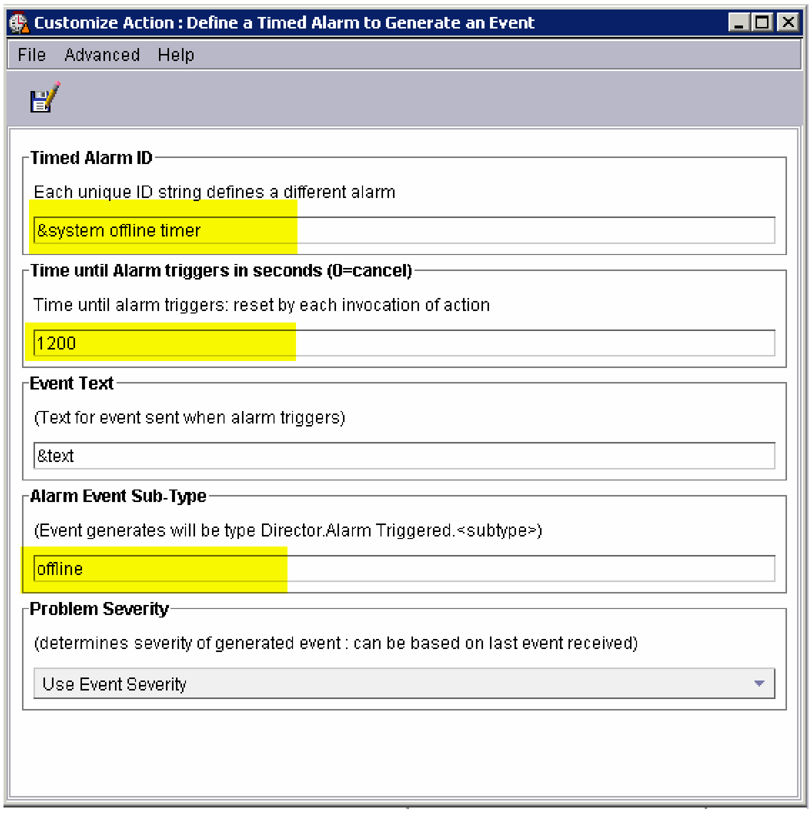
Actions

Add/Remove 'event' system to Static Group
Add/Remove source group members to target static group
Add a Message to the Console Ticker Tape
Add to the Event Log
Define a Timed Alarm to Generate an Eve
Define a Timed Alarm to Start a Program o
Log to Textual Log File
Post to a News Group (NNTP)
Resend Modified Event
Send an Alphanumeric Page (via TAP)
Send an E-mail to a Mobile Phone
Send an Event Message to a Console User

7. The timed alarm action can be used to start a timer when an event occurs. When customizing, you need to take note of the "Timed Alarm ID" field which has to be a unique value. To ensure it is unique to each system that generates the event, use the "&system" substitution variable.

   You can also set the length of the timer (seconds), the event text that should get generated when the timer expires, and the event sub-type for the expiration event.

   The following screenshot indicates a 20 minute timer that will generate a "Director.Alarm Triggered.offline" event if the timer expires:



Customize Action : Define a Timed Alarm to Generate an Event
File
Advanced
Help

Timed Alarm ID

Each unique ID string defines a different alarm

&system offline timer

Time until Alarm triggers in seconds (0=cancel)

Time until alarm triggers: reset by each invocation of action

1200

Event Text

(Text for event sent when alarm triggers)

&text

Alarm Event Sub-Type

(Event generates will be type Director.Alarm Triggered.<subtype>)

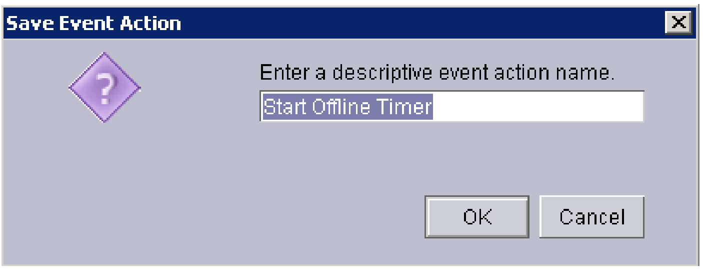
offline

Problem Severity

(determines severity of generated event : can be based on last event received)

Use Event Severity

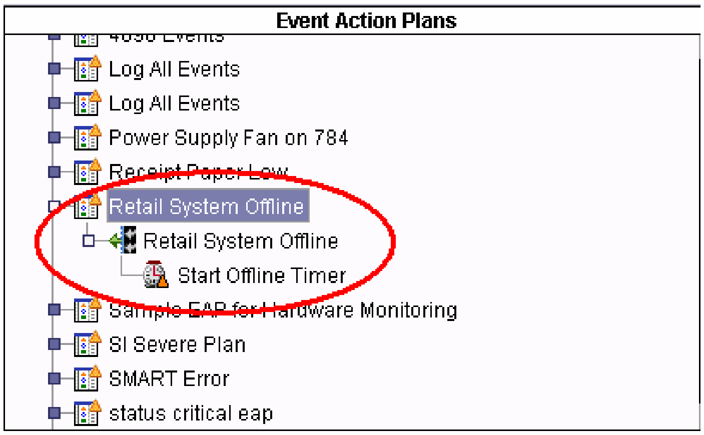
8. Click the “Save As” button and give the timer a descriptive name:



Enter a descriptive event action name.

Start Offline Timer

9. To begin building your Event Action Plan, drag the “Retail System Offline” event filter to the plan, and apply the “Start Offline Timer” action to the filter:

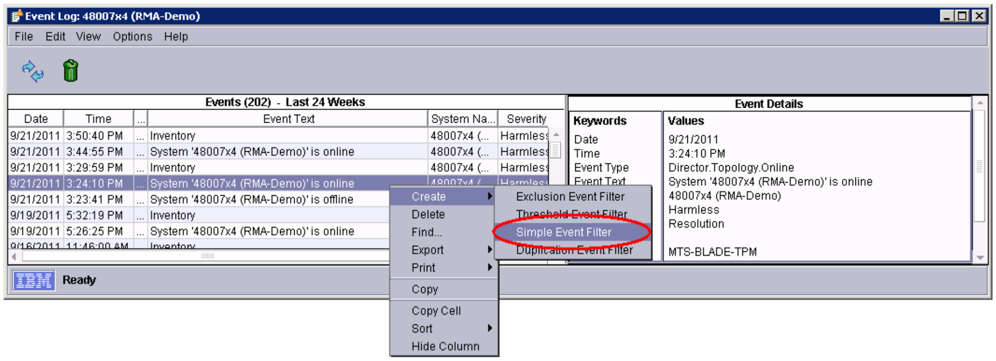


Event Action Plans

- 4096 Events
- Log All Events
- Log All Events
- Power Supply Fan on 784
- Receipt Paper Low
- Retail System Offline
  - Retail System Offline
    - Start Offline Timer
- Sample EAP for Hardware Monitoring
- SI Severe Plan
- SMART Error
- status critical eap

Now, when an offline event is received, the 20 minute timer will begin its count down.

10. Next, we need to cancel the timer if an **online** event is received for the system. Just as with the offline event, find an example of the online event in the event log, then right-click and create a simple event filter:



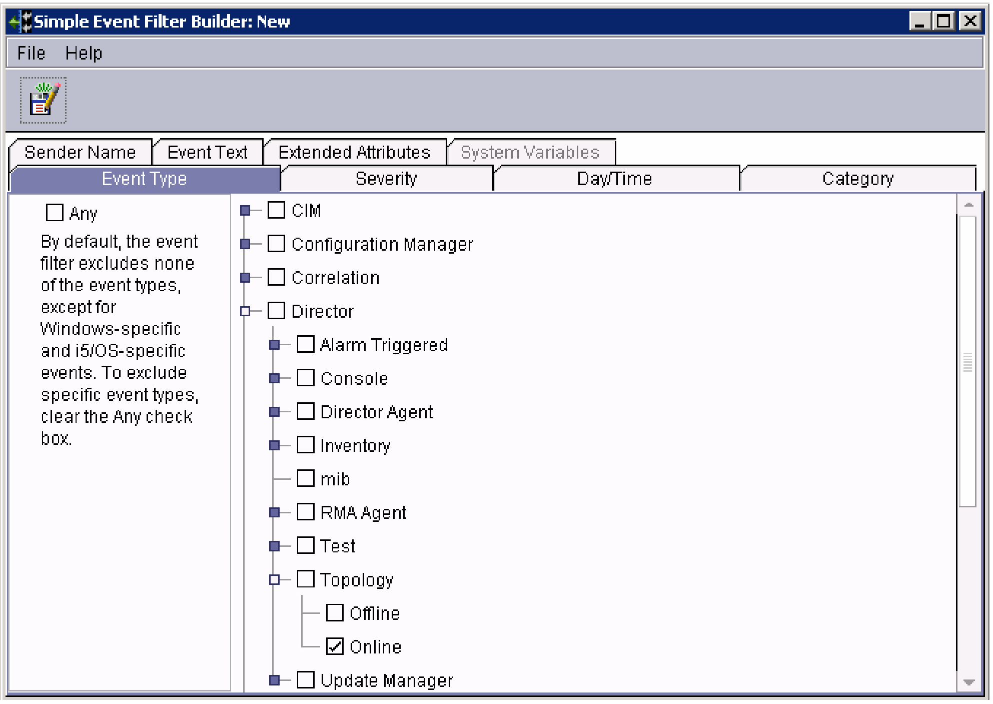
Events (202) - Last 24 Weeks

Date	Time	...	Event Text	System Na...	Severity
9/21/2011	3:50:40 PM	...	Inventory	48007x4 (...	Harmless
9/21/2011	3:44:55 PM	...	System '48007x4 (RMA-Demo)' is online	48007x4 (...	Harmless
9/21/2011	3:29:59 PM	...	Inventory	48007x4 (...	Harmless
9/21/2011	3:24:10 PM	...	System '48007x4 (RMA-Demo)' is online	48007x4 (...	Harmless
9/21/2011	3:23:41 PM	...	System '48007x4 (RMA-Demo)' is offline		
9/19/2011	5:32:19 PM	...	Inventory		
9/19/2011	5:26:25 PM	...	System '48007x4 (RMA-Demo)' is online		
9/16/2011	11:46:00 AM	...	Inventory		

Event Details

Keywords	Values
Date	9/21/2011
Time	3:24:10 PM
Event Type	Director.Topology.Online
Event Text	System '48007x4 (RMA-Demo)' is online
	48007x4 (RMA-Demo)
	Harmless
	Resolution
	MTS-BLADE-TPM

11. Ensure that the Event Type is set to “**Director.Topology.Online**”



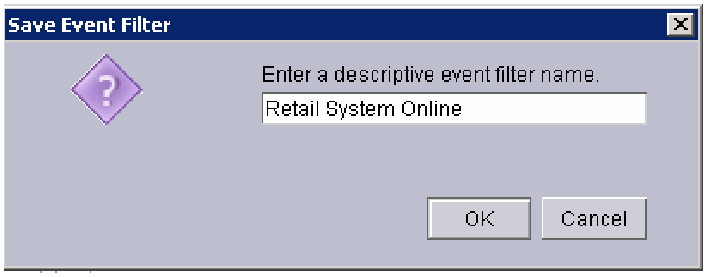
□ Any

By default, the event filter excludes none of the event types, except for Windows-specific and i5/OS-specific events. To exclude specific event types, clear the Any check box.

- □ CIM
- □ Configuration Manager
- □ Correlation
- □ Director
  - □ Alarm Triggered
  - □ Console
  - □ Director Agent
  - □ Inventory
  - □ mib
  - □ RMA Agent
  - □ Test
  - □ Topology
    - □ Offline
    - ☑ Online
  - □ Update Manager

12. For all other tabs, select “**Any**”. (In this example, you’ll check the “**Any**” checkbox for the “Severity”, “Day/Time”, “Category”, “Sender Name”, “Event Text”, and “Extended Attributes” tabs.)

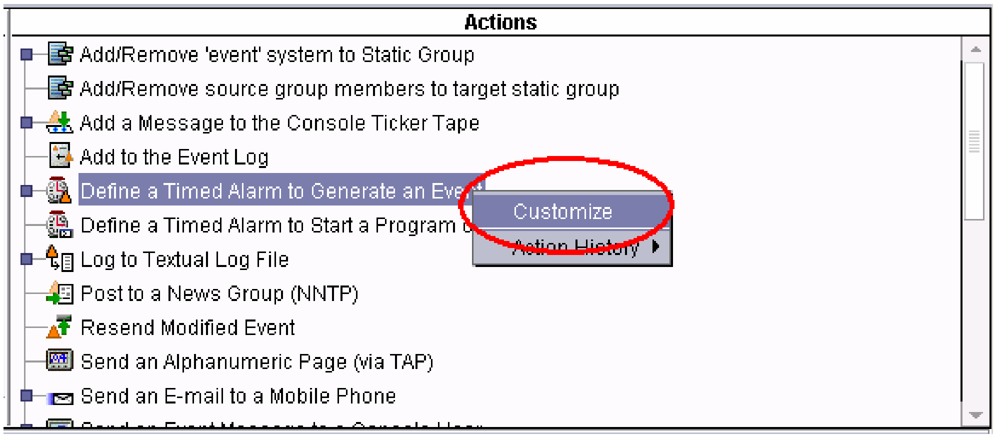
13. Save the event filter and give it a descriptive name



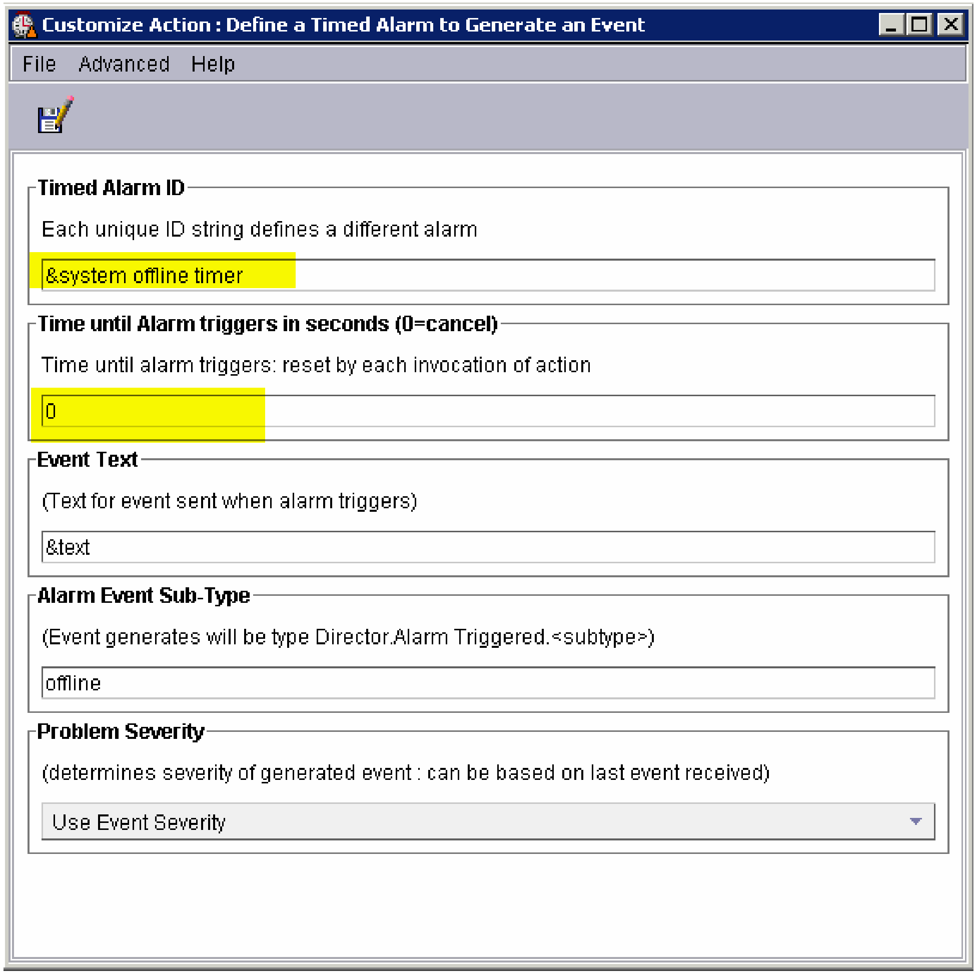
Enter a descriptive event filter name.

Retail System Online

14. Return to the Event Action Plan Builder, right-click on “Define a Timed Alarm to Generate an Event” and click “Customize”.


Actions
Add/Remove 'event' system to Static Group
Add/Remove source group members to target static group
Add a Message to the Console Ticker Tape
Add to the Event Log
Define a Timed Alarm to Generate an Eve
Define a Timed Alarm to Start a Program
Log to Textual Log File
Post to a News Group (NNTP)
Resend Modified Event
Send an Alphanumeric Page (via TAP)
Send an E-mail to a Mobile Phone
Customize
Action History

15. This time you will want to make sure you specify the same “Timed Alarm ID” as before with a “Time until alarm triggers in seconds” of “0” (zero). A value of 0 will cause a running timer with the same “Timed Alarm ID” to cancel.


Customize Action : Define a Timed Alarm to Generate an Event

Timed Alarm ID

Each unique ID string defines a different alarm

&system offline timer

Time until Alarm triggers in seconds (0=cancel)

Time until alarm triggers: reset by each invocation of action

0

Event Text

(Text for event sent when alarm triggers)

&text

Alarm Event Sub-Type

(Event generates will be type Director.Alarm Triggered.<subtype>)

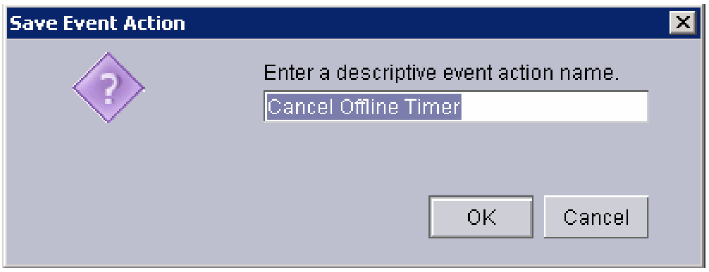
offline

Problem Severity

(determines severity of generated event : can be based on last event received)

Use Event Severity

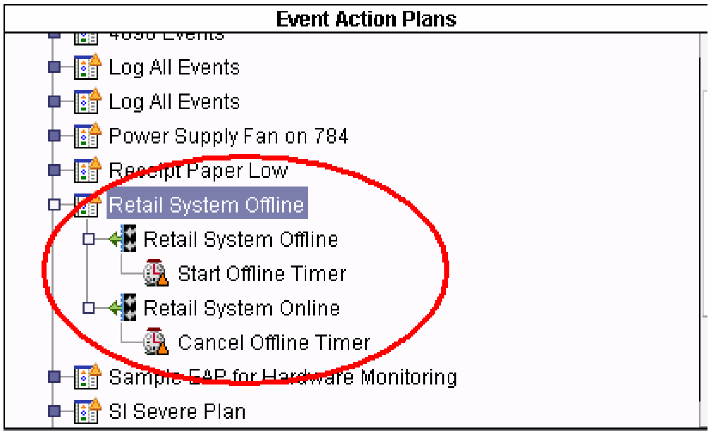
16. Click “Save As” and give this action an appropriate name:


Save Event Action

Enter a descriptive event action name.

Cancel Offline Timer

17. To continue to build your Event Action Plan, drag the “Retail System Online” event filter to the plan, and apply the “Cancel Offline Timer” action to the filter:


Event Action Plans

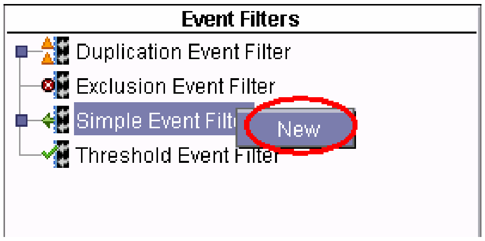
- 4690 Events
- Log All Events
- Log All Events
- Power Supply Fan on 784
- Receipt Paper Low
- Retail System Offline
  - Retail System Offline
    - Start Offline Timer
  - Retail System Online
    - Cancel Offline Timer
- Sample EAP for Hardware Monitoring
- SI Severe Plan

Now, when an offline event is received, the 20 minute timer will begin its count down. If an online event is received during that 20 minute window, the timer will be canceled.

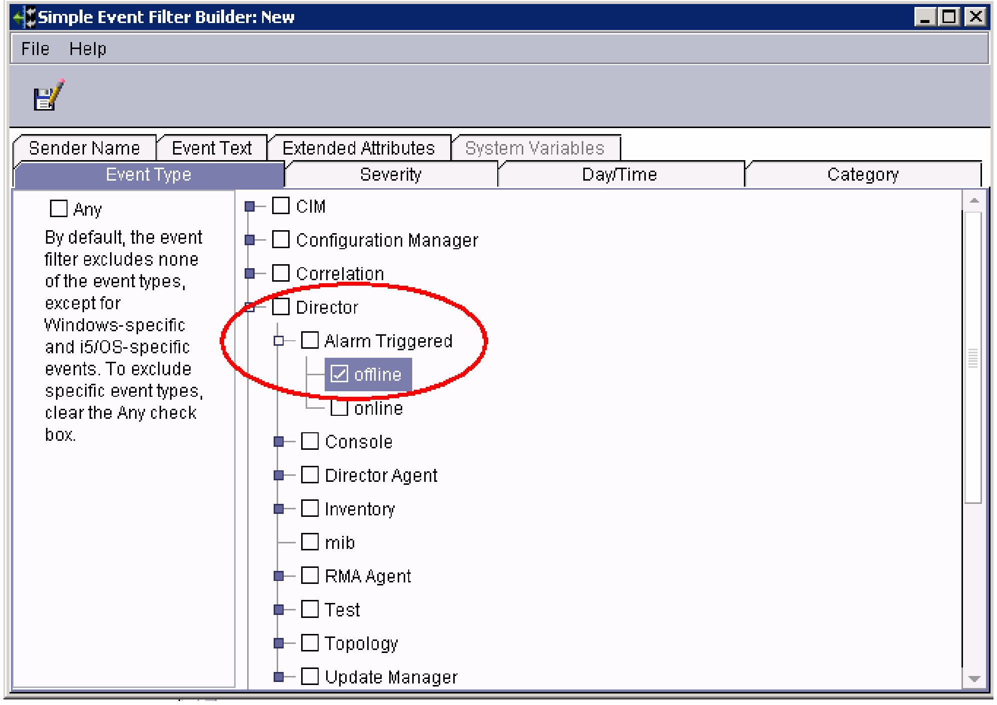
18. To complete the event action plan, you lastly need to add the action that will occur if the timer expires without getting canceled by an online event. To do this, you will need to create an event filter for the timer expiration event.

    To create the filter, you can either generate the offline event and allow the timer to expire (so you have a sample event to work with), or you could create it from scratch.

    To create the filter from scratch, right-click on "Simple Event Filter" within the "Event Action Plan Builder" and select "New".



19. In the "Simple Event Filter Builder" you will want to un-check "Any" from the "Event Type" tab and select the "Alarm Event Sub-Type" that you specified in the Timed Alarm Action. It will appear in the list under "**Director.Alarm Triggered**":



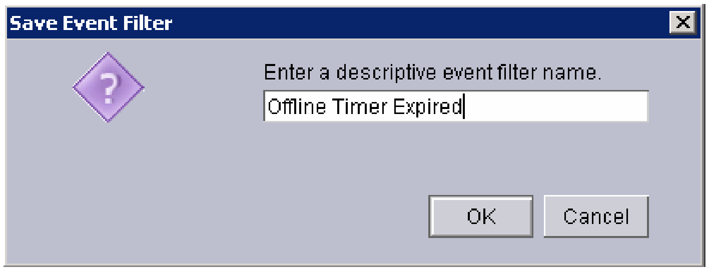
□ Any

By default, the event filter excludes none of the event types, except for Windows-specific and i5/OS-specific events. To exclude specific event types, clear the Any check box.

- □ CIM
- □ Configuration Manager
- □ Correlation
- □ Director
  - □ Alarm Triggered
    - ☑ offline
    - □ online
  - □ Console
  - □ Director Agent
  - □ Inventory
  - □ mib
  - □ RMA Agent
  - □ Test
  - □ Topology
  - □ Update Manager

20. For all other tabs, select “**Any**”. (In this example, you’ll check the “**Any**” checkbox for the “Severity”, “Day/Time”, “Category”, “Sender Name”, “Event Text”, and “Extended Attributes” tabs.)

21. Save the event filter and give it a descriptive name

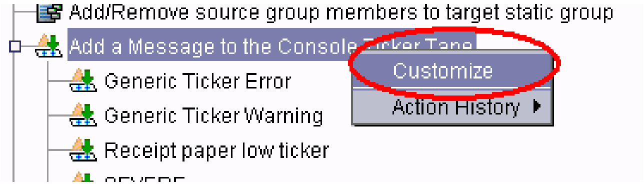


Enter a descriptive event filter name.

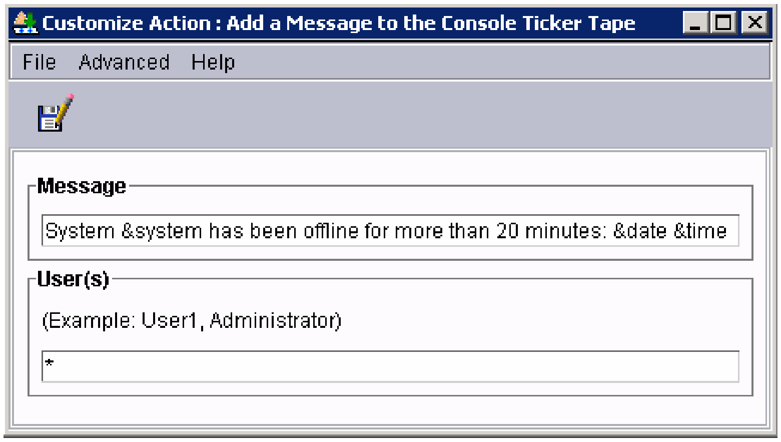
Offline Timer Expired

22. Now we need to create an action for when the timer expires. In this example we will use a scrolling ticker tape message. In production it may make more sense to have an email or text alert.

    To create the ticker tape action, “Right-Click” on the “Add a Message to the Console Ticker Tape” action and select “Customize”:



23. Add a descriptive message using the “&system”, “&date”, and “&time” substitution variables to include details about where and when the event occurred. Specify “*” in the “User(s)” field so that all console users will get this ticker tape message:



Message

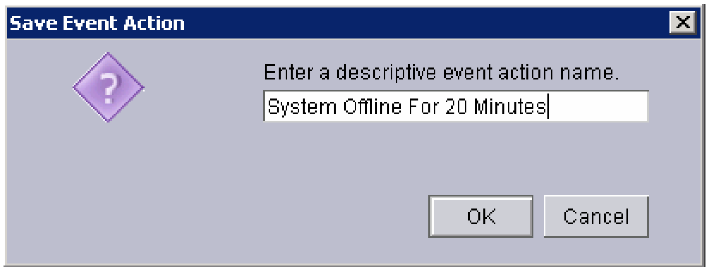
System &system has been offline for more than 20 minutes: &date &time

User(s)

(Example: User1, Administrator)

*

24. Save this action and give it a descriptive name:

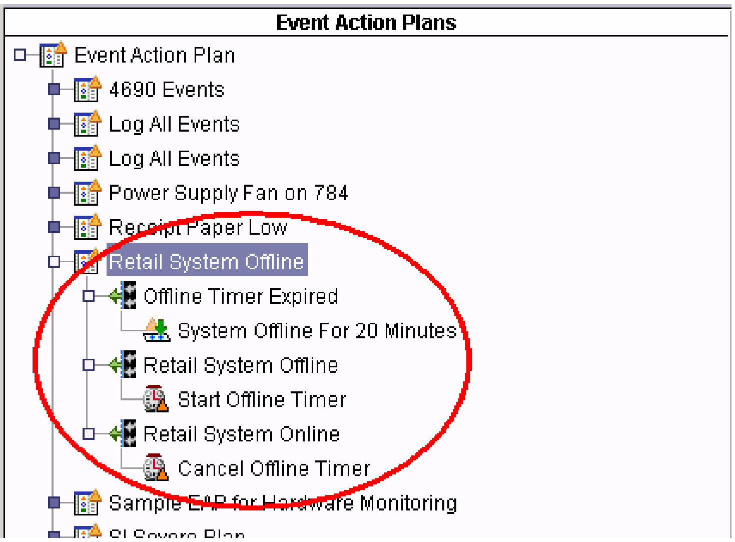


Enter a descriptive event action name.

System Offline For 20 Minutes

25. To complete your Event Action Plan, drag the “Offline Timer Expired” filter under the Event Action Plan and drag the “System Offline For 20 Minutes” action under the filter.

Your completed Event Action Plan should look like this:

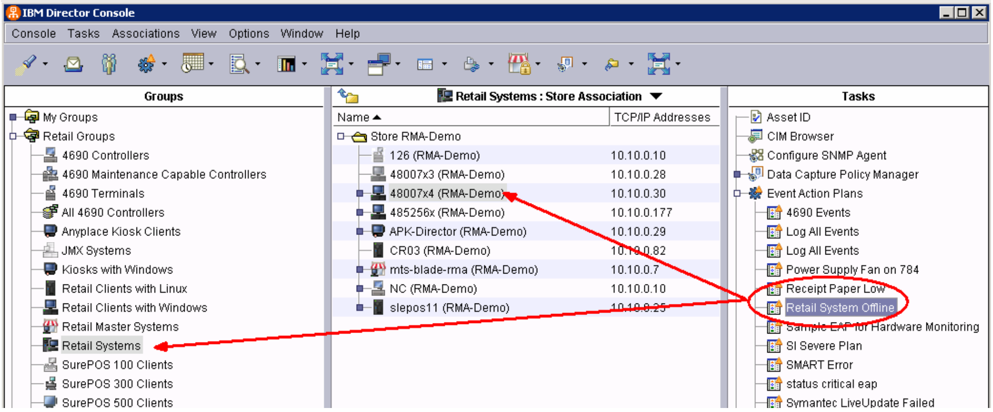


Event Action Plans

- Event Action Plan
  - 4690 Events
  - Log All Events
  - Log All Events
  - Power Supply Fan on 784
  - Receipt Paper Low
  - Retail System Offline
    - Offline Timer Expired
      - System Offline For 20 Minutes
    - Retail System Offline
      - Start Offline Timer
    - Retail System Online
      - Cancel Offline Timer
  - Sample EAP for Hardware Monitoring
  - SI Severe Plan

Now, there is an action plan that starts a timer when a system goes offline. If the system comes back online within a 20 minute window, the timer is canceled. If the system remains offline for more than 20 minutes, an alert is generated.

26. To apply your Event Action Plan, on the main IBM Director Console, drag and drop the plan to the system or group of systems that it applies to:



Groups

- My Groups
- Retail Groups
  - 4690 Controllers
  - 4690 Maintenance Capable Controllers
  - 4690 Terminals
  - All 4690 Controllers
  - Anyplace Kiosk Clients
  - JMX Systems
  - Kiosks with Windows
  - Retail Clients with Linux
  - Retail Clients with Windows
  - Retail Master Systems
  - Retail Systems
  - SurePOS 100 Clients
  - SurePOS 300 Clients
  - SurePOS 500 Clients

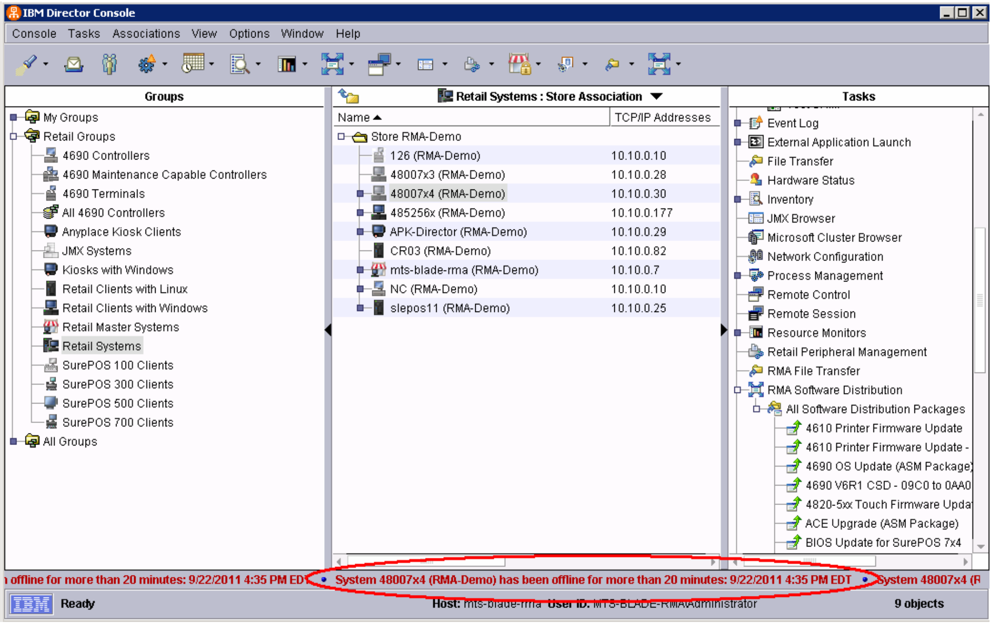
Retail Systems : Store Association

Name	TCP/IP Addresses
Store RMA-Demo	
126 (RMA-Demo)	10.10.0.10
48007x3 (RMA-Demo)	10.10.0.28
48007x4 (RMA-Demo)	10.10.0.30
485256x (RMA-Demo)	10.10.0.177
APK-Director (RMA-Demo)	10.10.0.29
CR03 (RMA-Demo)	10.10.0.82
mts-blade-rma (RMA-Demo)	10.10.0.7
NC (RMA-Demo)	10.10.0.10
slepos11 (RMA-Demo)	10.10.0.25

Tasks

- Asset ID
- CIM Browser
- Configure SNMP Agent
- Data Capture Policy Manager
- Event Action Plans
  - 4690 Events
  - Log All Events
  - Log All Events
  - Power Supply Fan on 784
  - Receipt Paper Low
  - Retail System Offline
  - Sample EAP for Hardware Monitoring
  - SI Severe Plan
  - SMART Error
  - status critical eap
  - Symantec LiveUpdate Failed

27. Now, if one of those systems is offline for more than 20 minutes, the scrolling ticker will activate:


IBM Director Console
Console Tasks Associations View Options Window Help
Groups
My Groups
Retail Groups
4690 Controllers
4690 Maintenance Capable Controllers
4690 Terminals
All 4690 Controllers
Anyplace Kiosk Clients
JMX Systems
Kiosks with Windows
Retail Clients with Linux
Retail Clients with Windows
Retail Master Systems
Retail Systems
SurePOS 100 Clients
SurePOS 300 Clients
SurePOS 500 Clients
SurePOS 700 Clients
All Groups
Retail Systems : Store Association
Tasks
Event Log
External Application Launch
File Transfer
Hardware Status
Inventory
JMX Browser
Microsoft Cluster Browser
Network Configuration
Process Management
Remote Control
Remote Session
Resource Monitors
Retail Peripheral Management
RMA File Transfer
RMA Software Distribution
All Software Distribution Packages
4610 Printer Firmware Update
4610 Printer Firmware Update -
4690 OS Update (ASM Package)
4690 V6R1 CSD - 09C0 to 0AA0
4820-5xx Touch Firmware Upda
ACE Upgrade (ASM Package)
BIOS Update for SurePOS 7x4

Name	TCP/IP Addresses
Store RMA-Demo	
126 (RMA-Demo)	10.10.0.10
48007x3 (RMA-Demo)	10.10.0.28
48007x4 (RMA-Demo)	10.10.0.30
485256x (RMA-Demo)	10.10.0.177
APK-Director (RMA-Demo)	10.10.0.29
CR03 (RMA-Demo)	10.10.0.82
mts-blade-rma (RMA-Demo)	10.10.0.7
NC (RMA-Demo)	10.10.0.10
slepos11 (RMA-Demo)	10.10.0.25

offline for more than 20 minutes: 9/22/2011 4:35 PM EDT • System 48007x4 (RMA-Demo) has been offline for more than 20 minutes: 9/22/2011 4:35 PM EDT • System 48007x4 (R

Ready Host: mts-blade-rma User ID: MTS-BLADE-RMA\Administrator 9 objects

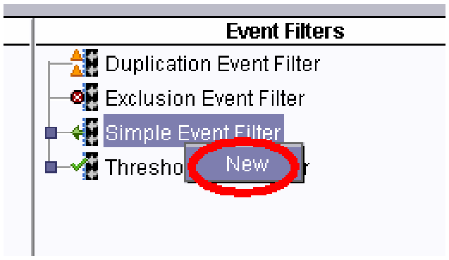
Example: Monitor S.M.A.R.T. events (hard drive predictive failure)

On Windows, it's possible to monitor for S.M.A.R.T. events that are forwarded to RMA via the CIM event forwarders for WMI. When a SMART-capable hard drive signals to the Windows operating system that a failure is predicted, an event is sent to WMI, which is then forwarded to RMA. This example shows you how to create an event filter to handle that event.

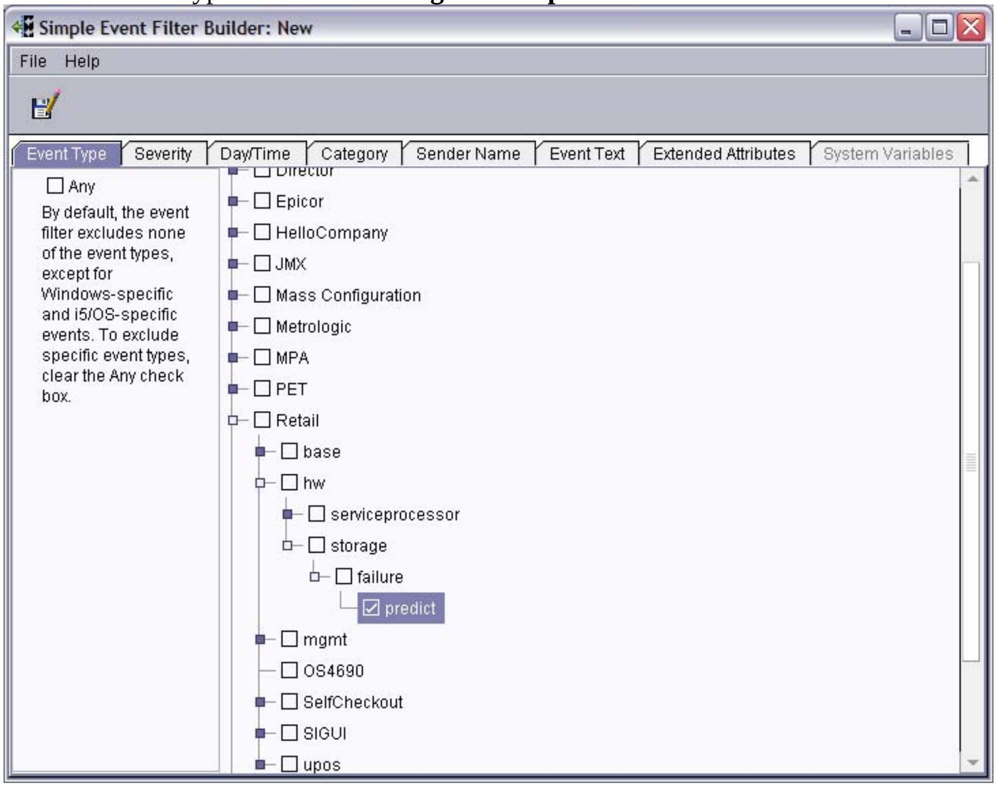
> **Note**: This example assumes you've already become familiar with the basics of creating an event filter and an event action plan. If not, you should first try "**Example: Create a Custom Group for Agents Offline**", and read the introduction to event management, before proceeding with this example.

Also note that there are several different ways to monitor for hard drive failures – including the "Resource Monitors" task, and via the service processor LED's for certain hardware models.

1. Create an event filter from scratch using the event action plans builder task. Right-click "Simple Event Filter", and select "New".



2. Select the event type “**Retail.hw.storage.failure.predict**”.



□ Any

By default, the event filter excludes none of the event types, except for Windows-specific and i5/OS-specific events. To exclude specific event types, clear the Any check box.

3. Finish selecting your criteria on the other tabs in the event filter (i.e. click “Any” for all the other tabs if you want this filter to apply broadly).

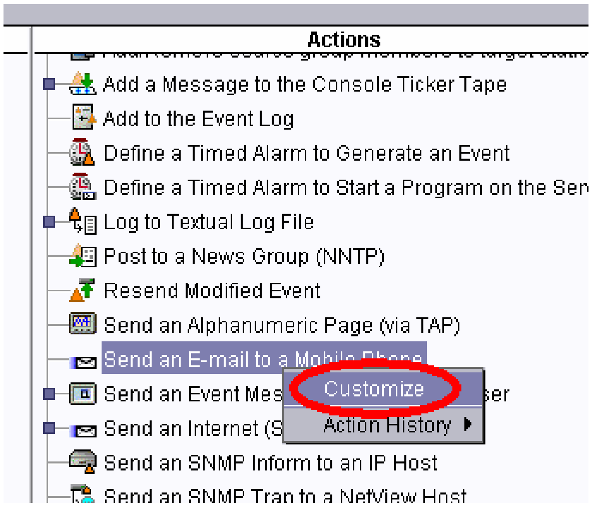
4. Save your filter, create an event action plan that uses this new event filter, then apply the EAP to the system(s) or group(s) that you want to monitor.

Example: Send message to a mobile cell phone

For critical events, you may want to configure Director to send an email to someone so the problem can be immediately addressed. Follow the instructions below to create an action (within the event action plans builder) that will send an email message to a mobile phone. (This can also be used to send messages to a normal email address.) This requires that an SMTP server is set up in the enterprise.

Note: This example assumes you've already become familiar with the basics of creating an event filter and an event action plan. If not, you should first try "**Example: Create a Custom Group for Agents Offline**", and read the introduction to event management, before proceeding with this example.

1. Open the event action plans builder task, and right-click on "Send an E-mail to a Mobile Phone" under "Actions". Select "Customize" from the drop-down menu.

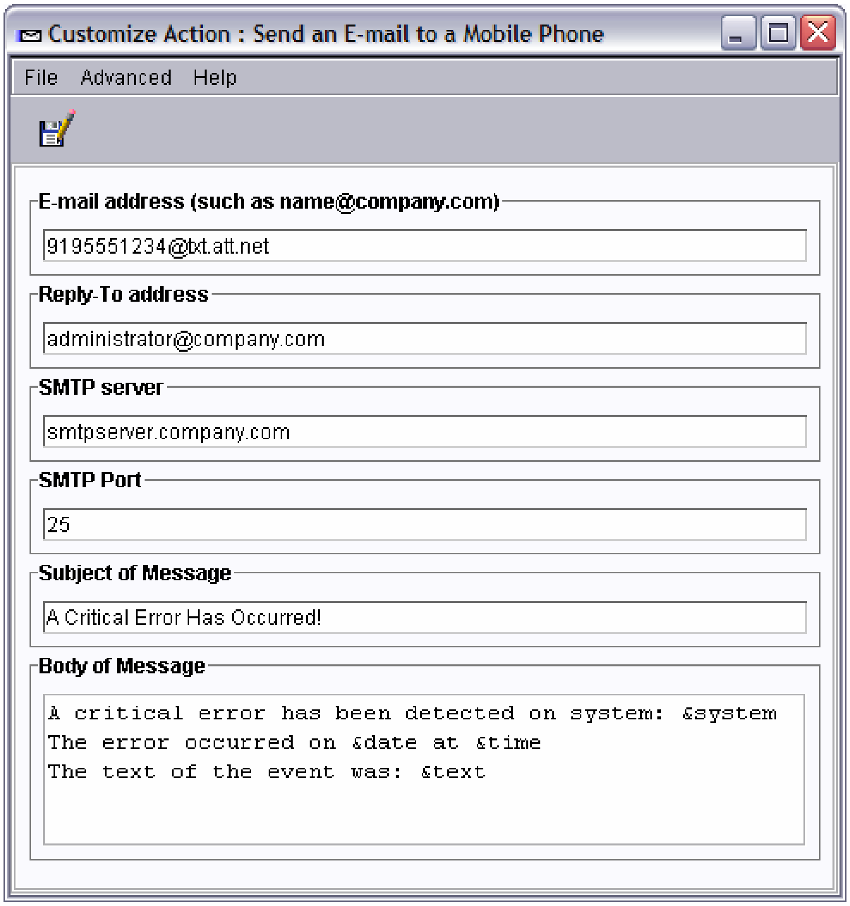

Actions
Add a Message to the Console Ticker Tape
Add to the Event Log
Define a Timed Alarm to Generate an Event
Define a Timed Alarm to Start a Program on the Ser
Log to Textual Log File
Post to a News Group (NNTP)
Resend Modified Event
Send an Alphanumeric Page (via TAP)
Send an E-mail to a Mobile Phone
Send an Event Mes
ser
Send an Internet (S
Send an SNMP Inform to an IP Host
Send an SNMP Trap to a NetView Host
Customize
Action History

2. Customize the action with the recipient's email address, the reply-to email address, and the other information requested.

Note: Most major phone service providers allow users to email a text message to a cell phone using a format similar to the following:

AT&T: number@txt.att.net
Verizon: number@vtext.com
Sprint: number@messaging.sprintpcs.com
T-Mobile: number@tmomail.net

So, in order to send a text message to AT&T number 888-123-4567 via email, a user would send an email to 8881234567@txt.att.net



E-mail address (such as name@company.com)
9195551234@txt.att.net

Reply-To address
administrator@company.com

SMTP server
smtpserver.company.com

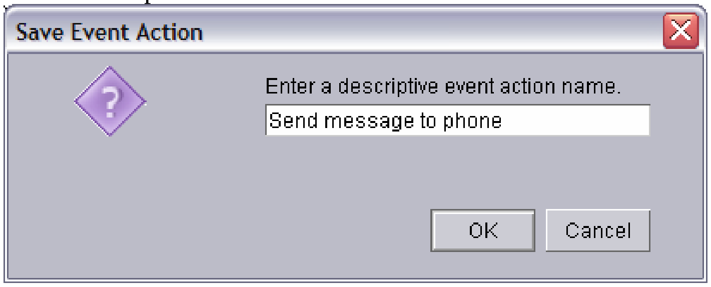
SMTP Port
25

Subject of Message
A Critical Error Has Occurred!

Body of Message

```
A critical error has been detected on system: &system
The error occurred on &date at &time
The text of the event was: &text
```

3. Save the action, then you can begin incorporating this action into any of your event action plans.



Enter a descriptive event action name.
Send message to phone

Example: Detect when telnet session started on 4690 controller

A telnet session gives a remote operator access to the 4690 console. It may be advisable to monitor this access to verify that this access is valid.

When the 4690 controller's telnet server is initiated an event with the text in the form "W893 Telnet connection from nnn.nnn.nnn" is logged to the 4690 system event log. The "nnn.nnn.nnn.nnn" is the IP address of the host initiating the connection. RMA can be used to provide alerts when this event is logged. (Several other system events track the progress of the telnet session showing the start and end times of the connection.)

To set this up, perform the following steps.

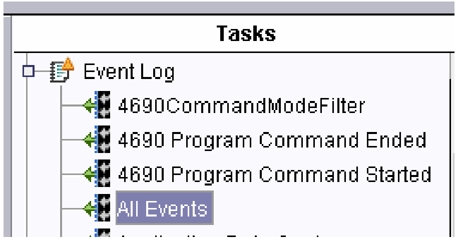
1. Define an event Filter
2. Define an event Action Plan
3. Associate the Event Action Plan with managed objects

In this example, a message will be added to the console ticker tape when a telnet session is detected.

Define an Event Filter

From any system on the network with a 4690 controller monitored by RMA, initiate a telnet session with that controller to generate the event to be monitored. A simple command like "telnet nnn.nnn.nnn.nnn", where nnn.nnn.nnn.nnn is the IP address of the controller will usually suffice. This can even be done from a command window on the controller itself.

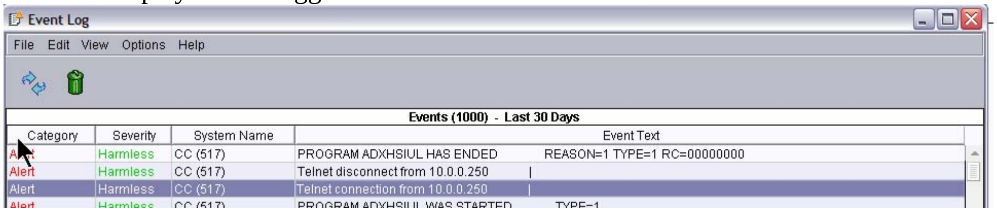
1. From the Director console, double click "All Events" in the task list.



Tasks

- Event Log
  - 4690CommandModeFilter
  - 4690 Program Command Ended
  - 4690 Program Command Started
  - All Events

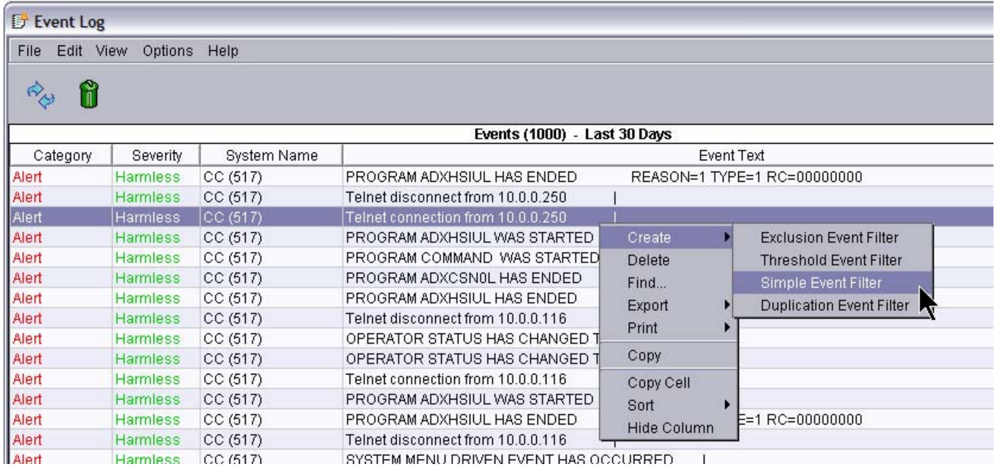
2. This will display events logged.



Events (1000) - Last 30 Days

Category	Severity	System Name	Event Text
Alert	Harmless	CC (517)	PROGRAM ADXHSIUL HAS ENDED REASON=1 TYPE=1 RC=00000000
Alert	Harmless	CC (517)	Telnet disconnect from 10.0.0.250 |
Alert	Harmless	CC (517)	Telnet connection from 10.0.0.250 |
Alert	Harmless	CC (517)	PROGRAM ADXHSIUL WAS STARTED TYPE=1

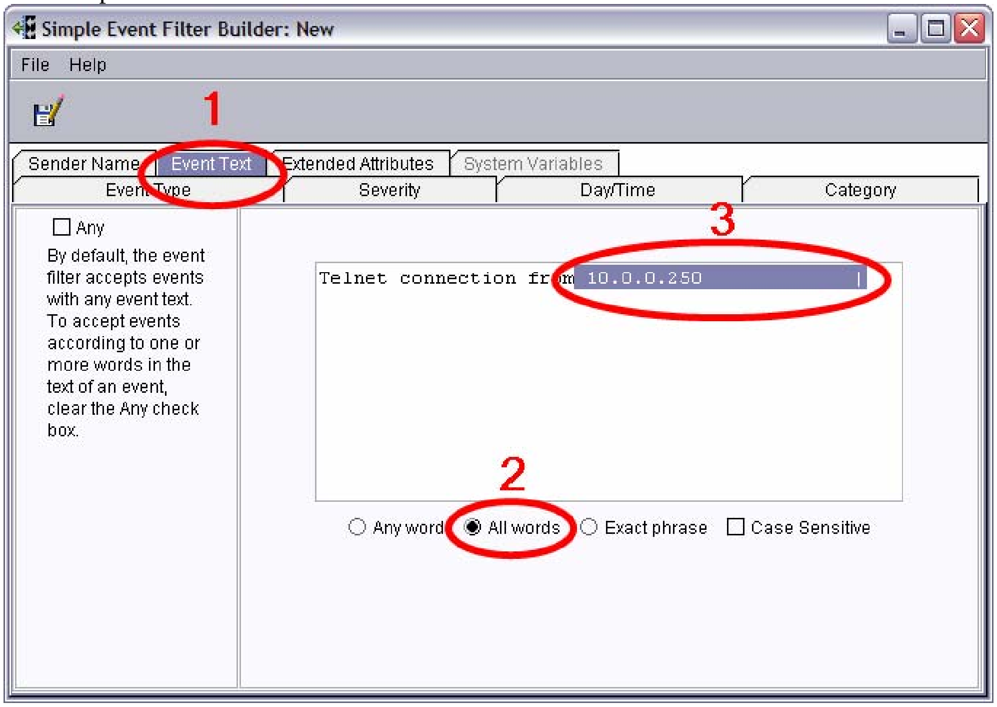
3. Right click the event of interest and select “Create” and then “Simple Filter”.



Events (1000) - Last 30 Days

Category	Severity	System Name	Event Text
Alert	Harmless	CC (517)	PROGRAM ADXHSIUL HAS ENDED REASON=1 TYPE=1 RC=00000000
Alert	Harmless	CC (517)	Telnet disconnect from 10.0.0.250 |
Alert	Harmless	CC (517)	Telnet connection from 10.0.0.250 |
Alert	Harmless	CC (517)	PROGRAM ADXHSIUL WAS STARTED
Alert	Harmless	CC (517)	PROGRAM COMMAND WAS STARTED
Alert	Harmless	CC (517)	PROGRAM ADXCSN0L HAS ENDED
Alert	Harmless	CC (517)	PROGRAM ADXHSIUL HAS ENDED
Alert	Harmless	CC (517)	Telnet disconnect from 10.0.0.116
Alert	Harmless	CC (517)	OPERATOR STATUS HAS CHANGED T
Alert	Harmless	CC (517)	OPERATOR STATUS HAS CHANGED T
Alert	Harmless	CC (517)	Telnet connection from 10.0.0.116
Alert	Harmless	CC (517)	PROGRAM ADXHSIUL WAS STARTED
Alert	Harmless	CC (517)	PROGRAM ADXHSIUL HAS ENDED E=1 RC=00000000
Alert	Harmless	CC (517)	Telnet disconnect from 10.0.0.116
Alert	Harmless	CC (517)	SYSTEM MENU DRIVEN EVENT HAS OCCURRED |

4. To define the filter (**1**) select the Event Text tab, (**2**) click the “All words” button, and (**3**) trim the text to “FTP connection from” by highlighting and deleting the variable portion of the text.



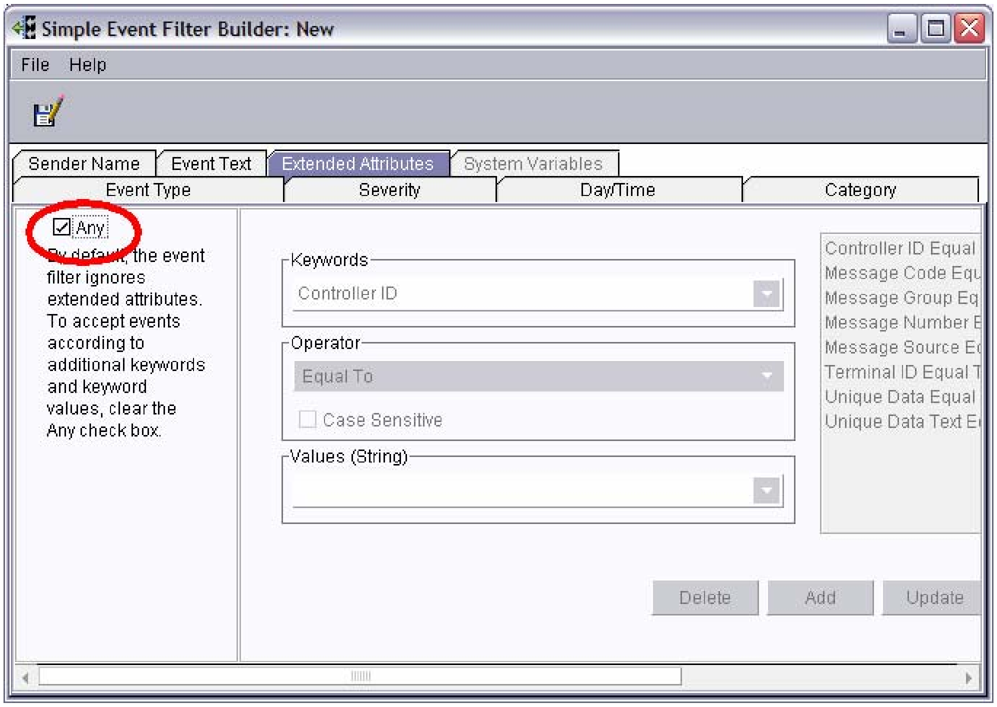
□ Any

By default, the event filter accepts events with any event text. To accept events according to one or more words in the text of an event, clear the Any check box.

Telnet connection from 10.0.0.250

○ Any word ● All words ○ Exact phrase □ Case Sensitive

5. If you are using 4690 V6, be sure to remove all the “extended attrbutes” from the event filter. The simplest way to ignore all the extended attributes is to click “Any” on that tab.



☑ Any

By default, the event filter ignores extended attributes. To accept events according to additional keywords and keyword values, clear the Any check box.

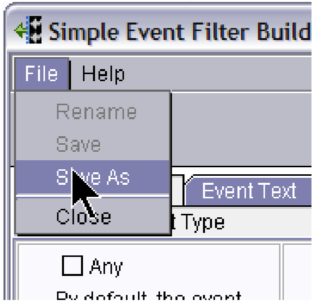
Keywords: Controller ID

Operator: Equal To

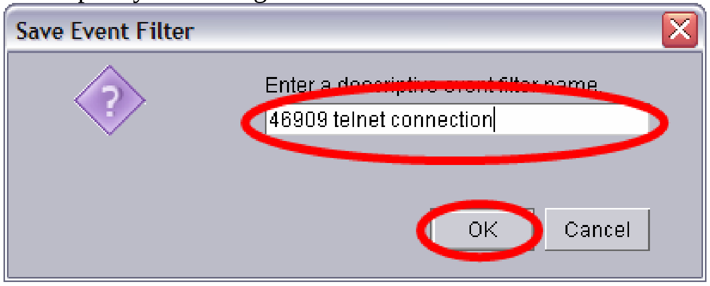
□ Case Sensitive

Controller ID Equal
Message Code Equ
Message Group Eq
Message Number E
Message Source E
Terminal ID Equal T
Unique Data Equal
Unique Data Text E

6. To save the filter, click file and “Save as”.



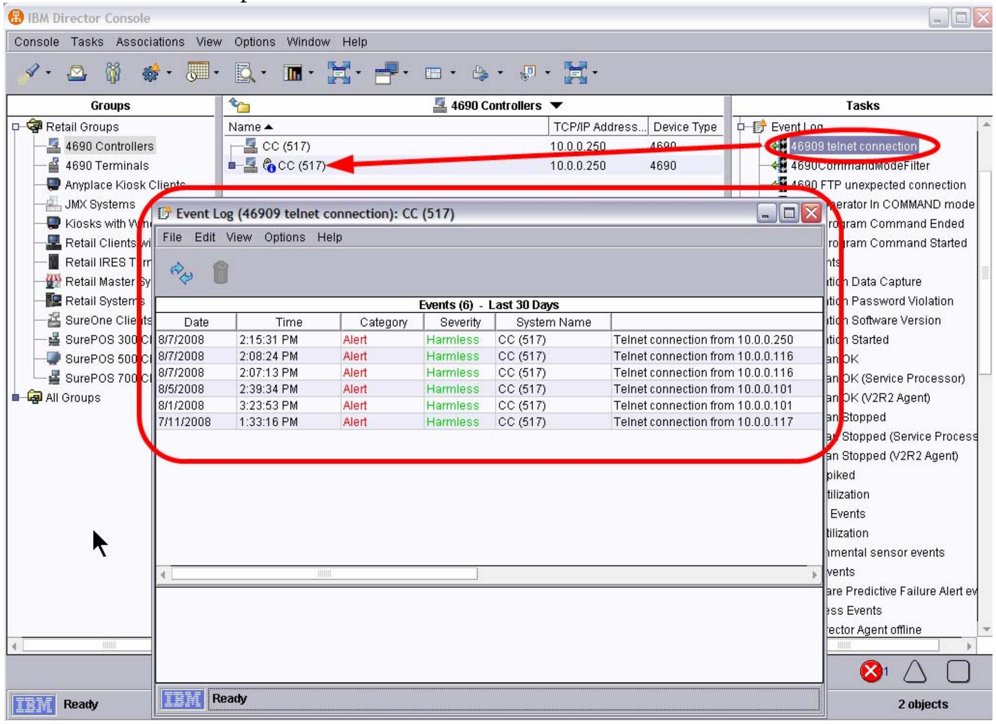
7. Then specify a meaningful name for the filter and click OK.



Enter a descriptive event filter name

46909 telnet connection

8. To verify that the filter is properly defined, expand Event Log under Tasks on the IBM director console and drag the filter to the 4690 controller on which the event was created. The sample event and all like it should be listed.



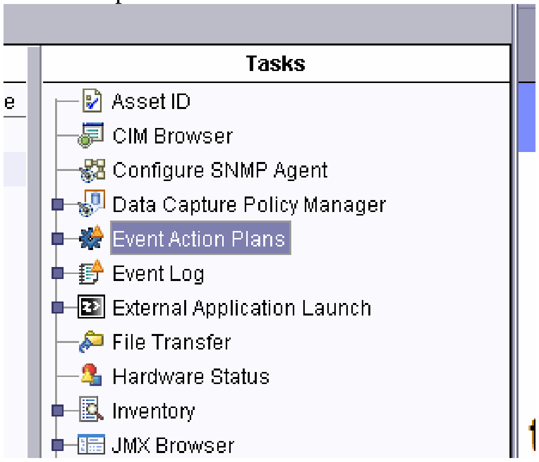
Event Log (46909 telnet connection): CC (517)

Events (6) - Last 30 Days

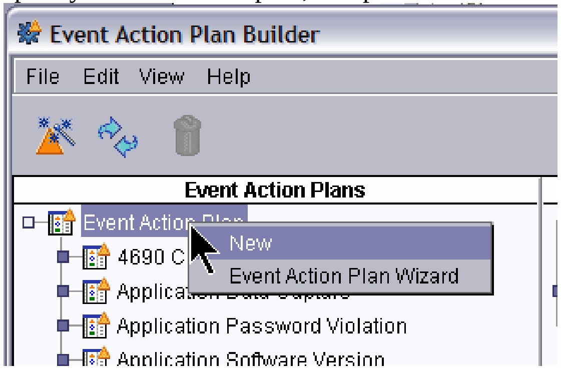
Date	Time	Category	Severity	System Name	
8/7/2008	2:15:31 PM	Alert	Harmless	CC (517)	Telnet connection from 10.0.0.250
8/7/2008	2:08:24 PM	Alert	Harmless	CC (517)	Telnet connection from 10.0.0.116
8/7/2008	2:07:13 PM	Alert	Harmless	CC (517)	Telnet connection from 10.0.0.116
8/5/2008	2:39:34 PM	Alert	Harmless	CC (517)	Telnet connection from 10.0.0.101
8/1/2008	3:23:53 PM	Alert	Harmless	CC (517)	Telnet connection from 10.0.0.101
7/11/2008	1:33:16 PM	Alert	Harmless	CC (517)	Telnet connection from 10.0.0.117

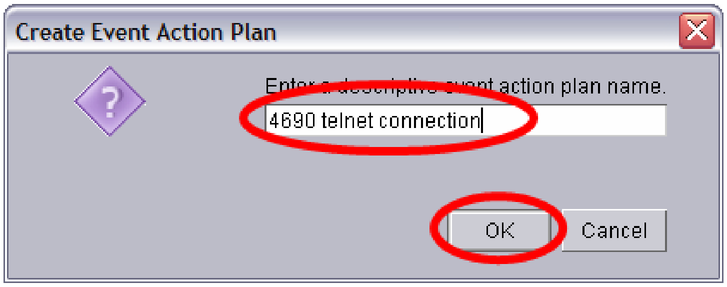
Define an Event Action Plan

1. Launch the Event Action Plan Builder by double clicking “Event Action Plans” in the Tasks pain of the IBM Director console.



2. To create a new action plan, right click “Event Action Plan”, select “New”, specify a name for the plan, and press “OK”.

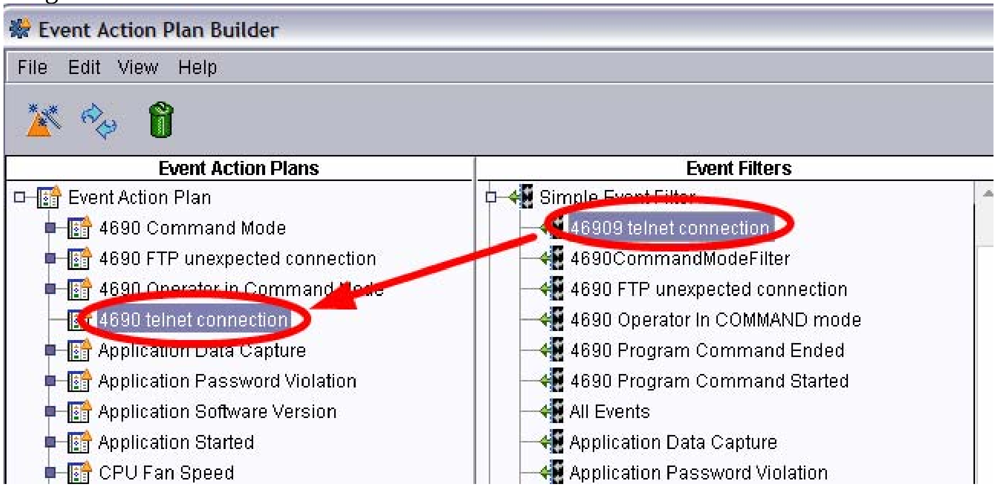



Create Event Action Plan

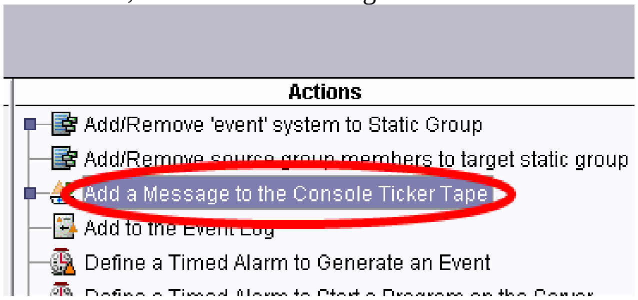
Enter a descriptive event action plan name.

4690 telnet connection

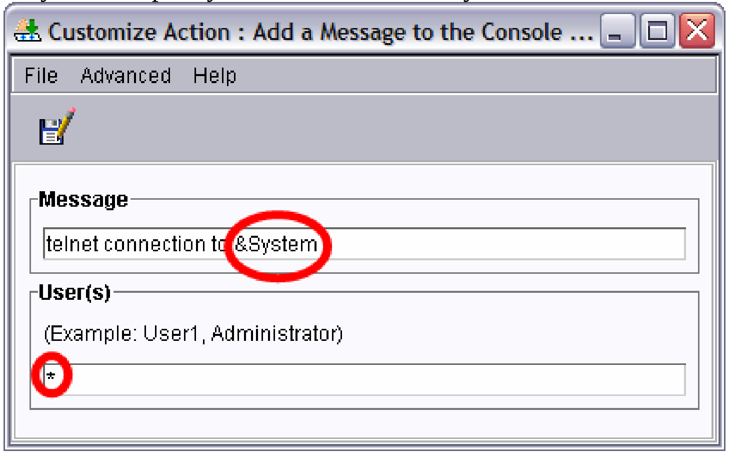
3. Drag the event filter to the Event Action Plan.


Event Action Plan Builder
File Edit View Help
Event Action Plans
Event Action Plan
4690 Command Mode
4690 FTP unexpected connection
4690 Operator in Command Mode
4690 telnet connection
Application Data Capture
Application Password Violation
Application Software Version
Application Started
CPU Fan Speed
Event Filters
Simple Event Filter
46909 telnet connection
4690CommandModeFilter
4690 FTP unexpected connection
4690 Operator In COMMAND mode
4690 Program Command Ended
4690 Program Command Started
All Events
Application Data Capture
Application Password Violation

4. Choose an action from the list in the right pane, right click it, and select customize. In this case, we will add a message to the Console Ticker Tape.


Actions
Add/Remove 'event' system to Static Group
Add/Remove source group members to target static group
Add a Message to the Console Ticker Tape
Add to the Event Log
Define a Timed Alarm to Generate an Event
Define a Timed Alarm to Start a Program on the Server

5. Specify text to be displayed and specify all users with a ‘*’. Note the use of &System to specify that the name of the system is to be included in the text.


Customize Action : Add a Message to the Console ...
File Advanced Help
(Example: User1, Administrator)

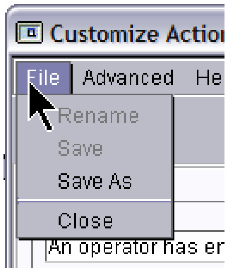
Message

telnet connection to &System

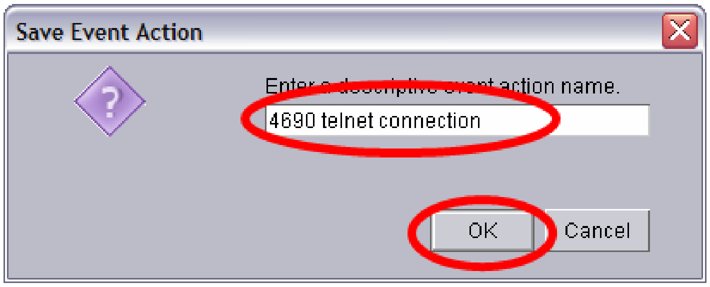
User(s)

*

6. Click “File” and select “Save as” to give action a name and save it.



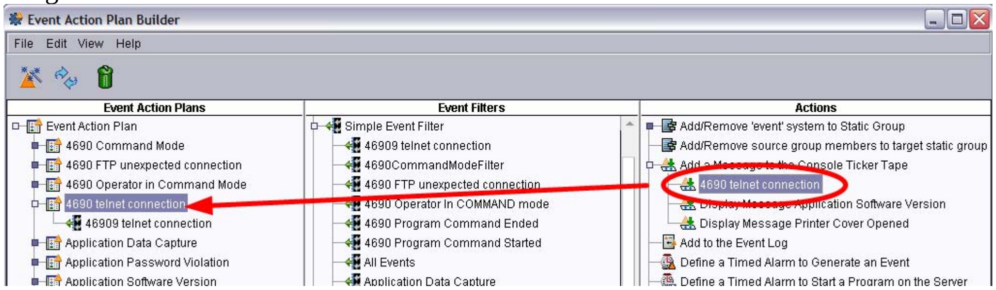
An operator has er



Enter a descriptive event action name.

4690 telnet connection

7. Drag the action created to the Event Action Plan.



Event Action Plans:

- Event Action Plan
  - 4690 Command Mode
  - 4690 FTP unexpected connection
  - 4690 Operator in Command Mode
  - 4690 telnet connection
    - 46909 telnet connection
  - Application Data Capture
  - Application Password Violation
  - Application Software Version

Event Filters:

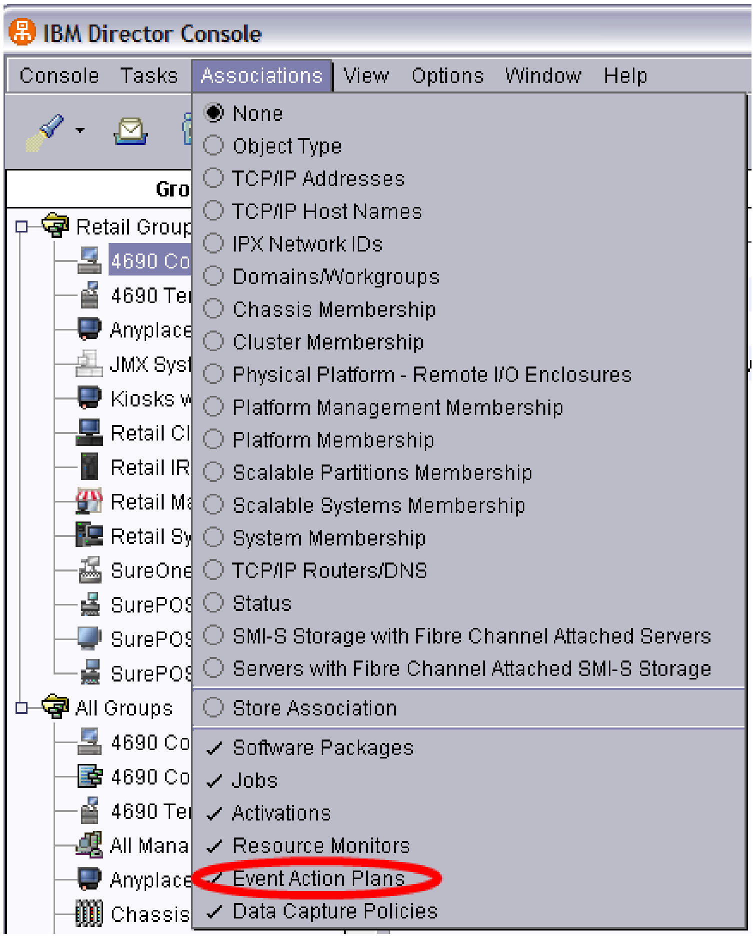
- Simple Event Filter
  - 46909 telnet connection
  - 4690CommandModeFilter
  - 4690 FTP unexpected connection
  - 4690 Operator In COMMAND mode
  - 4690 Program Command Ended
  - 4690 Program Command Started
  - All Events
  - Application Data Capture

Actions:

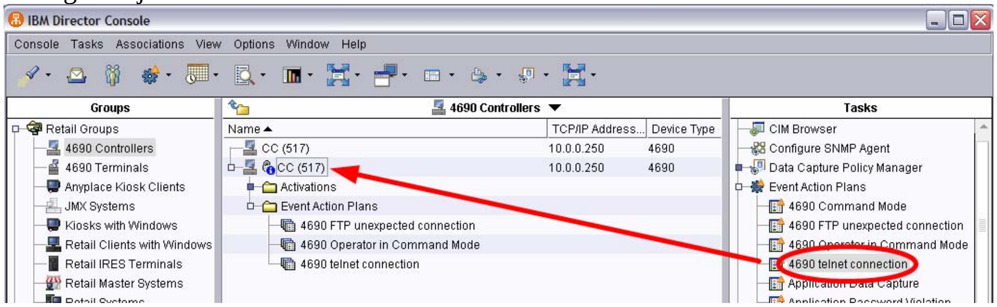
- Add/Remove 'event' system to Static Group
- Add/Remove source group members to target static group
- Add a Message to the Console Ticker Tape
  - 4690 telnet connection
  - Display Message Application Software Version
  - Display Message Printer Cover Opened
- Add to the Event Log
- Define a Timed Alarm to Generate an Event
- Define a Timed Alarm to Start a Program on the Server

Associate Event Action Plan with Managed Objects

1. Make sure “Event Action Plans” is checked in the Associations menu.

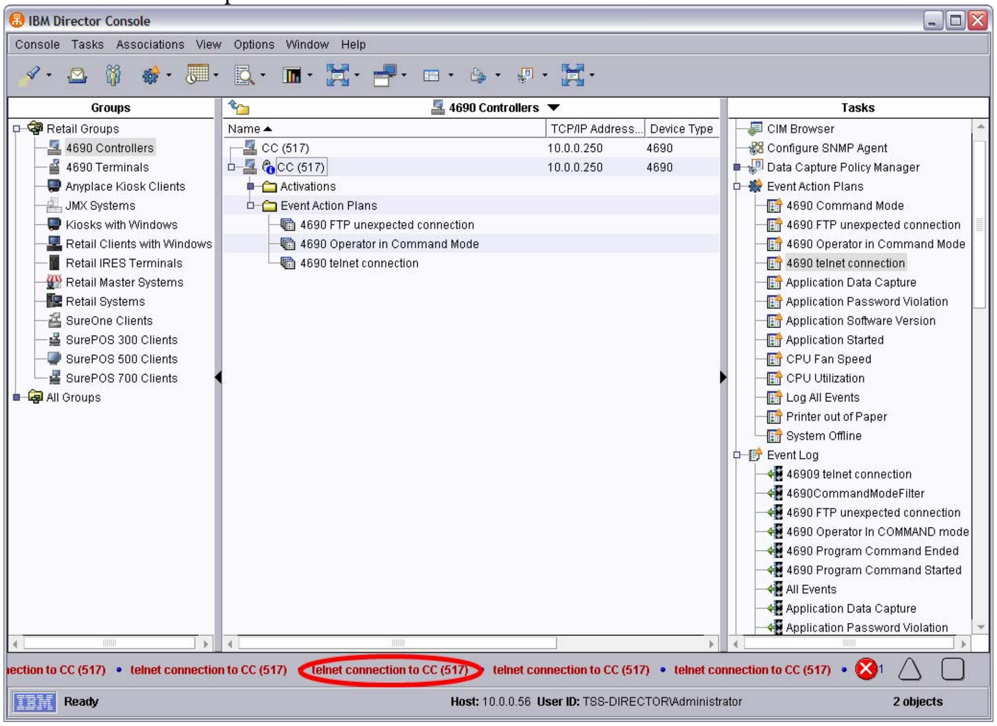


2. Associate the new event action plan with a group, managed object, or selection of managed objects.



Name	TCP/IP Address...	Device Type
CC (517)	10.0.0.250	4690
CC (517)	10.0.0.250	4690

3. Test the event action plan by initiating a telnet connection to the 4690 controller with which the action plan is associated. The message will start being displayed in the console ticker tape.

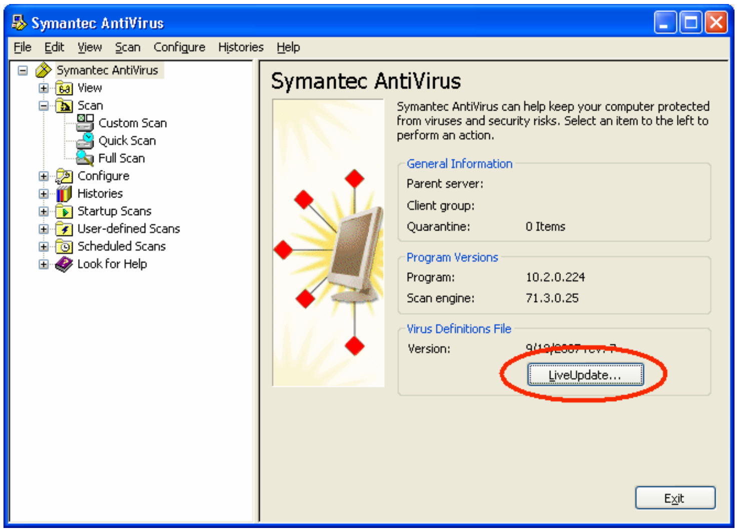


Example: Monitoring for Antivirus events from the Windows Event Log

This example will walk you through configuring RMA to forward all events from the "Symantec Antivirus" application to IBM Director.

> **Note**: This example assumes you've already become familiar with the basics of creating an event filter and an event action plan. If not, you should first try "**Example: Create a Custom Group for Agents Offline**", and read the introduction to event management, before proceeding with this example.

1. The first thing to do is to generate an example of the event in the Windows event log. To do so, disconnect the system from the internet and attempt to update the antivirus definitions. Specifically, open the Symantec Antivirus application (e.g. double-click on the icon in the task tray), then click the "LiveUpdate":



Symantec AntiVirus

Symantec AntiVirus can help keep your computer protected from viruses and security risks. Select an item to the left to perform an action.

General Information

Parent server:

Client group:

Quarantine: 0 Items

Program Versions

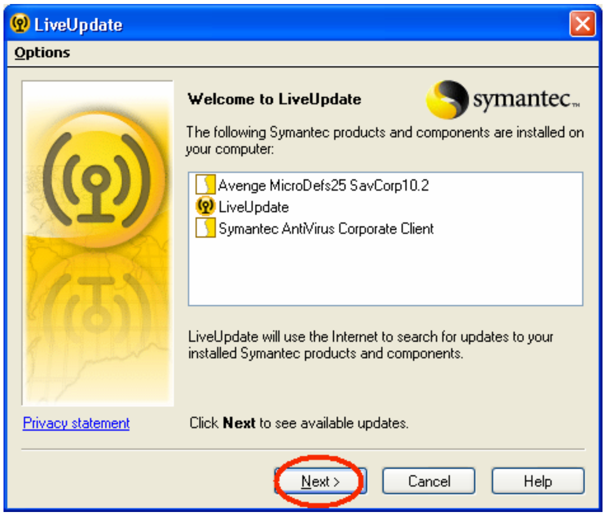
Program: 10.2.0.224

Scan engine: 71.3.0.25

Virus Definitions File

Version: 9/19/2007 rev. 7

2. Continue the LiveUpdate process (e.g. by clicking "Next") until you see a message stating that it has failed.



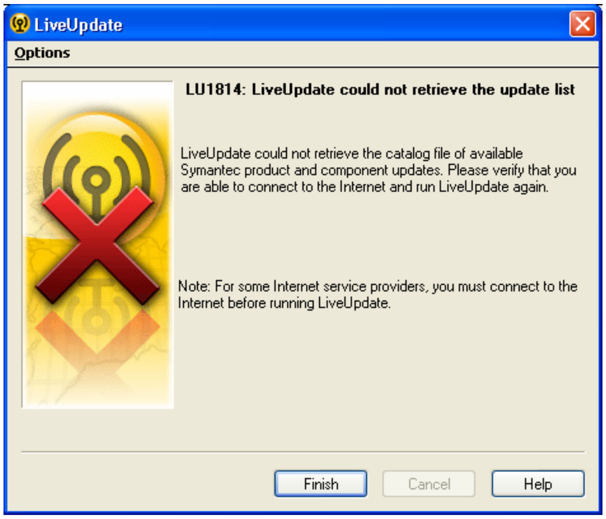
Welcome to LiveUpdate

The following Symantec products and components are installed on your computer:

- Avenge MicroDefs25 SavCorp10.2
- LiveUpdate
- Symantec AntiVirus Corporate Client

LiveUpdate will use the Internet to search for updates to your installed Symantec products and components.

Click **Next** to see available updates.

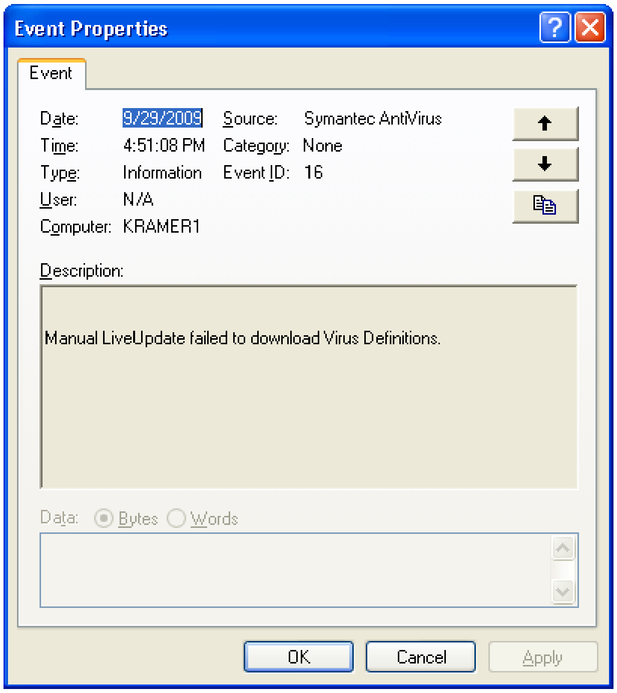


LU1814: LiveUpdate could not retrieve the update list

LiveUpdate could not retrieve the catalog file of available Symantec product and component updates. Please verify that you are able to connect to the Internet and run LiveUpdate again.

Note: For some Internet service providers, you must connect to the Internet before running LiveUpdate.

3. Next, open the Windows Event Log (Start → Control Panel → Administrative Tools → Event Viewer), and select the "Application" event log category. Locate the Symantec event and double-click it to view its properties:

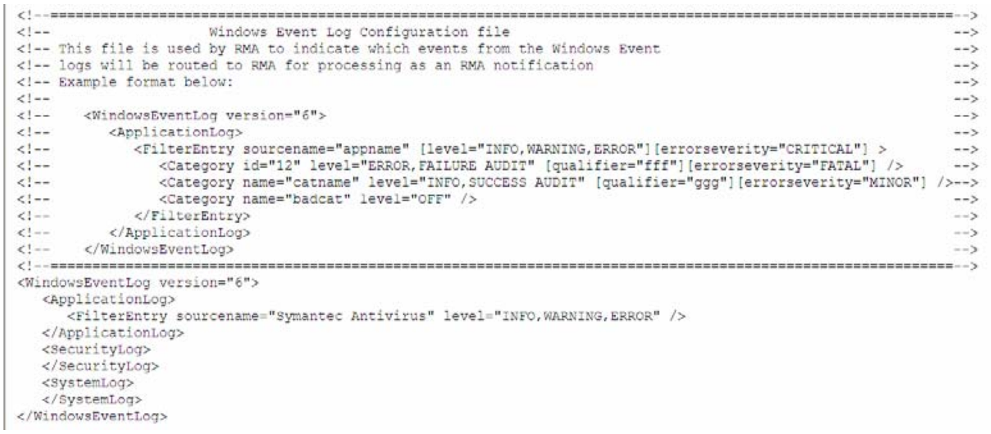


Date: 9/29/2009 Source: Symantec AntiVirus
Time: 4:51:08 PM Category: None
Type: Information Event ID: 16
User: N/A
Computer: KRAMER1

Description:

Manual LiveUpdate failed to download Virus Definitions.

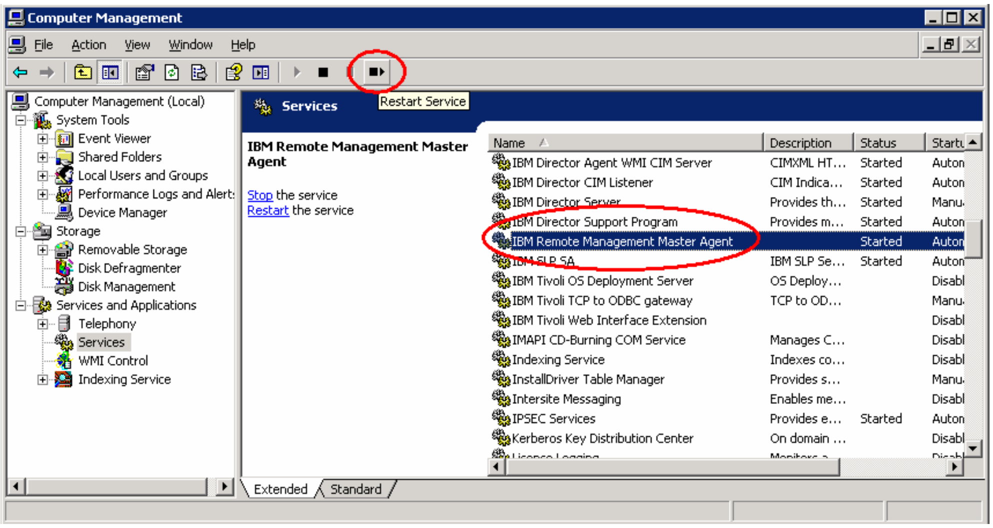
4. Next, modify the Win32EventLogConfig.xml on your RMA Agent system found in "C:\Program Files\IBM\StoreIntegrator\user\rma\config\events" to add a <FilterEntry> tag for the Symantec Antivirus program:



```
<!--==============================================================================================================-->
<!--                   Windows Event Log Configuration file                                                       -->
<!-- This file is used by RMA to indicate which events from the Windows Event                                     -->
<!-- logs will be routed to RMA for processing as an RMA notification                                             -->
<!-- Example format below:                                                                                        -->
<!--                                                                                                              -->
<!--    <WindowsEventLog version="6">                                                                             -->
<!--       <ApplicationLog>                                                                                       -->
<!--          <FilterEntry sourcename="appname" [level="INFO,WARNING,ERROR"][errorseverity="CRITICAL"] >          -->
<!--             <Category id="12" level="ERROR,FAILURE AUDIT" [qualifier="fff"][errorseverity="FATAL"] />        -->
<!--             <Category name="catname" level="INFO,SUCCESS AUDIT" [qualifier="ggg"][errorseverity="MINOR"] />-->
<!--             <Category name="badcat" level="OFF" />                                                           -->
<!--          </FilterEntry>                                                                                      -->
<!--       </ApplicationLog>                                                                                      -->
<!--    </WindowsEventLog>                                                                                        -->
<!--==============================================================================================================-->
<WindowsEventLog version="6">
   <ApplicationLog>
      <FilterEntry sourcename="Symantec Antivirus" level="INFO,WARNING,ERROR" />
   </ApplicationLog>
   <SecurityLog>
   </SecurityLog>
   <SystemLog>
   </SystemLog>
</WindowsEventLog>
```

Note: Before using this XML file with RMA, it is important to double-check for typing errors and to verify that the XML file is "well-formed". To do so, simply double-click the XML file within Windows Explorer and it should open using your web browser. If the file appears in a "tree view" (i.e. you can expand or collapse the individual elements) without errors, then the XML file is "well-formed" and you are ready to use the file with RMA.

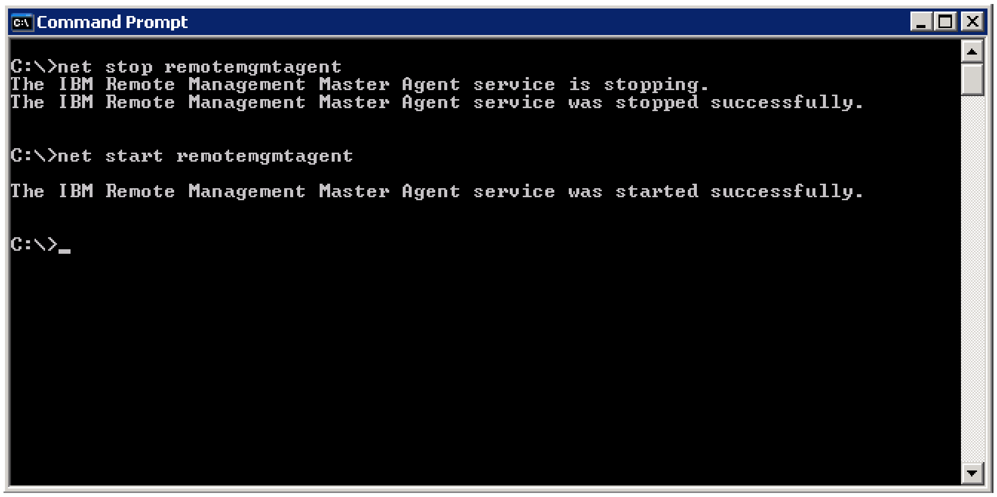
5. When finished, save the file and restart the RMA Agent so that the changes can take effect. This can be done from the Windows Services menu, or from a command line:



IBM Remote Management Master Agent

Stop the service
Restart the service

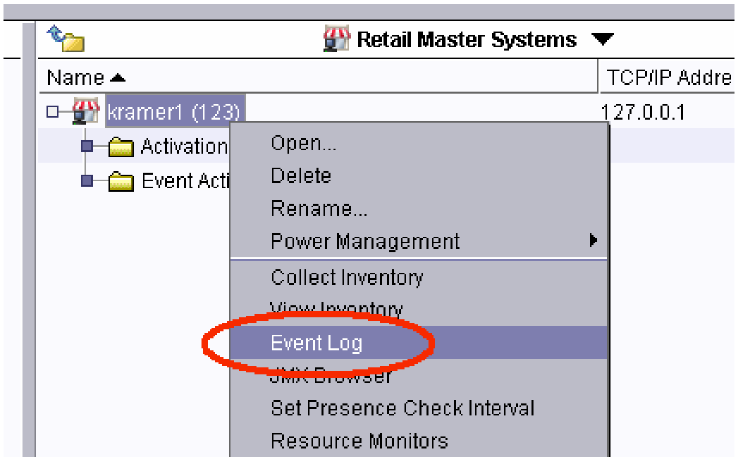
Name	Description	Status	Startu
IBM Director Agent WMI CIM Server	CIMXML HT…	Started	Auton
IBM Director CIM Listener	CIM Indica…	Started	Auton
IBM Director Server	Provides th…	Started	Manu
IBM Director Support Program	Provides m…	Started	Auton
IBM Remote Management Master Agent		Started	Auton
IBM SLP SA	IBM SLP Se…	Started	Auton
IBM Tivoli OS Deployment Server	OS Deploy…		Disabl
IBM Tivoli TCP to ODBC gateway	TCP to OD…		Manu
IBM Tivoli Web Interface Extension			Disabl
IMAPI CD-Burning COM Service	Manages C…		Disabl
Indexing Service	Indexes co…		Disabl
InstallDriver Table Manager	Provides s…		Manu
Intersite Messaging	Enables me…		Disabl
IPSEC Services	Provides e…	Started	Auton
Kerberos Key Distribution Center	On domain …		Disabl
Licence Logging	Monitors a…		Disabl



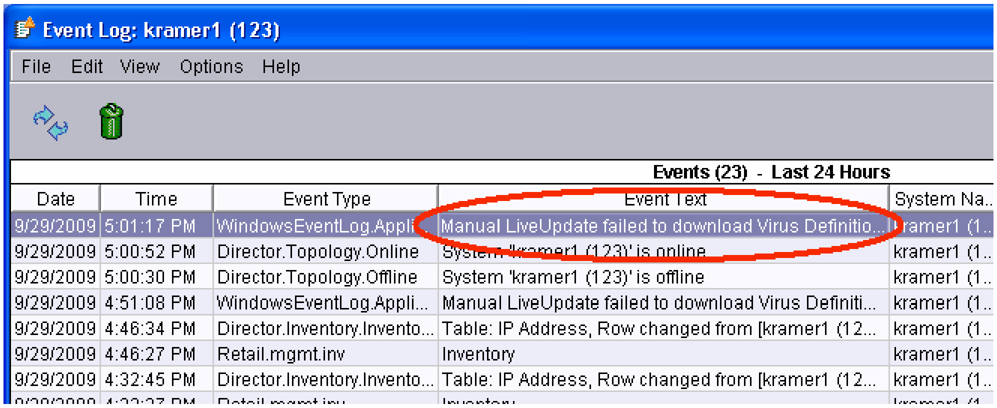
```
C:\>net stop remotemgmtagent
The IBM Remote Management Master Agent service is stopping.
The IBM Remote Management Master Agent service was stopped successfully.

C:\>net start remotemgmtagent

The IBM Remote Management Master Agent service was started successfully.

C:\>_
```

6. After the RMA Agent is restarted, repeat steps 1 and 2 to regenerate the Symantec Antivirus event.

7. From the Director Console, open the event log for the RMA system where you generated the Symantec event.



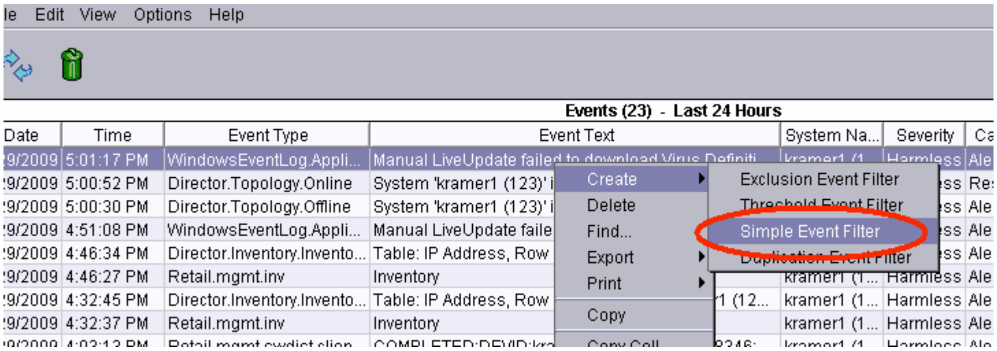
8. You should be able to find the Symantec event in the Director event log:



Events (23) - Last 24 Hours

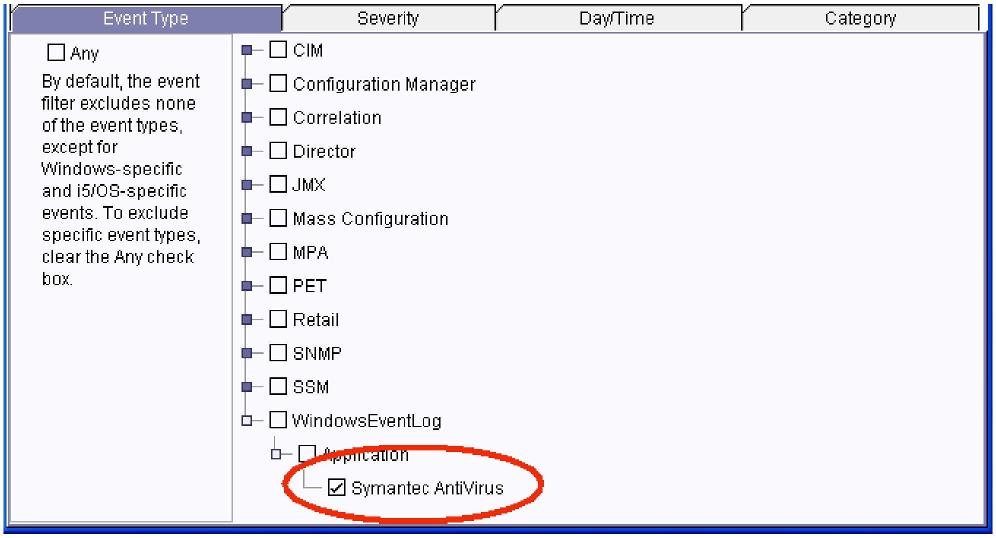
Date	Time	Event Type	Event Text	System Na...
9/29/2009	5:01:17 PM	WindowsEventLog.Appli	Manual LiveUpdate failed to download Virus Definitio...	kramer1 (1...
9/29/2009	5:00:52 PM	Director.Topology.Online	System 'kramer1 (123)' is online	kramer1 (1...
9/29/2009	5:00:30 PM	Director.Topology.Offline	System 'kramer1 (123)' is offline	kramer1 (1...
9/29/2009	4:51:08 PM	WindowsEventLog.Appli...	Manual LiveUpdate failed to download Virus Definiti...	kramer1 (1...
9/29/2009	4:46:34 PM	Director.Inventory.Invento...	Table: IP Address, Row changed from [kramer1 (12...	kramer1 (1...
9/29/2009	4:46:27 PM	Retail.mgmt.inv	Inventory	kramer1 (1...
9/29/2009	4:32:45 PM	Director.Inventory.Invento...	Table: IP Address, Row changed from [kramer1 (12...	kramer1 (1...

9. You can now use this event as a template to create an Event Filter for the Symantec Antivirus application and an Event Action Plan as you did in the previous examples. Also note that the event type in the event filter will be populated with the source application from the Windows Event Log: "WindowsEventLog.Application.Symantec Antivirus"



Events (23) - Last 24 Hours

Date	Time	Event Type	Event Text	System Na...	Severity	Ca
9/2009	5:01:17 PM	WindowsEventLog.Appli...	Manual LiveUpdate failed to download Virus Definiti	kramer1 (1	Harmless	Ale
9/2009	5:00:52 PM	Director.Topology.Online	System 'kramer1 (123)' i		ss	Re
9/2009	5:00:30 PM	Director.Topology.Offline	System 'kramer1 (123)' i		ss	Ale
9/2009	4:51:08 PM	WindowsEventLog.Appli...	Manual LiveUpdate faile		ss	Ale
9/2009	4:46:34 PM	Director.Inventory.Invento...	Table: IP Address, Row		ss	Ale
9/2009	4:46:27 PM	Retail.mgmt.inv	Inventory	kramer1 (1...	Harmless	Ale
9/2009	4:32:45 PM	Director.Inventory.Invento...	Table: IP Address, Row 1 (12...	kramer1 (1...	Harmless	Ale
9/2009	4:32:37 PM	Retail.mgmt.inv	Inventory	kramer1 (1...	Harmless	Ale



□ Any

By default, the event filter excludes none of the event types, except for Windows-specific and i5/OS-specific events. To exclude specific event types, clear the Any check box.

- □ CIM
- □ Configuration Manager
- □ Correlation
- □ Director
- □ JMX
- □ Mass Configuration
- □ MPA
- □ PET
- □ Retail
- □ SNMP
- □ SSM
- □ WindowsEventLog
  - □ Application
    - ☑ Symantec AntiVirus

Chapter 7 – Resource Monitoring

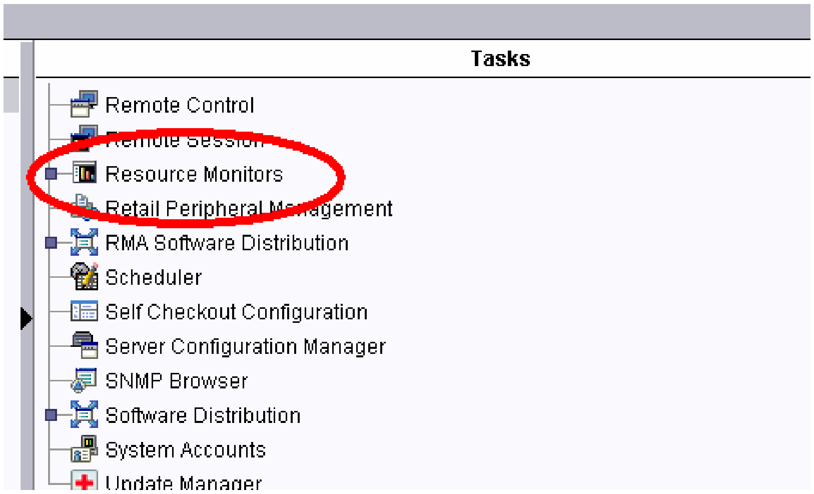
This chapter explains how to use the "Resource Monitors" task in IBM Director for RMA agents, which allows you to define thresholds for proactively monitoring the attributes on your remote retail systems. For example, you can monitor the system for low disk space, or monitor the health of the motherboard or power supply.

Introduction to Resource Monitoring

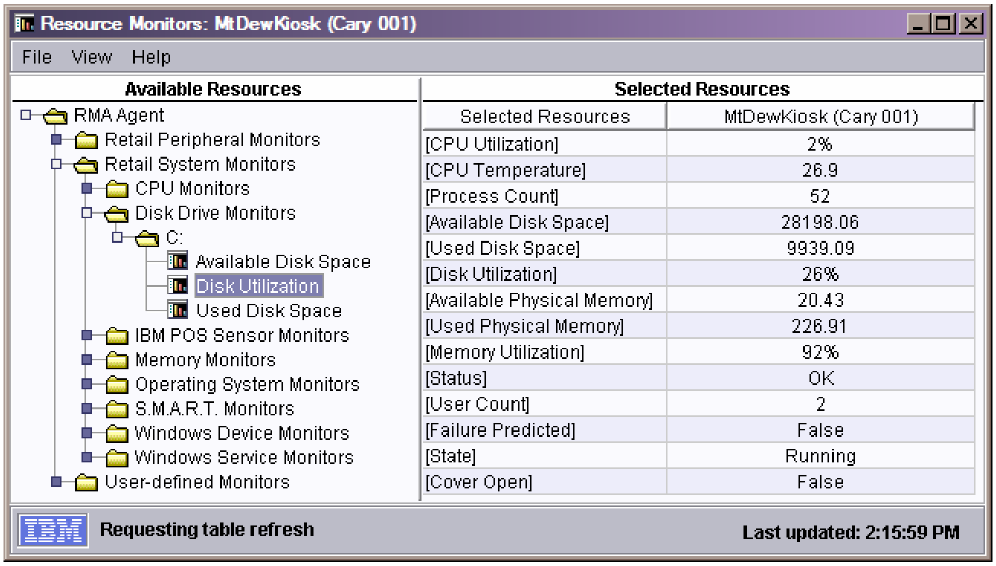
Resource monitors task

The "Resource Monitors" task appears in the tasks pane in the Director Console, and can be launched like any other task, using any of the following methods:

- Drag-and-drop (to a group, a single managed object, or a selection of multiple groups or MO's)
- Right-click a selection of MO's or groups, and use the context menu to select "Resource Monitors"
- Use the console toolbar or "tasks" menu



Once you launch the resource monitors task, you will see the "Resource Monitors" window appear, as shown below.



Selected Resources	MtDewKiosk (Cary 001)
[CPU Utilization]	2%
[CPU Temperature]	26.9
[Process Count]	52
[Available Disk Space]	28198.06
[Used Disk Space]	9939.09
[Disk Utilization]	26%
[Available Physical Memory]	20.43
[Used Physical Memory]	226.91
[Memory Utilization]	92%
[Status]	OK
[User Count]	2
[Failure Predicted]	False
[State]	Running
[Cover Open]	False

Requesting table refresh

Last updated: 2:15:59 PM

To view the available monitors, you can expand the tree on the left to locate a resource monitor. Then, double-click an attribute in the tree to show the current/live value on the right-hand side of the screen.

Once you have added attributes to your “Selected Resources” (on the right-hand side of the screen), you can then right-click any value (on the right), to define a threshold (individual or group). You can also initiate recording of the value by right-clicking.

Pre-defined / Default Monitors

When you open the resource monitors task, you will find a number of attributes listed under “Available Resources”.

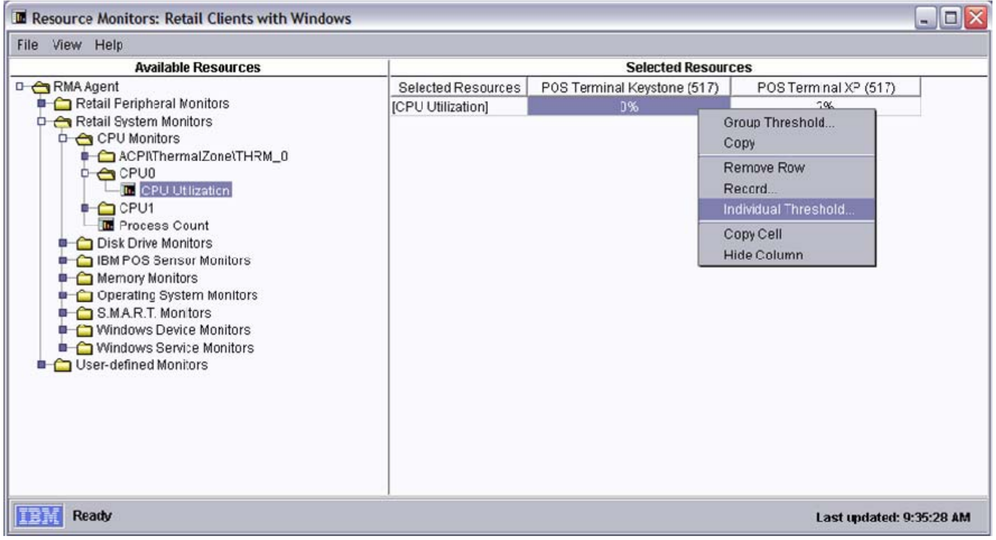
Here are a few examples:

- Retail System Monitors
  - CPU monitors
  - Disk drive monitors
  - IBM POS sensor monitors (requires separate installation of sensor drivers)
  - Memory monitors
  - Operating system monitors
  - S.M.A.R.T. monitors
  - Windows device monitors
  - Windows service monitors
- Retail Peripheral Monitors – defined per peripheral device type, both general and device-specific monitors are available
- Self-Checkout Monitors (for use with IBM CHEC software)

Creating single and group thresholds

Defining an “individual threshold”

Right-click a value (i.e. underneath the column of the system for which you want to define the threshold), then select “Individual Threshold”. In this example, the threshold will apply to “POS Terminal Keystone”:



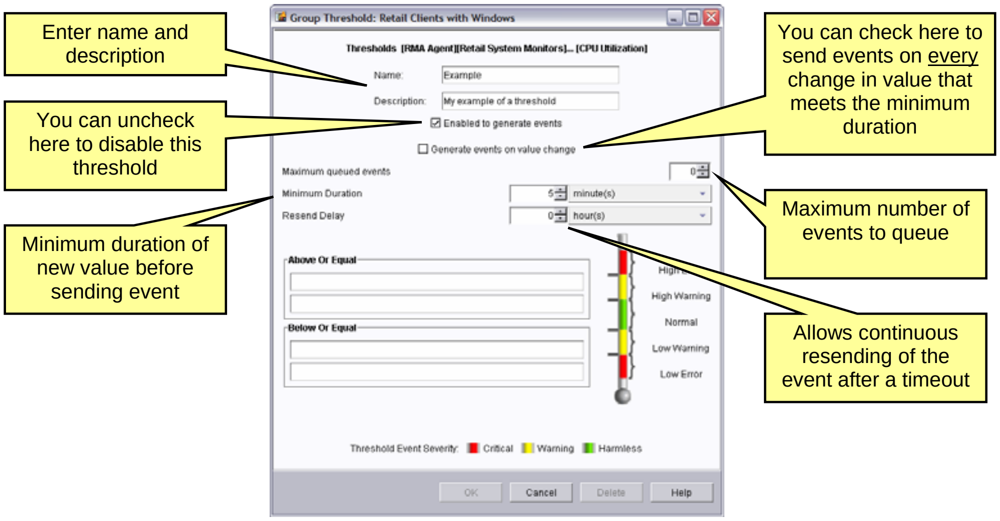
Resource Monitors: Retail Clients with Windows

Selected Resources	POS Terminal Keystone (517)	POS Terminal XP (517)
[CPU Utilization]	0%	0%

Ready

Last updated: 9:35:28 AM

To define the threshold, enter the appropriate values into the threshold configuration window, as shown below:



Group Threshold: Retail Clients with Windows

Thresholds [RMA Agent][Retail System Monitors]... [CPU Utilization]

Name: Example

Description: My example of a threshold

☑ Enabled to generate events

☐ Generate events on value change

Maximum queued events: 0

Minimum Duration: 5 minute(s)

Resend Delay: 0 hour(s)

Enter name and description

You can uncheck here to disable this threshold

Minimum duration of new value before sending event

You can check here to send events on every change in value that meets the minimum duration

Maximum number of events to queue

Allows continuous resending of the event after a timeout

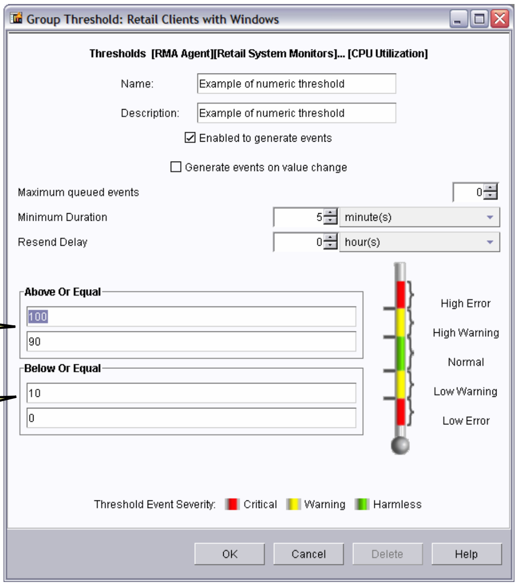
There are 2 different types of thresholds:

- Numeric thresholds – generates events of appropriate severity when value is above or below certain configured numerical ranges
- String thresholds – generates events when a value matches or differs from defined value sets

For numeric thresholds, you can define 4 different values for the threshold:

- High error
- High warning
- Low warning
- Low error

Note: You do NOT need to define all 4 values! Usually you will only enter a value for one or two of these fields. For example, if you want to send a warning when the disk space goes below 2GB, and an error when the disk space goes below 1GB, then you will only need the "low warning" and "low error" fields.



Group Threshold: Retail Clients with Windows

Thresholds [RMA Agent][Retail System Monitors]... [CPU Utilization]

Name: Example of numeric threshold

Description: Example of numeric threshold

☑ Enabled to generate events

☐ Generate events on value change

Maximum queued events: 0

Minimum Duration: 5 minute(s)

Resend Delay: 0 hour(s)

Above Or Equal

100

90

Below Or Equal

10

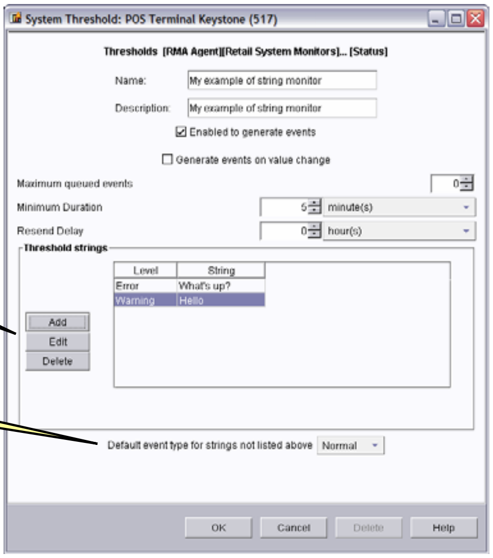
0

If value >= 100, sends error event
If value >= 90 (and < 100), sends warning event

If value <= 0, sends error event
If value <= 10 (and > 0), sends warning event

If value > 10 and < 90, no event will be sent!

For string thresholds, you must define a list of strings to compare against. Each comparison can be assigned a level of "Error", "Warning", or "Normal". ("Error" and "Warning" matches will generate events. "Normal" will not.)



Add, edit, or delete string values to compare against

Default level for all other string values

System Threshold: POS Terminal Keystone (517)

Thresholds [RMA Agent][Retail System Monitors]... [Status]

Name: My example of string monitor

Description: My example of string monitor

☑ Enabled to generate events

☐ Generate events on value change

Maximum queued events 0

Minimum Duration 5 minute(s)

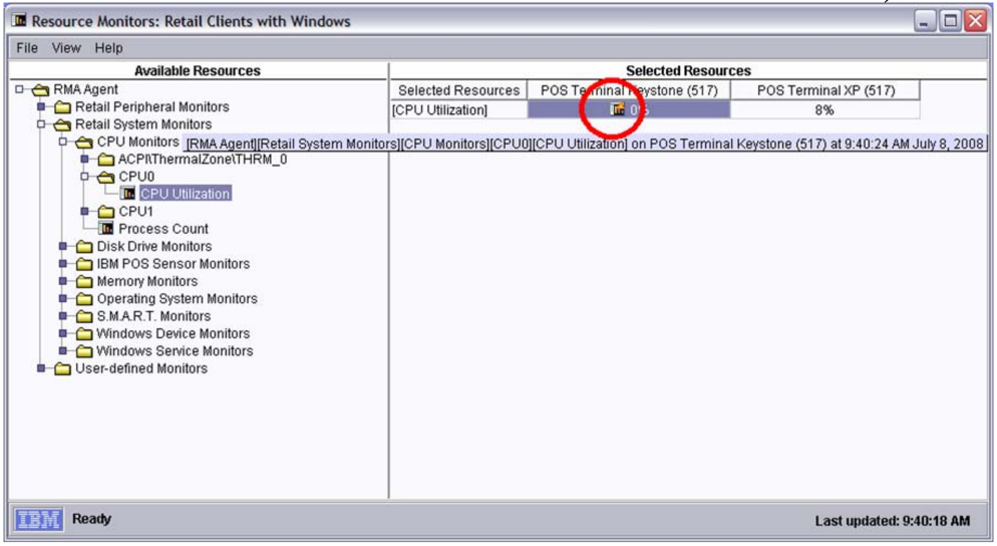
Resend Delay 0 hour(s)

Threshold strings

Level	String
Error	What's up?
Warning	Hello

Default event type for strings not listed above Normal

Once the threshold is defined, an icon will appear next to the selected value (i.e. underneath the column for the device that the individual threshold is defined for).



Resource Monitors: Retail Clients with Windows

Selected Resources	POS Terminal Keystone (517)	POS Terminal XP (517)
[CPU Utilization]	0%	8%

[RMA Agent][Retail System Monitors][CPU Monitors][CPU0][CPU Utilization] on POS Terminal Keystone (517) at 9:40:24 AM July 8, 2008

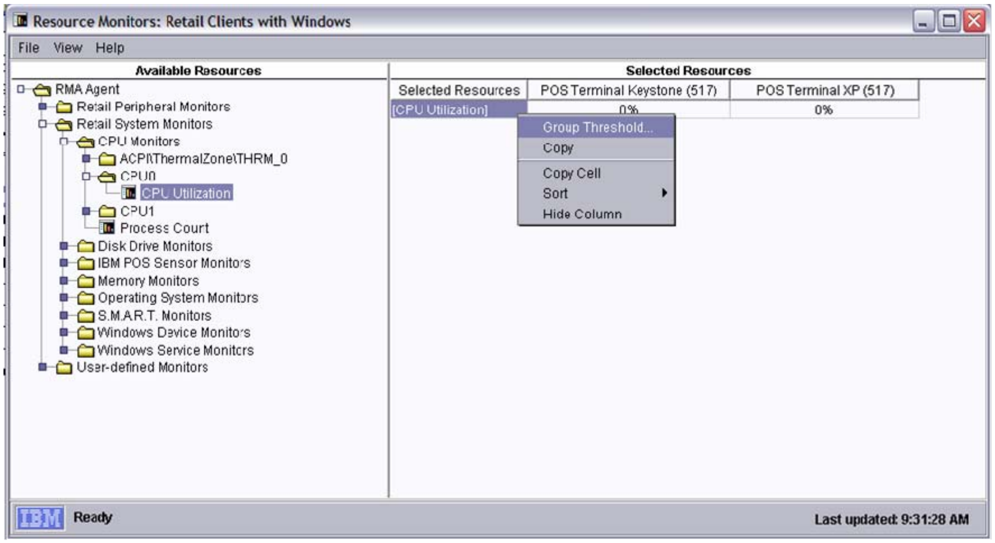
Ready

Last updated: 9:40:18 AM

Defining a "group threshold"

Within the resource monitors task, right-click any value and select "Group Threshold" to begin defining a threshold that will apply to all the members of that group.

> **Note**: To define a group threshold, you must have launched the Resource Monitors task against a group (not against a selection of one or more individual managed objects).

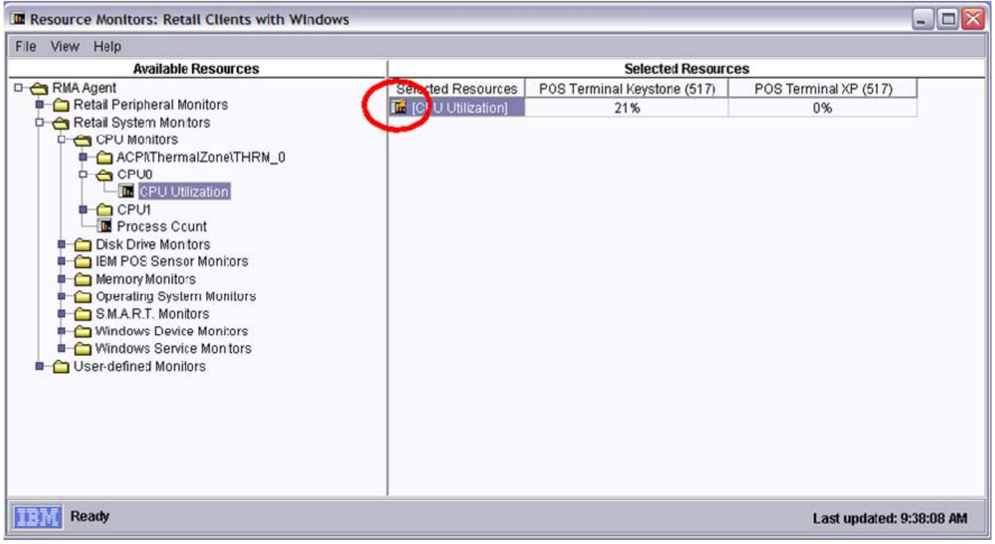


Selected Resources	POS Terminal Keystone (517)	POS Terminal XP (517)
[CPU Utilization]	0%	0%

Ready

Last updated: 9:31:28 AM

Once the threshold is defined, an icon will appear next to the selected group of values:



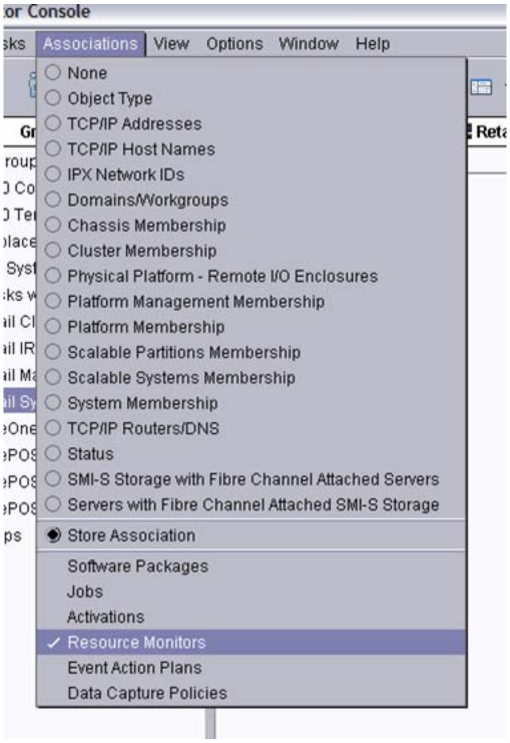
Selected Resources	POS Terminal Keystone (517)	POS Terminal XP (517)
[CPU Utilization]	21%	0%

Ready

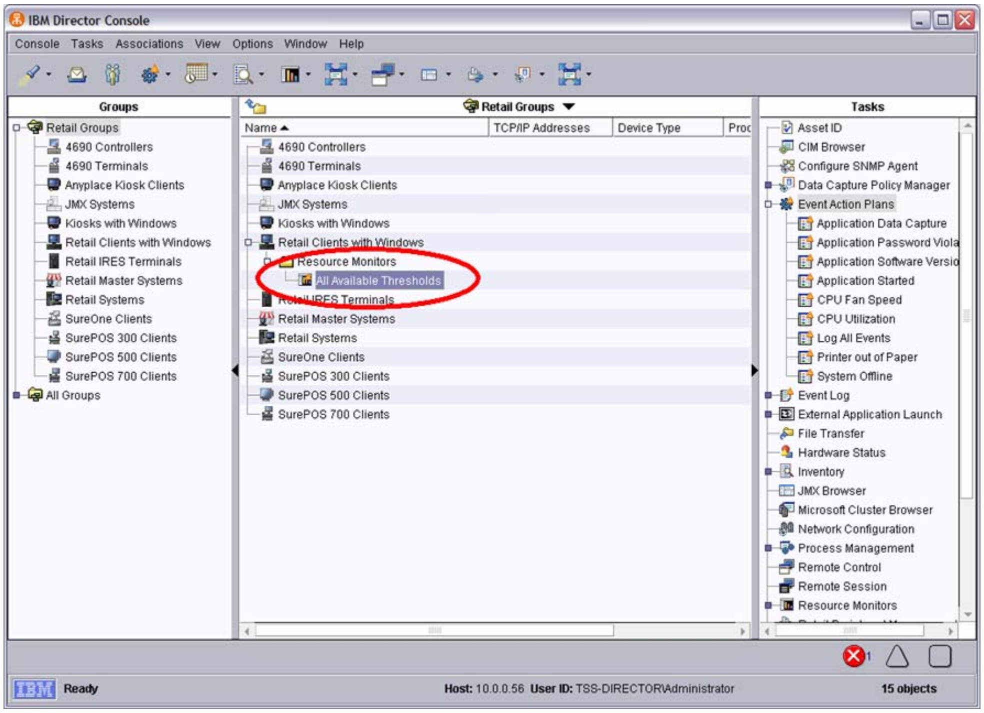
Last updated: 9:38:08 AM

Editing and viewing thresholds

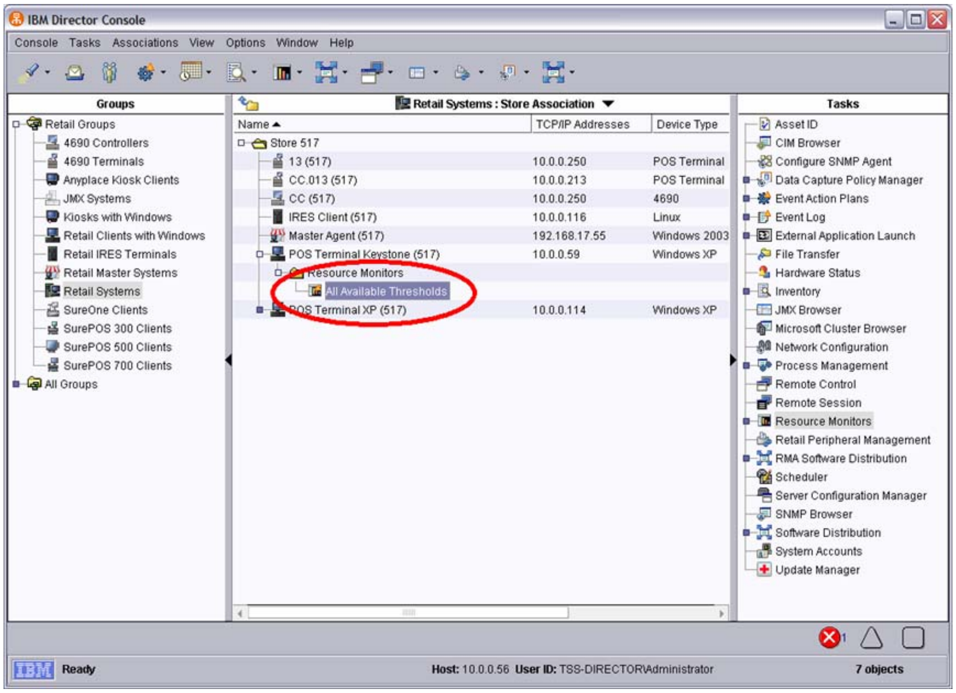
After you've defined a threshold, there are several ways to view it and/or edit it. First, use the "Associations" menu and make sure that "Resource Monitors" is checked.



If you've defined a group threshold, click on "All Groups" in the groups pane. You can now expand the tree in the middle of the screen to see "All Available Thresholds" under your group. Double-click to view and/or edit your threshold.

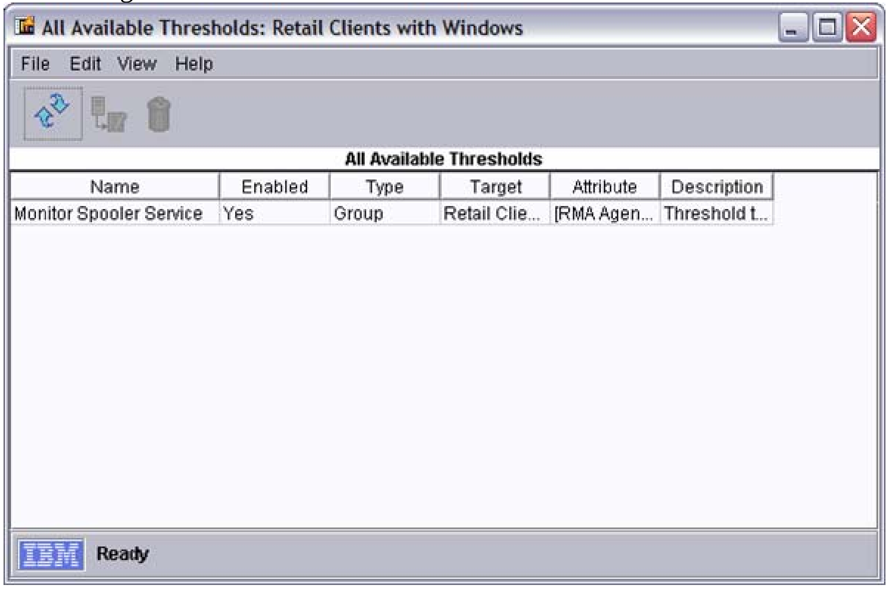


If you’ve created an individual threshold, select the group to which your system belongs, and you’ll see “All Available Thresholds” listed under the individual system for which you created the threshold. Double-click to view/edit your threshold.



Name ▲	TCP/IP Addresses	Device Type
Store 517		
13 (517)	10.0.0.250	POS Terminal
CC.013 (517)	10.0.0.213	POS Terminal
CC (517)	10.0.0.250	4690
IRES Client (517)	10.0.0.116	Linux
Master Agent (517)	192.168.17.55	Windows 2003
POS Terminal Keystone (517)	10.0.0.59	Windows XP
Resource Monitors		
All Available Thresholds		
POS Terminal XP (517)	10.0.0.114	Windows XP

When you click on “All Available Thresholds” (under a group or under an individual managed object), you will see a list of thresholds applied to that group or system. You can right-click a row to edit and/or view the threshold.



All Available Thresholds

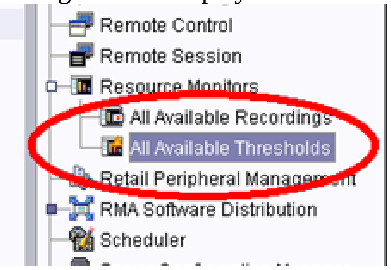
Name	Enabled	Type	Target	Attribute	Description
Monitor Spooler Service	Yes	Group	Retail Clie...	[RMA Agen...	Threshold t...

Organizing and applying thresholds

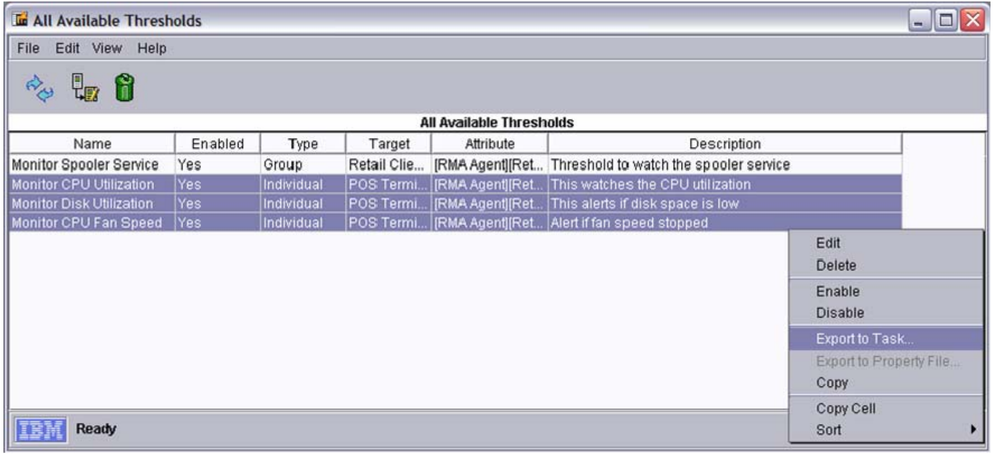
You can organize several thresholds into a single “Threshold Plan”. This makes it easier to track and apply the thresholds to the specific managed objects or groups that you need.

Once you’ve defined a threshold plan, you can drag that threshold plan to a group, a single object, or to a group of managed objects. This allows you to easily apply the same threshold to additional systems.

Double-click “All Available Thresholds” under “Resource Monitors” in the tasks pane on the right. This displays all thresholds that have been defined.



To create a threshold plan, select one or more thresholds, then right-click and select “Export to Task”.

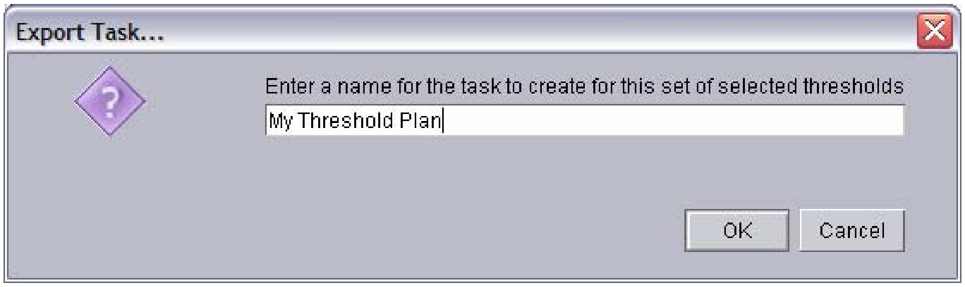


All Available Thresholds

Name	Enabled	Type	Target	Attribute	Description
Monitor Spooler Service	Yes	Group	Retail Clie...	[RMA Agent][Ret...	Threshold to watch the spooler service
Monitor CPU Utilization	Yes	Individual	POS Termi...	[RMA Agent][Ret...	This watches the CPU utilization
Monitor Disk Utilization	Yes	Individual	POS Termi...	[RMA Agent][Ret...	This alerts if disk space is low
Monitor CPU Fan Speed	Yes	Individual	POS Termi...	[RMA Agent][Ret...	Alert if fan speed stopped

Ready

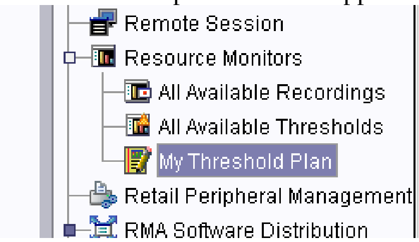
Give it a name and click OK.


Export Task...

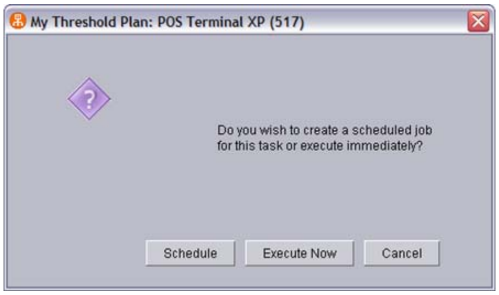
Enter a name for the task to create for this set of selected thresholds

My Threshold Plan

Your threshold plan will now appear under “Resource Monitors” in the tasks pane.

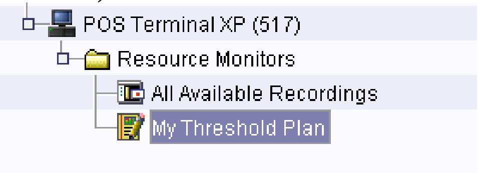


You can now drag-and-drop your threshold plan to a group, to an individual managed object, or to a selection of multiple managed objects. Click “Execute Now” to apply the threshold.


My Threshold Plan: POS Terminal XP (517)

Do you wish to create a scheduled job for this task or execute immediately?

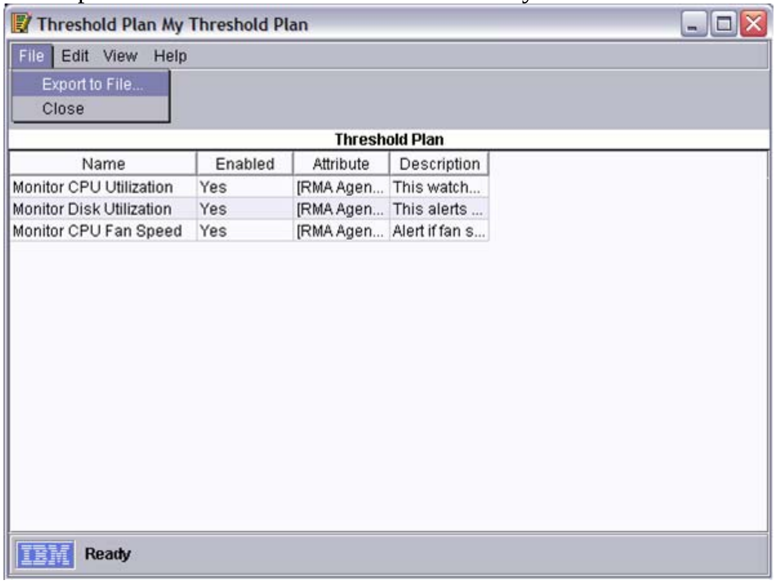
Once you’ve applied the plan to a group or an object, you’ll see the plan listed underneath that object. (Assuming the Associations menu has “Resource Monitors” checked.)



Importing/exporting threshold plans

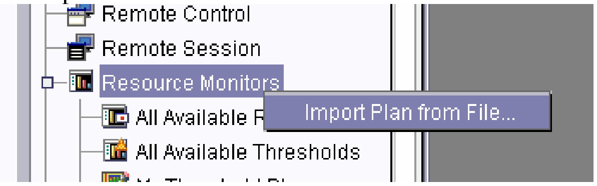
Threshold plans can be imported and exported. This allows you to backup/save your threshold plans, or move them from one Director Server to another easily. (For example, you may want to set up a lab test server, define your thresholds, then import them to your production server after you've verified them.)

To open your threshold plan, double-click the threshold plan under "Resource Monitors" in the tasks pane. Use the menu option "File / Export to File". This will create a ".thrshplan" file with the name and location of your choice.



Name	Enabled	Attribute	Description
Monitor CPU Utilization	Yes	[RMA Agen...	This watch...
Monitor Disk Utilization	Yes	[RMA Agen...	This alerts ...
Monitor CPU Fan Speed	Yes	[RMA Agen...	Alert if fan s...

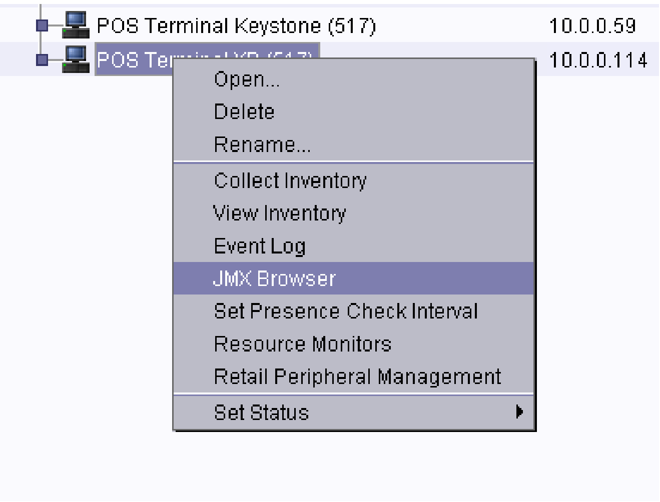
To import your threshold plan (".thrshplan" file), right-click "Resource Monitors" in the tasks pane.



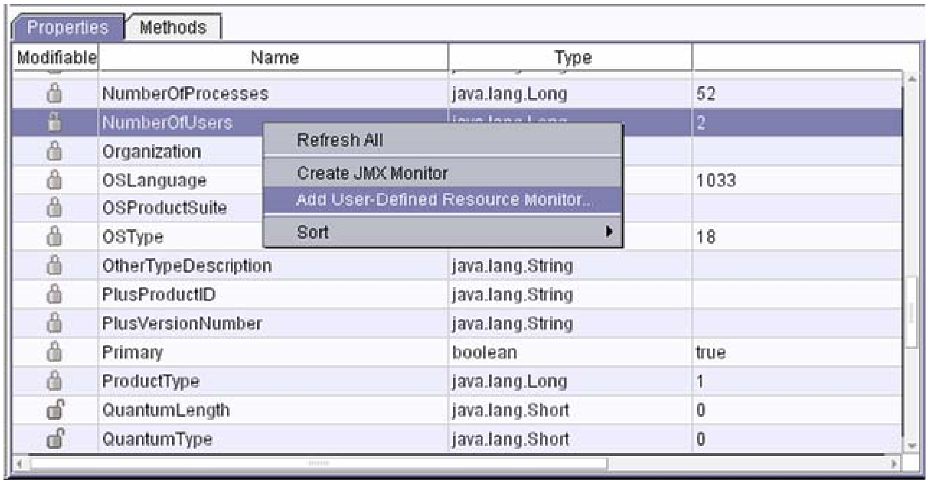
Custom resource monitors

If you can't find the value that you're looking for in the "Resource Monitors" task, you can create a custom (user-defined) monitor based on any value available in the JMX browser.

To create a custom-monitor, first open the JMX Browser for a system.

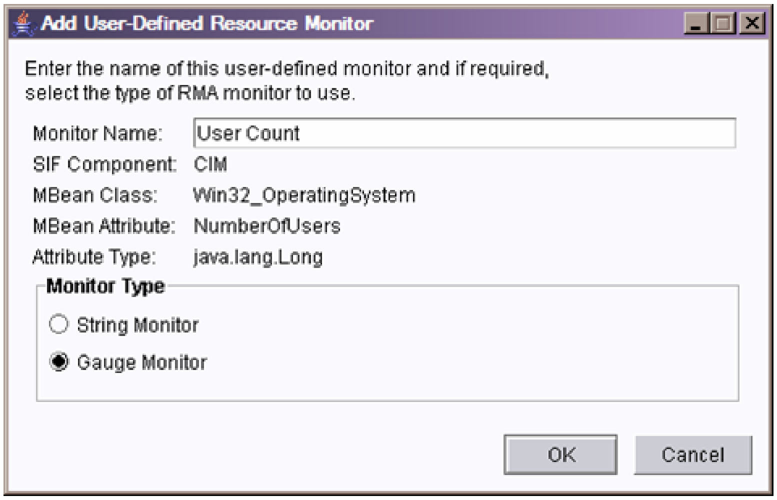


Within the JMX Browser, locate the value you want to monitor, then right-click and select “Add User-Defined Resource Monitor”.



Modifiable	Name	Type	
🔒	NumberOfProcesses	java.lang.Long	52
🔒	NumberOfUsers	java.lang.Long	2
🔒	Organization		
🔒	OSLanguage		1033
🔒	OSProductSuite		
🔒	OSType		18
🔒	OtherTypeDescription	java.lang.String	
🔒	PlusProductID	java.lang.String	
🔒	PlusVersionNumber	java.lang.String	
🔒	Primary	boolean	true
🔒	ProductType	java.lang.Long	1
🔓	QuantumLength	java.lang.Short	0
🔓	QuantumType	java.lang.Short	0

Give it a name and click OK.



Enter the name of this user-defined monitor and if required, select the type of RMA monitor to use.

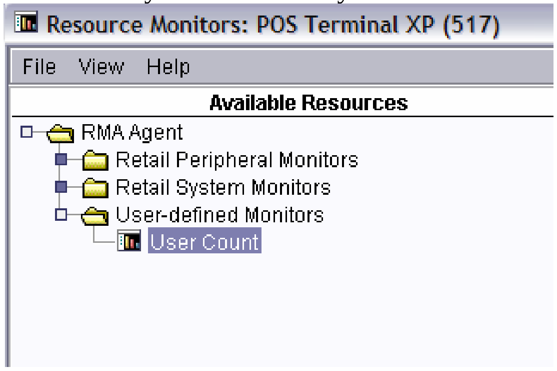
Monitor Name:	User Count
SIF Component:	CIM
MBean Class:	Win32_OperatingSystem
MBean Attribute:	NumberOfUsers
Attribute Type:	java.lang.Long

Monitor Type

○ String Monitor

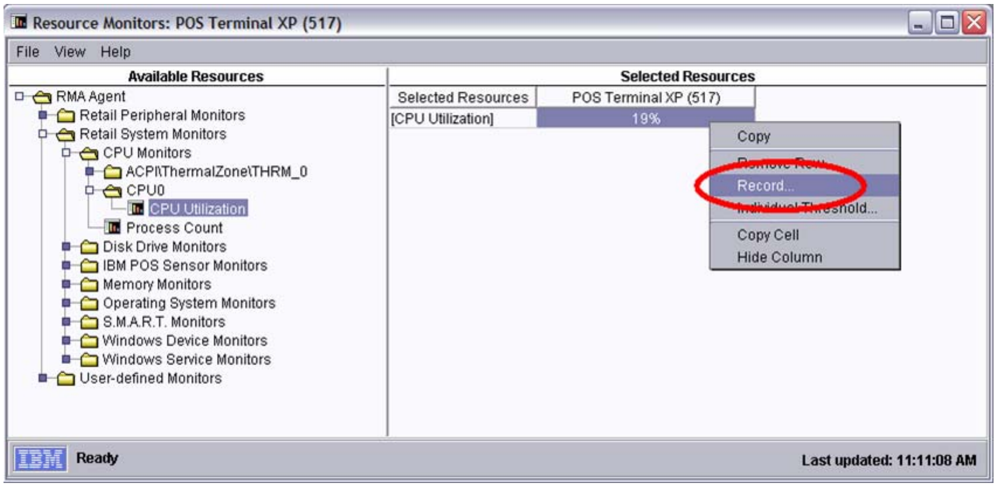
● Gauge Monitor

Your custom resource monitor will now appear in the "Resource Monitors" UI, and you can use it as you would use any other resource monitor.



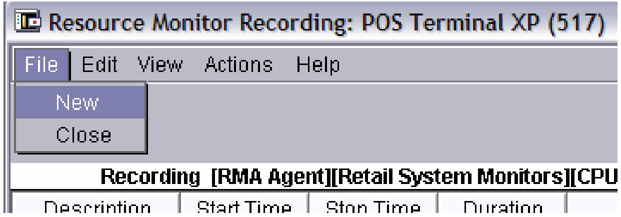
Recording resource monitors

You can record and graph any value from the resource monitors task. To initiate a recording, right-click a value and select "Record".

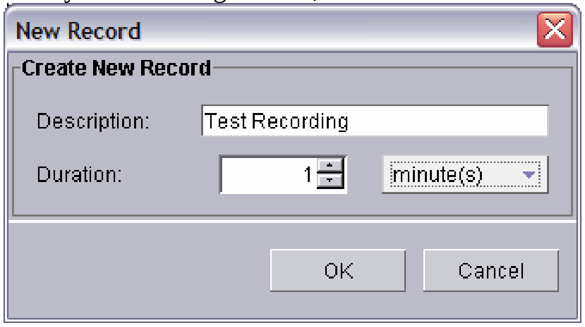


Selected Resources	POS Terminal XP (517)
[CPU Utilization]	19%

On the next screen, select "File / New" from the menu.


Resource Monitor Recording: POS Terminal XP (517)
File Edit View Actions Help
New
Close
Recording [RMA Agent][Retail System Monitors][CPU
Description
Start Time
Stop Time
Duration

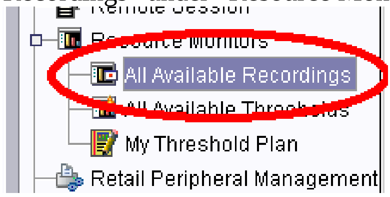
Give your recording a name; select the duration for the recording; then click OK.



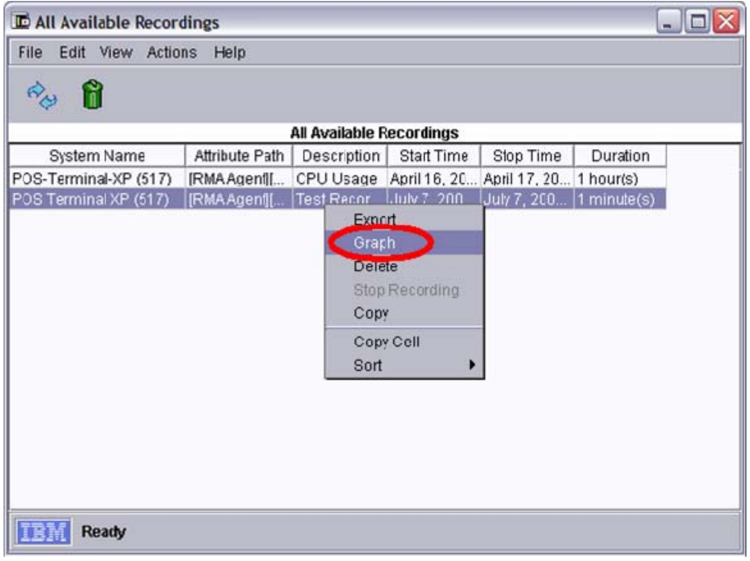
Description: Test Recording

Duration: 1 minute(s)

Later (after the recording duration has elapsed), you can click on "All Available Recordings" under "Resource Monitors" in the tasks pane.



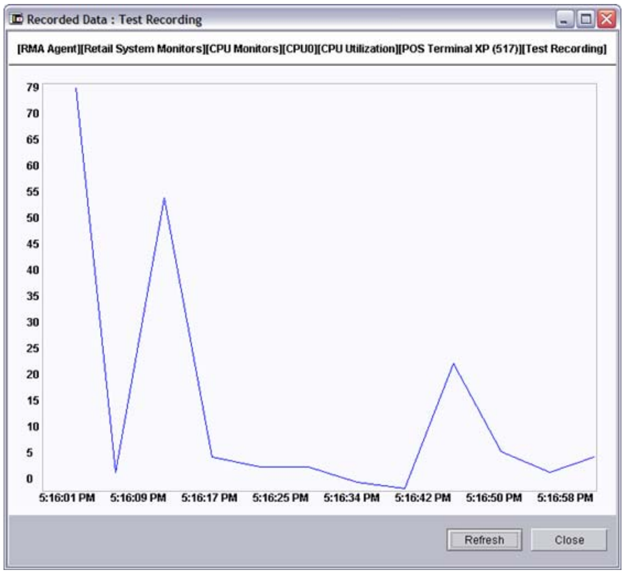
This will bring up the list of recordings. Right-click on your recording, and select "Graph" to show the graph of the recording.



All Available Recordings

System Name	Attribute Path	Description	Start Time	Stop Time	Duration
POS-Terminal-XP (517)	[RMA Agent][...	CPU Usage	April 16, 20...	April 17, 20...	1 hour(s)
POS Terminal XP (517)	[RMA Agent][...	Test Recor	July 7, 200	July 7, 200...	1 minute(s)

Ready



Recorded Data : Test Recording

[RMA Agent][Retail System Monitors][CPU Monitors][CPU0][CPU Utilization][POS Terminal XP (517)][Test Recording]

POS sensor drivers

Before you can use the "IBM POS Sensor Monitors" you must install the IBM POS sensor drivers on the remote system. These can be downloaded from the following URL, along with a list of supported hardware types:
http://www-01.ibm.com/support/docview.wss?rs=219&uid=pos1R4000167

Once you have installed the POS sensor drivers on the remote system, you will be able to begin creating thresholds using the "IBM POS Sensor Monitors" under the resource monitors task.

You may find it helpful to download pre-configured threshold plans from IBM that are tailored for the specific hardware models in your stores. These pre-configured, importable threshold plans can save you considerable time and effort in defining the resource monitors for your hardware. They can be downloaded from the following URL: http://www-01.ibm.com/support/docview.wss?rs=219&uid=pos1R1004330

Note: It is also possible to distribute the POS sensor drivers remotely using RMA software distribution – see "**Chapter 8 – Software Distribution**" for more details on easy deployment of the sensor drivers.

Example: Monitoring a Windows Service

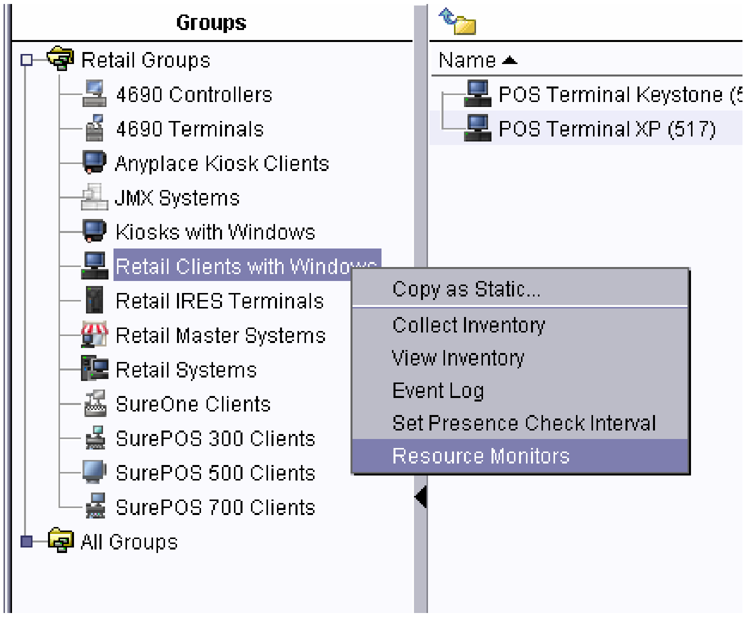
In this example, we'll monitor all Windows POS terminals to make sure the "spooler" service is running. If the service stops and remains stopped for at least 5 seconds, an alert will be generated. We'll define an event action plan to flag the system's status as "System Warning", which will cause the system status icon to appear in the main Director view.

This example demonstrates:

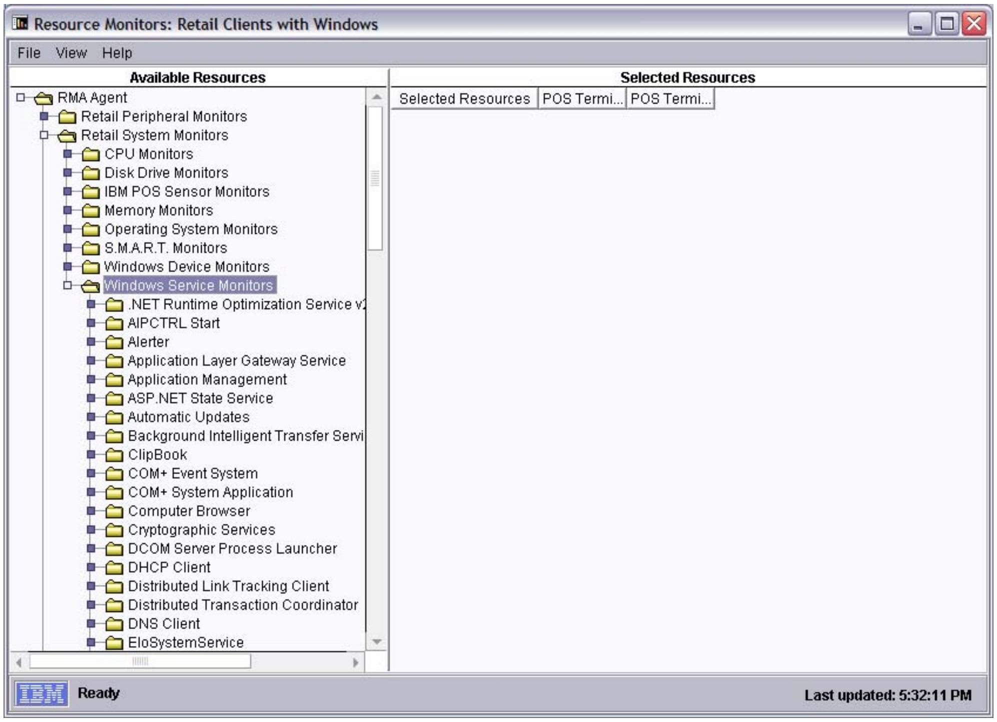
- Resource monitors task
- Group thresholds
- Event filters
- Event action plans

Steps:

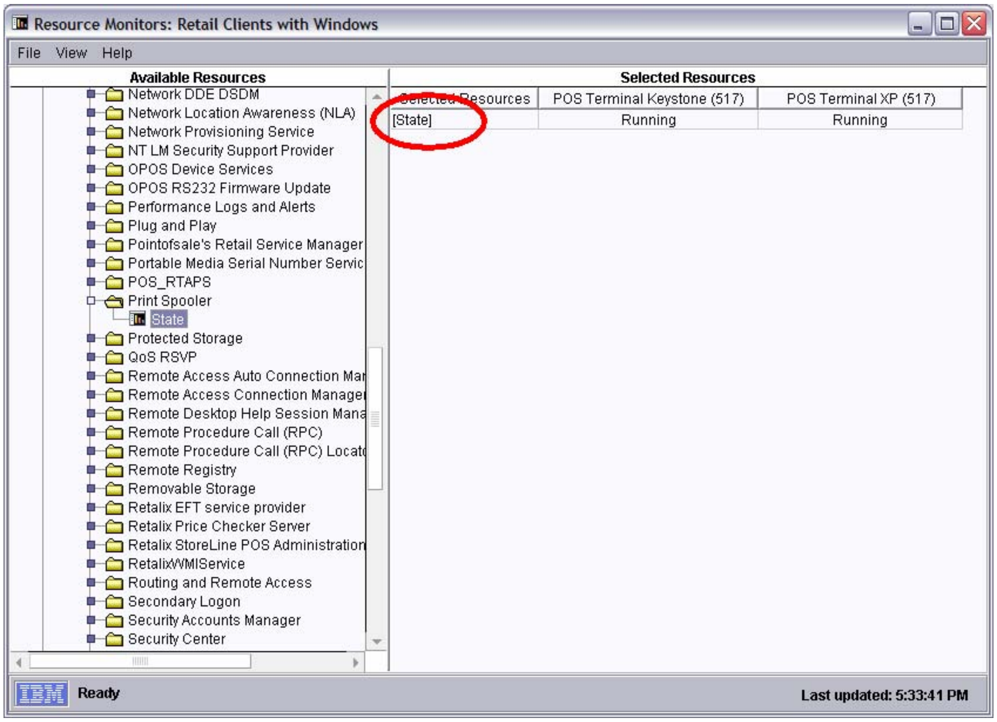
1. Right-click the group "Retail Clients with Windows" and then select "Resource Monitors". (**Note**: There are several other ways to invoke the resource monitors task, such as by dragging the "Resource Monitors" task to the group or to a selection of individual systems.)



2. When the “Resource Monitors” screen appears, expand the tree on the left to locate the “Windows Service Monitors”.

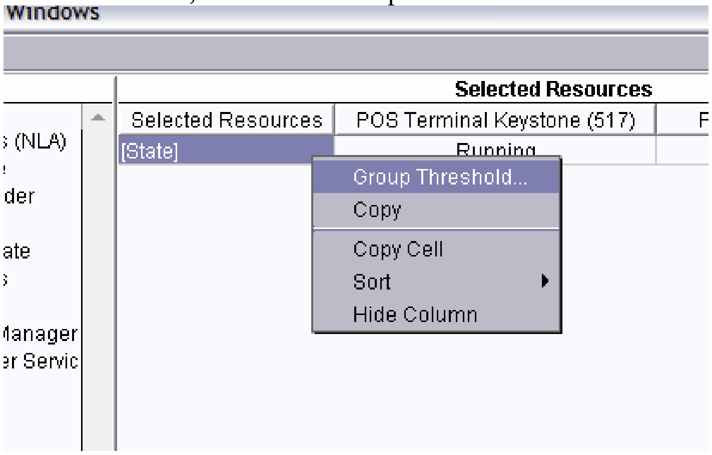


3. Double-click the “State” attribute within the “Print Spooler” monitor.


Resource Monitors: Retail Clients with Windows
File View Help
Available Resources
Network DDE DSDM
Network Location Awareness (NLA)
Network Provisioning Service
NT LM Security Support Provider
OPOS Device Services
OPOS RS232 Firmware Update
Performance Logs and Alerts
Plug and Play
Pointofsale's Retail Service Manager
Portable Media Serial Number Servic
POS_RTAPS
Print Spooler
State
Protected Storage
QoS RSVP
Remote Access Auto Connection Mar
Remote Access Connection Manager
Remote Desktop Help Session Mana
Remote Procedure Call (RPC)
Remote Procedure Call (RPC) Locat
Remote Registry
Removable Storage
Retalix EFT service provider
Retalix Price Checker Server
Retalix StoreLine POS Administration
RetalixWMIService
Routing and Remote Access
Secondary Logon
Security Accounts Manager
Security Center
Selected Resources
IBM
Ready
Last updated: 5:33:41 PM

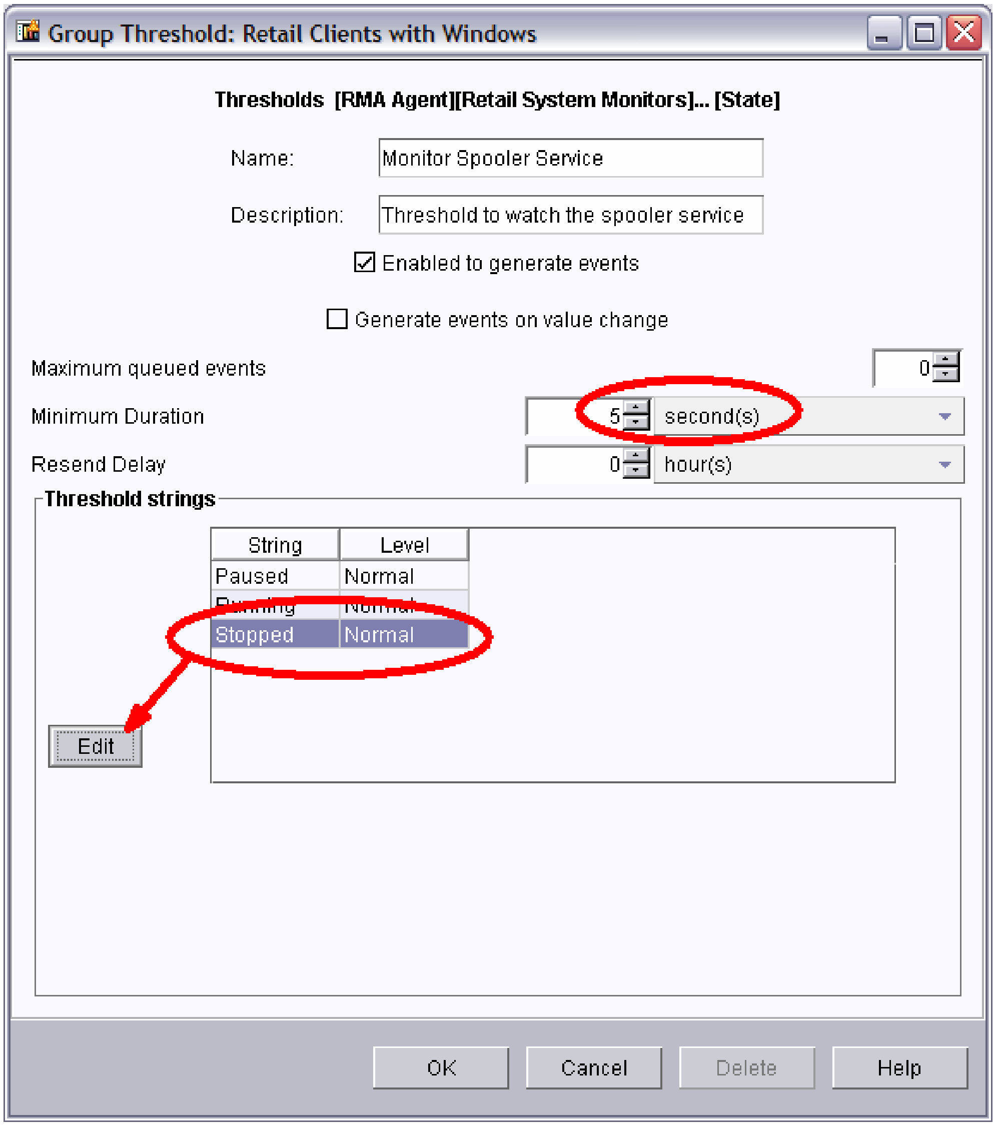
Selected Resources	POS Terminal Keystone (517)	POS Terminal XP (517)
[State]	Running	Running

4. Wait a few moments, and you will see the current state of “Running” for each of the systems in your group. Right-click the “[State]” entry under the “Selected Resources” view, and select “Group Threshold”.



Selected Resources	POS Terminal Keystone (517)	F
[State]	Running	

5. Enter a name and a description for your threshold. Change the number of seconds to “5”, then highlight the “Stopped” entry in the list of threshold strings. Click “Edit” to adjust the level for the “Stopped” string.



Group Threshold: Retail Clients with Windows

Thresholds [RMA Agent][Retail System Monitors]... [State]

Name: Monitor Spooler Service

Description: Threshold to watch the spooler service

☑ Enabled to generate events

□ Generate events on value change

Maximum queued events 0

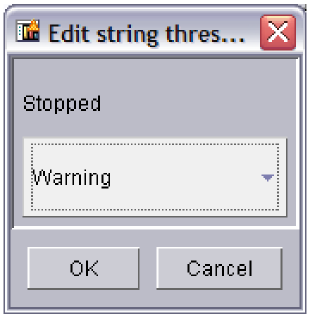
Minimum Duration 5 second(s)

Resend Delay 0 hour(s)

Threshold strings

String	Level
Paused	Normal
Running	Normal
Stopped	Normal

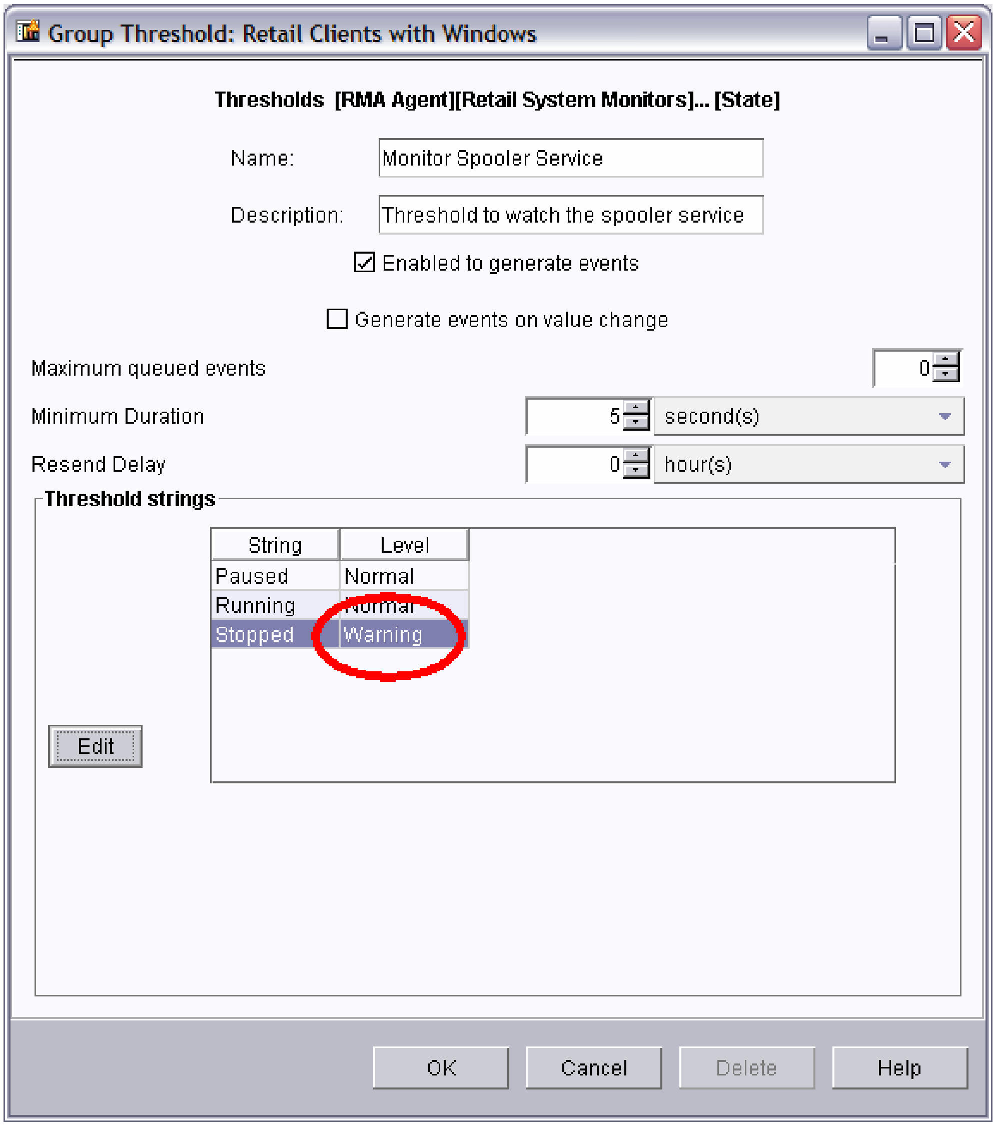
6. Select “Warning” and click OK.


Edit string thres...

Stopped

Warning

7. Your screen should now look like the following:



Group Threshold: Retail Clients with Windows

Thresholds [RMA Agent][Retail System Monitors]... [State]

Name: Monitor Spooler Service

Description: Threshold to watch the spooler service

☑ Enabled to generate events

□ Generate events on value change

Maximum queued events 0

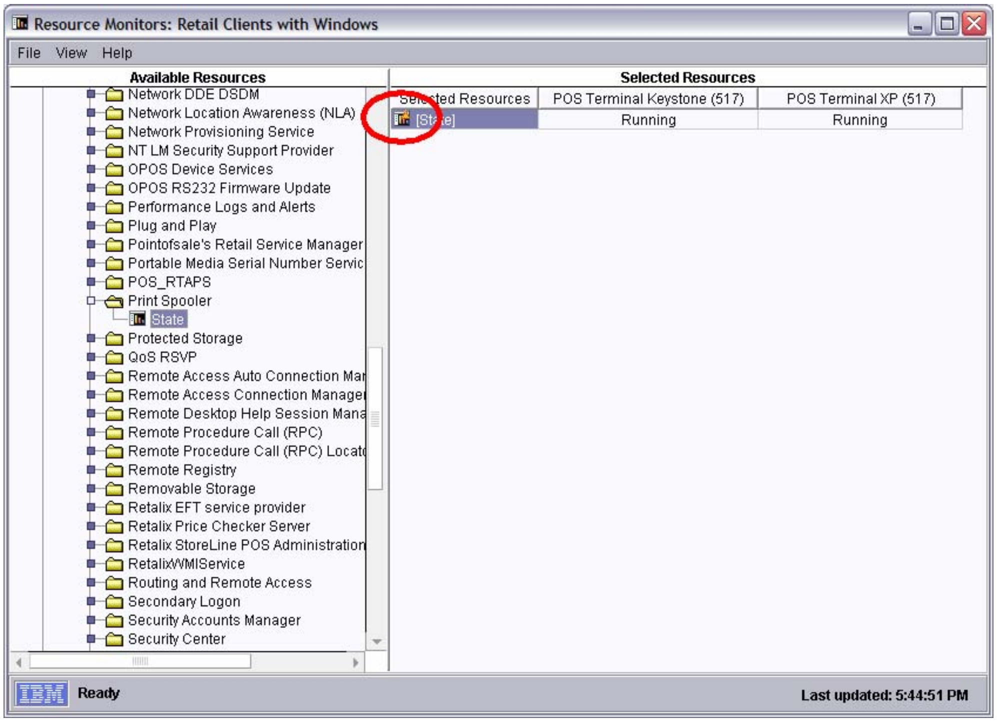
Minimum Duration 5 second(s)

Resend Delay 0 hour(s)

Threshold strings

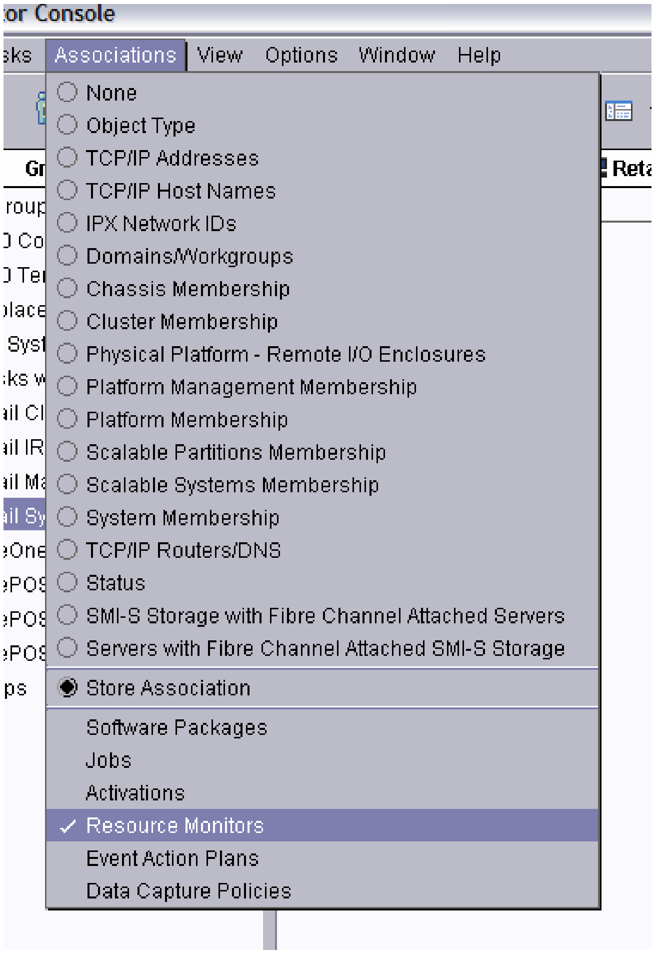
String	Level
Paused	Normal
Running	Normal
Stopped	Warning

8. Click OK to save your threshold. (**Note**: When you click OK your threshold will be automatically applied to the group.) You will now see an icon next to the resource monitors as shown below:

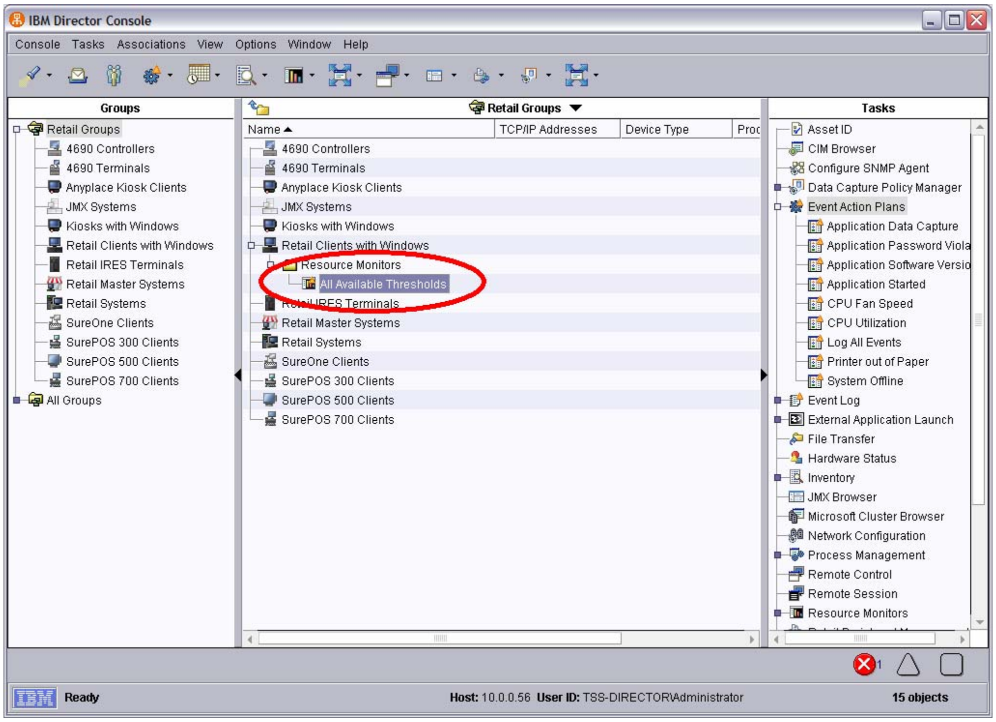

Resource Monitors: Retail Clients with Windows
File
View
Help
Available Resources
Selected Resources
Network DDE DSDM
Network Location Awareness (NLA)
Network Provisioning Service
NT LM Security Support Provider
OPOS Device Services
OPOS RS232 Firmware Update
Performance Logs and Alerts
Plug and Play
Pointofsale's Retail Service Manager
Portable Media Serial Number Servic
POS_RTAPS
Print Spooler
State
Protected Storage
QoS RSVP
Remote Access Auto Connection Mar
Remote Access Connection Manager
Remote Desktop Help Session Mana
Remote Procedure Call (RPC)
Remote Procedure Call (RPC) Locato
Remote Registry
Removable Storage
Retalix EFT service provider
Retalix Price Checker Server
Retalix StoreLine POS Administration
RetalixWMIService
Routing and Remote Access
Secondary Logon
Security Accounts Manager
Security Center
IBM
Ready
Last updated: 5:44:51 PM

Selected Resources	POS Terminal Keystone (517)	POS Terminal XP (517)
[State]	Running	Running

9. Close the resource monitors task. Under some circumstances you may wish to view your threshold later – after you've created it and closed the resource monitors task. To do this, you should first make sure that "Resource Monitors" is checked in the "Associations" menu.



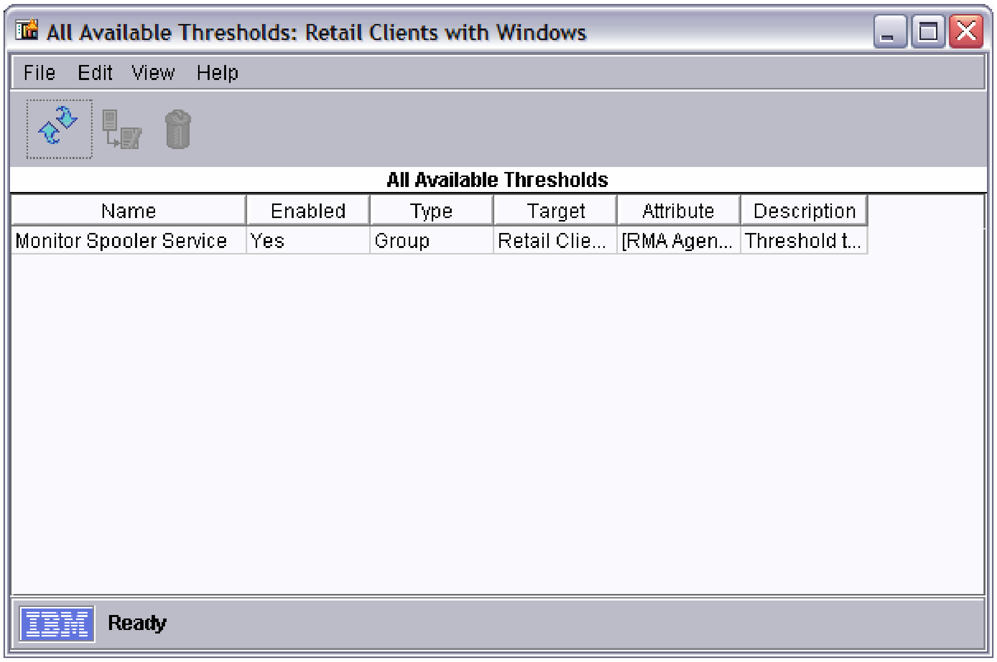
10. Click “Retail Groups” in the groups pane, and you will be able to expand the tree in the middle of the screen to show that “All Available Thresholds” is now listed under the group “Retail Clients with Windows”. You can double-click this to display all thresholds that have been applied to that group.



Host: 10.0.0.56 User ID: TSS-DIRECTOR\Administrator

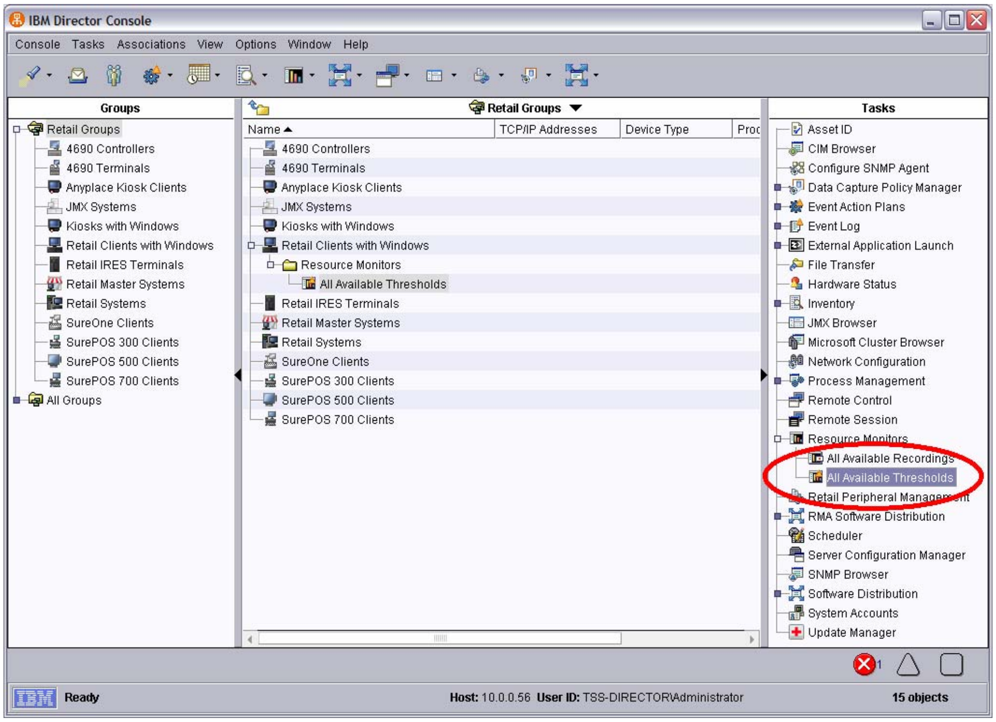
15 objects

11. The screen below shows the thresholds that have been applied to your group. (If for some reason you need to edit your threshold, you can do so by right-clicking the threshold from within this view and then choosing “Edit”.)

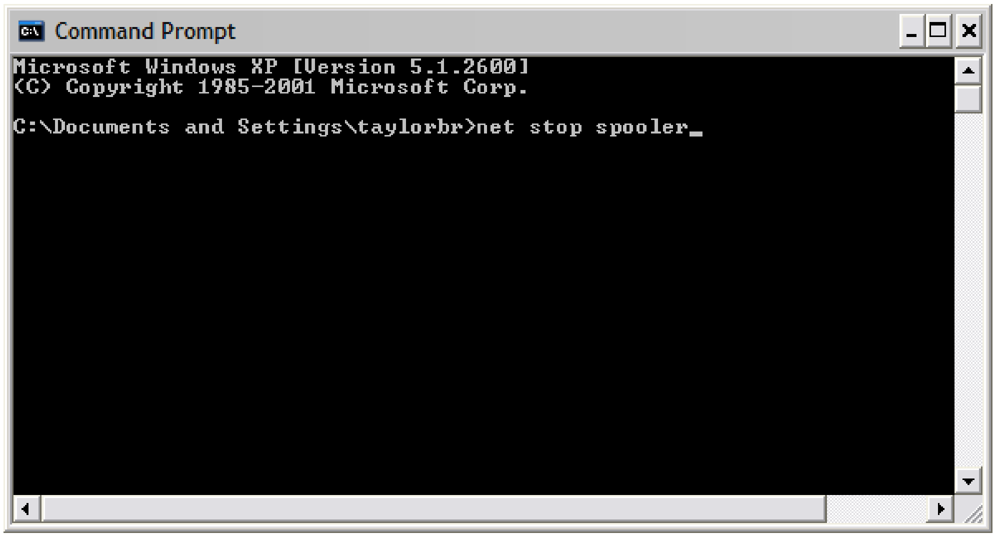


Name	Enabled	Type	Target	Attribute	Description
Monitor Spooler Service	Yes	Group	Retail Clie...	[RMA Agen...	Threshold t...

Note: If desired, you can also see all thresholds that have been defined for ALL systems by double-clicking on “All Available Thresholds” in the tasks pane on the right side of the screen.

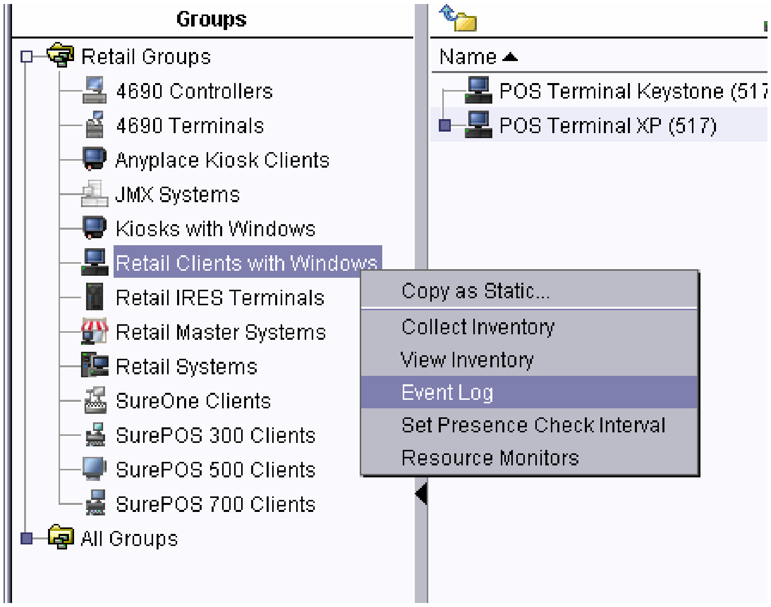


12. To test the threshold, log into your Windows system where the RMA general agent is running. Issue the command “net stop spooler” to stop the spooler service.

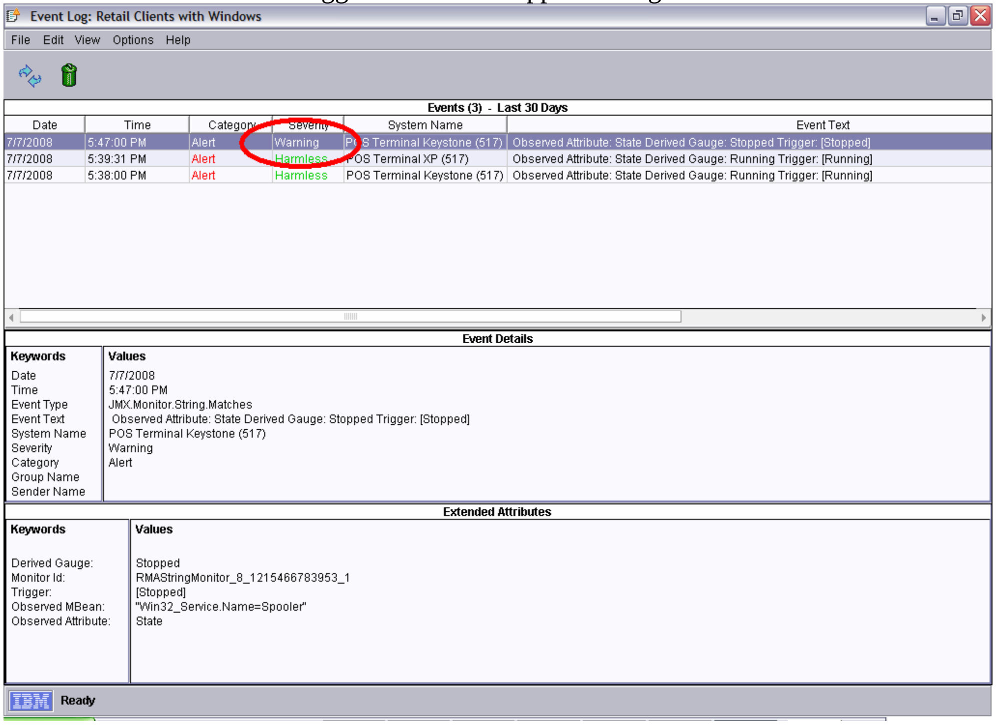


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\taylorbr>net stop spooler_
```

13. After about 5 seconds or so, right-click “Retail Clients with Windows” and select “Event Log” to bring up the event viewer for that group.



You should see the "Warning" event in the list, with the "Event Text" describing that the observed attribute triggered on the "Stopped" string.



Events (3) - Last 30 Days

Date	Time	Category	Severity	System Name	Event Text
7/7/2008	5:47:00 PM	Alert	Warning	POS Terminal Keystone (517)	Observed Attribute: State Derived Gauge: Stopped Trigger: [Stopped]
7/7/2008	5:39:31 PM	Alert	Harmless	POS Terminal XP (517)	Observed Attribute: State Derived Gauge: Running Trigger: [Running]
7/7/2008	5:38:00 PM	Alert	Harmless	POS Terminal Keystone (517)	Observed Attribute: State Derived Gauge: Running Trigger: [Running]

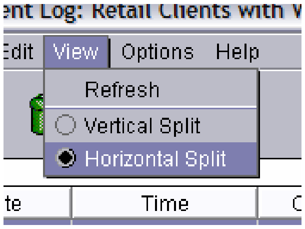
Event Details

Keywords	Values
Date	7/7/2008
Time	5:47:00 PM
Event Type	JMX.Monitor.String.Matches
Event Text	Observed Attribute: State Derived Gauge: Stopped Trigger: [Stopped]
System Name	POS Terminal Keystone (517)
Severity	Warning
Category	Alert
Group Name	
Sender Name	

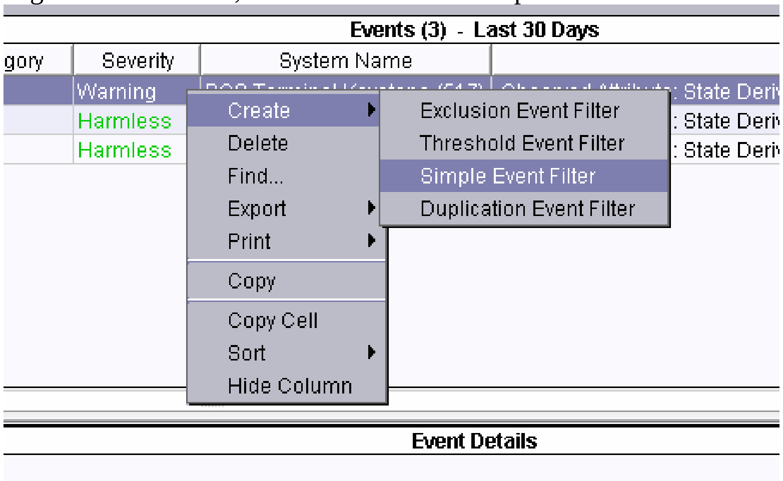
Extended Attributes

Keywords	Values
Derived Gauge:	Stopped
Monitor Id:	RMAStringMonitor_8_1215466783953_1
Trigger:	[Stopped]
Observed MBean:	"Win32_Service.Name=Spooler"
Observed Attribute:	State

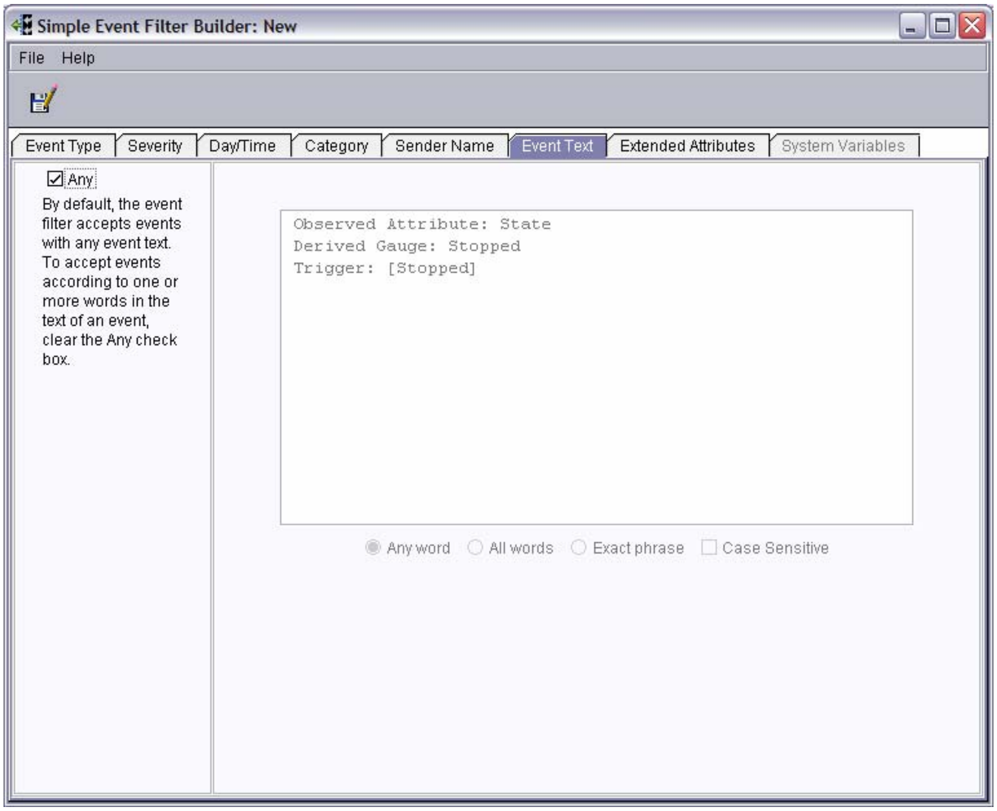
Note: To view events horizontally (as shown above), select "Horizontal Split" in the menu.



14. Right-click the event, and select "Create / Simple Event Filter".



15. In the "Event Text" tab, check "Any".



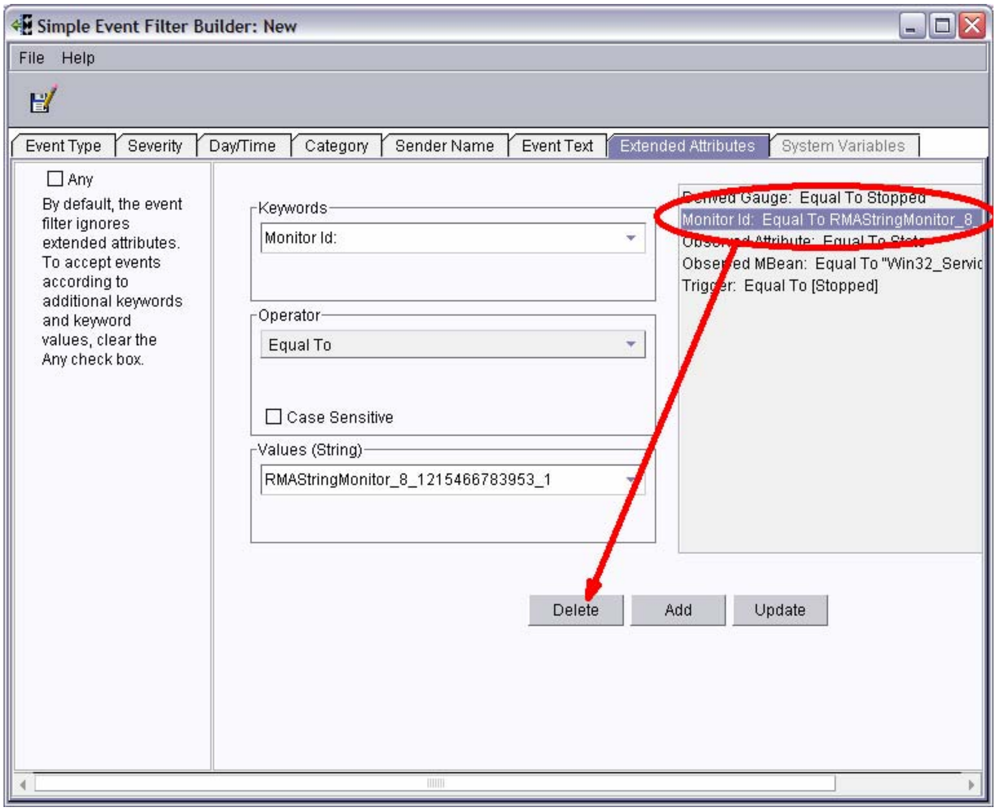
☑ Any

By default, the event filter accepts events with any event text. To accept events according to one or more words in the text of an event, clear the Any check box.

```
Observed Attribute: State
Derived Gauge: Stopped
Trigger: [Stopped]
```

● Any word ○ All words ○ Exact phrase □ Case Sensitive

16. In the “Extended Attributes” tab, select the “Monitor Id” entry, and click “Delete”. (This will ensure that the event filter continues to work even if you delete your threshold and create a new one that’s exactly the same.)



□ Any

By default, the event filter ignores extended attributes. To accept events according to additional keywords and keyword values, clear the Any check box.

Keywords: Monitor Id:

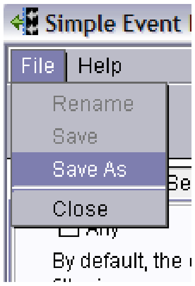
Operator: Equal To

□ Case Sensitive

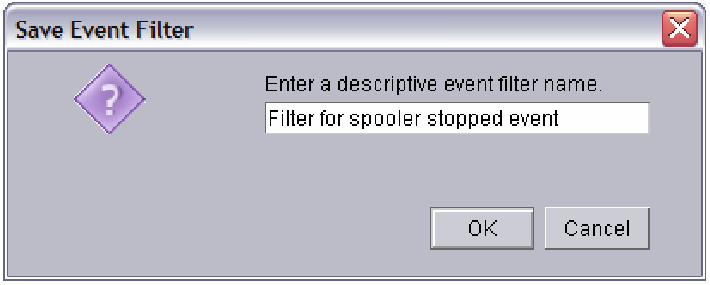
Values (String): RMAStringMonitor_8_1215466783953_1

Derived Gauge: Equal To Stopped
Monitor Id: Equal To RMAStringMonitor_8_
Observed Attribute: Equal To State
Observed MBean: Equal To "Win32_Servic
Trigger: Equal To [Stopped]

17. Click “File / Save As”.

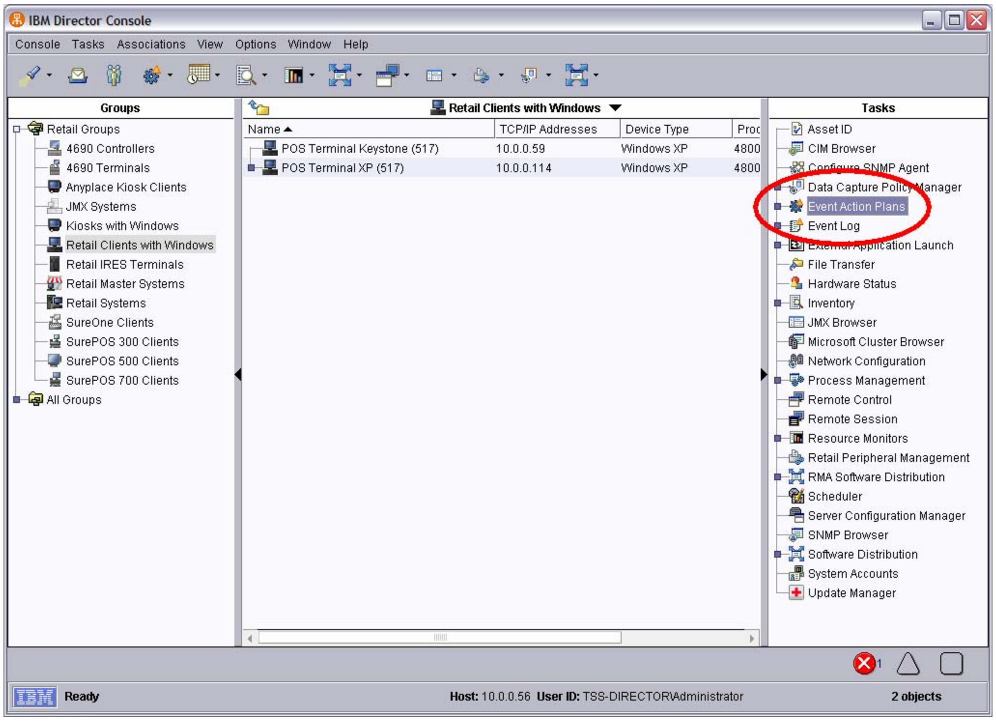


18. Give the event filter a name, and click OK.



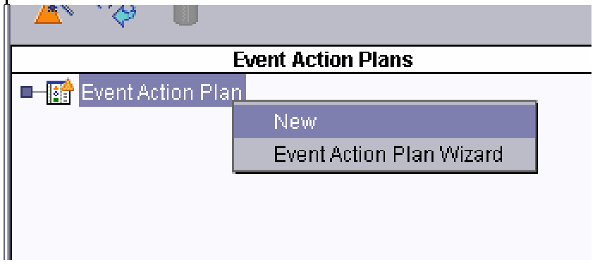
Enter a descriptive event filter name.
Filter for spooler stopped event

Close the event viewer.

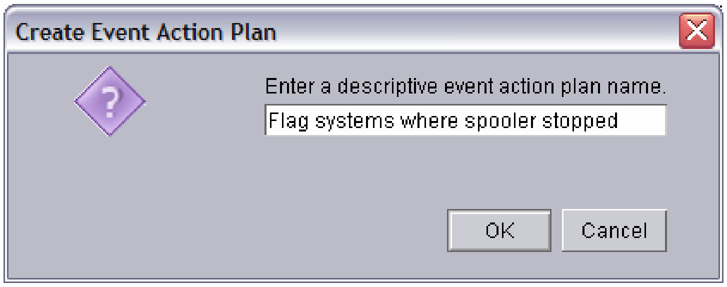


Name	TCP/IP Addresses	Device Type	Proc
POS Terminal Keystone (517)	10.0.0.59	Windows XP	4800
POS Terminal XP (517)	10.0.0.114	Windows XP	4800

19. Right-click “Event Action Plan” and select “New” to create a new event action plan.

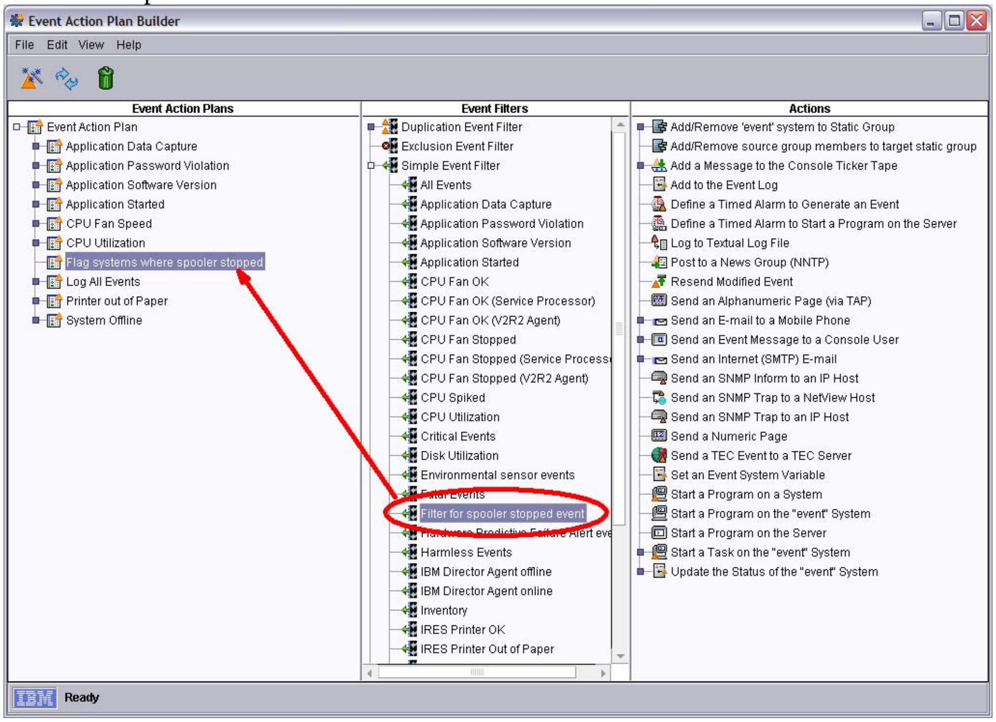


20. Give it a name and click OK.

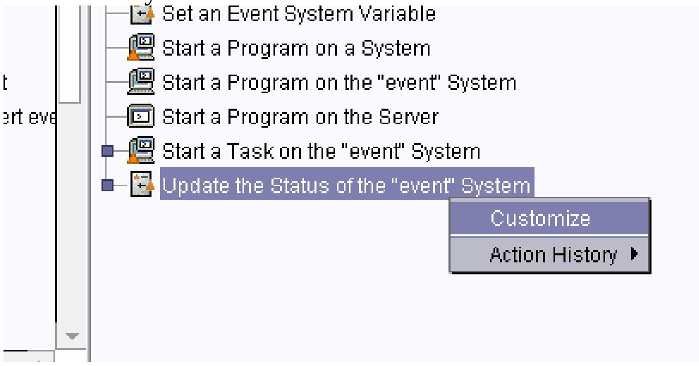


Enter a descriptive event action plan name.
Flag systems where spooler stopped

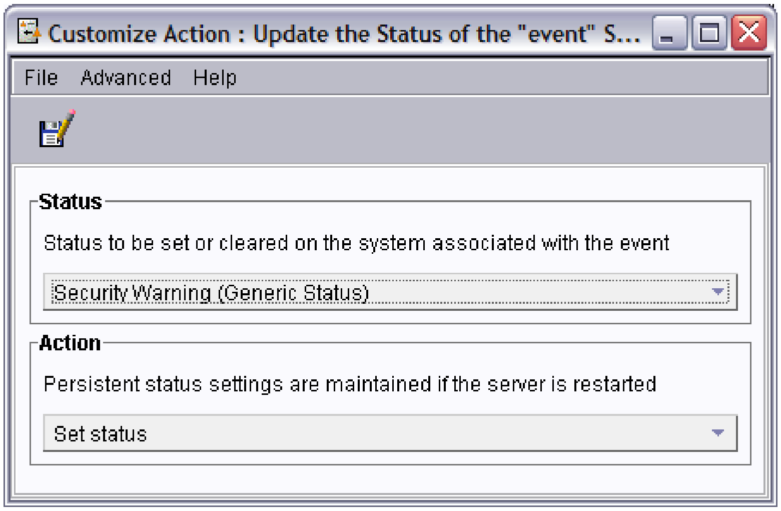
21. Find your simple event filter in the list of event filters, and then drag it to your event action plan on the left.


Event Action Plan Builder
File Edit View Help
Event Action Plans
Event Action Plan
Application Data Capture
Application Password Violation
Application Software Version
Application Started
CPU Fan Speed
CPU Utilization
Flag systems where spooler stopped
Log All Events
Printer out of Paper
System Offline
Event Filters
Duplication Event Filter
Exclusion Event Filter
Simple Event Filter
All Events
Application Data Capture
Application Password Violation
Application Software Version
Application Started
CPU Fan OK
CPU Fan OK (Service Processor)
CPU Fan OK (V2R2 Agent)
CPU Fan Stopped
CPU Fan Stopped (Service Process
CPU Fan Stopped (V2R2 Agent)
CPU Spiked
CPU Utilization
Critical Events
Disk Utilization
Environmental sensor events
Fatal Events
Filter for spooler stopped event
Hardware Predictive Failure Alert eve
Harmless Events
IBM Director Agent offline
IBM Director Agent online
Inventory
IRES Printer OK
IRES Printer Out of Paper
Actions
Add/Remove 'event' system to Static Group
Add/Remove source group members to target static group
Add a Message to the Console Ticker Tape
Add to the Event Log
Define a Timed Alarm to Generate an Event
Define a Timed Alarm to Start a Program on the Server
Log to Textual Log File
Post to a News Group (NNTP)
Resend Modified Event
Send an Alphanumeric Page (via TAP)
Send an E-mail to a Mobile Phone
Send an Event Message to a Console User
Send an Internet (SMTP) E-mail
Send an SNMP Inform to an IP Host
Send an SNMP Trap to a NetView Host
Send an SNMP Trap to an IP Host
Send a Numeric Page
Send a TEC Event to a TEC Server
Set an Event System Variable
Start a Program on a System
Start a Program on the "event" System
Start a Program on the Server
Start a Task on the "event" System
Update the Status of the "event" System
IBM
Ready

22. In the list of "Actions" on the right, right-click the action "Update the Status of the 'event' System". Select "Customize".


Set an Event System Variable
Start a Program on a System
Start a Program on the "event" System
Start a Program on the Server
Start a Task on the "event" System
Update the Status of the "event" System
Customize
Action History

23. Select "Security Warning" in the drop-down list. (And make sure the action is "Set status".)



Status

Status to be set or cleared on the system associated with the event

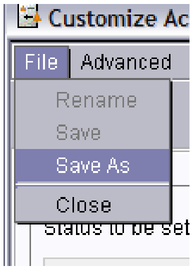
Security Warning (Generic Status)

Action

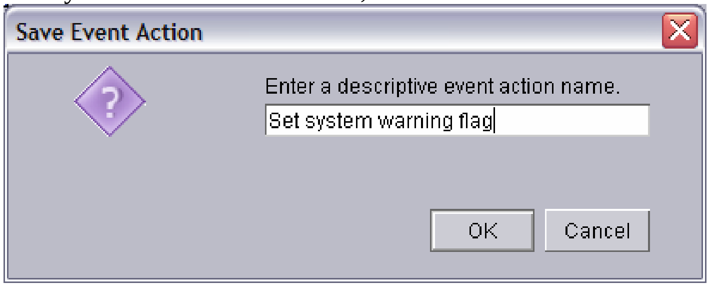
Persistent status settings are maintained if the server is restarted

Set status

24. Click “File / Save As” to save your custom action.



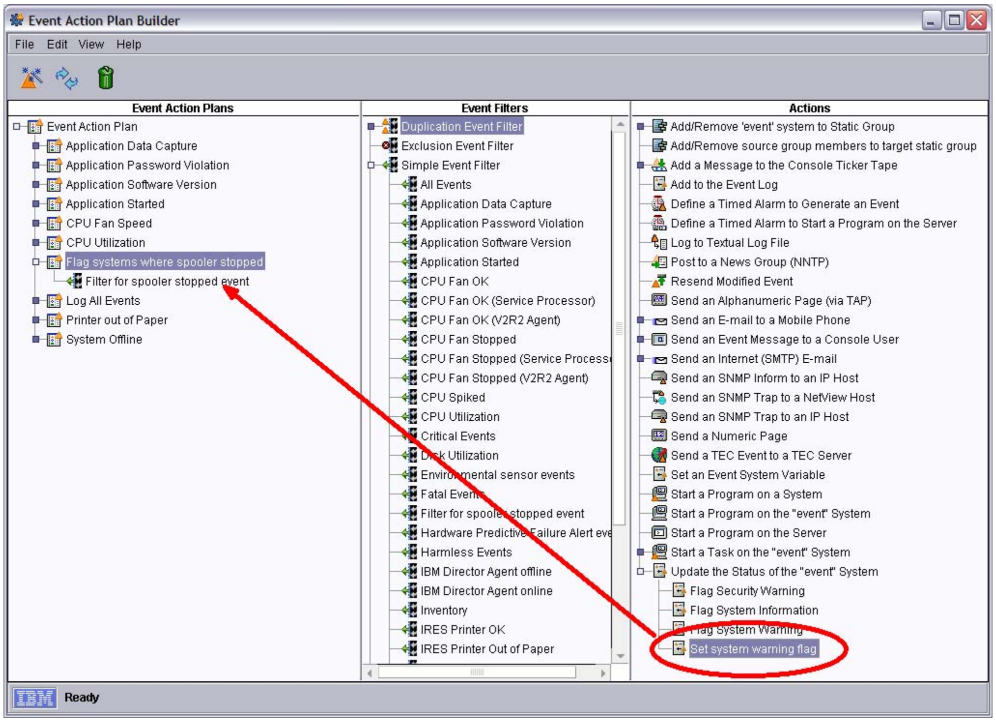
25. Give your custom action a name, and click OK.



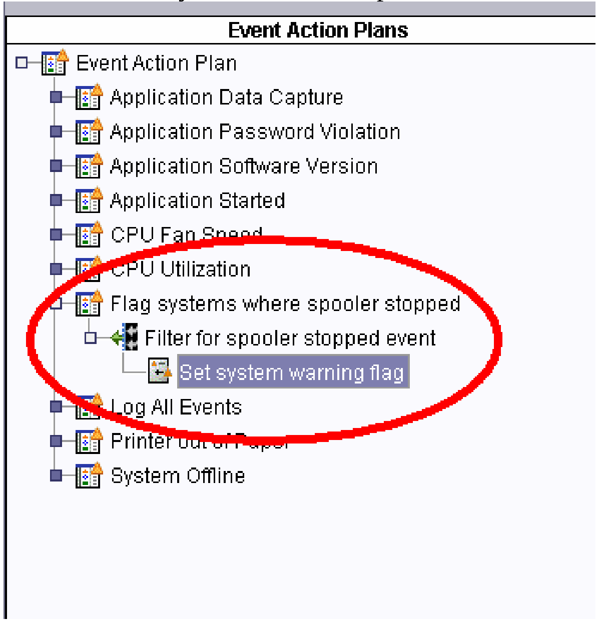
Enter a descriptive event action name.

Set system warning flag

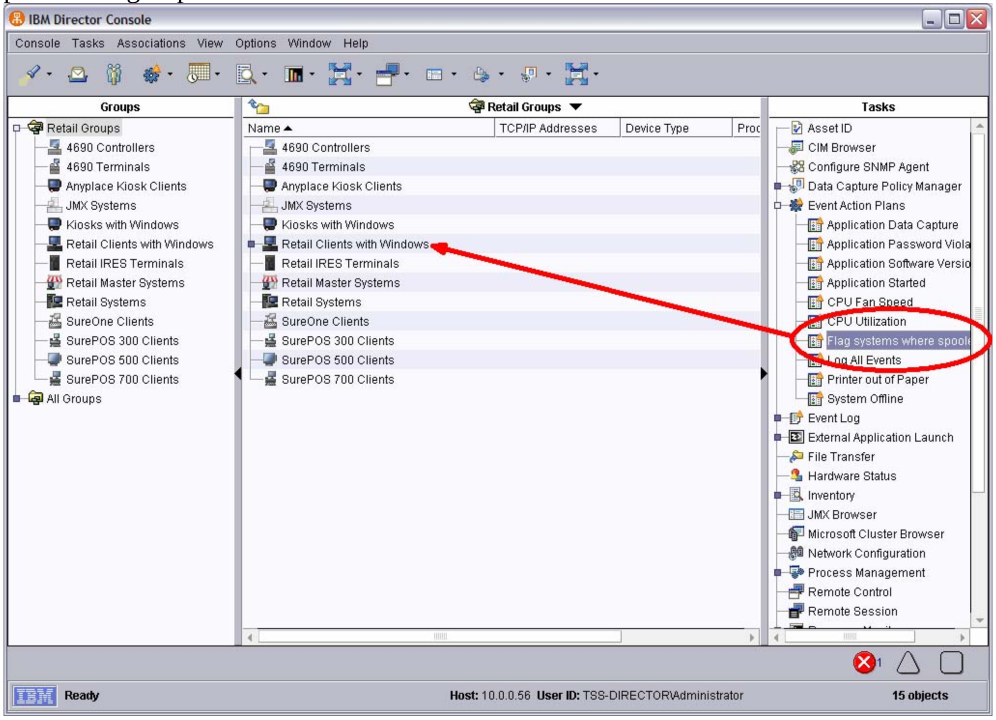
26. Drag your custom action underneath your filter in the event action plan.


Event Action Plan Builder
File Edit View Help
Event Action Plans
Event Action Plan
Application Data Capture
Application Password Violation
Application Software Version
Application Started
CPU Fan Speed
CPU Utilization
Flag systems where spooler stopped
Filter for spooler stopped event
Log All Events
Printer out of Paper
System Offline
Event Filters
Duplication Event Filter
Exclusion Event Filter
Simple Event Filter
All Events
Application Data Capture
Application Password Violation
Application Software Version
Application Started
CPU Fan OK
CPU Fan OK (Service Processor)
CPU Fan OK (V2R2 Agent)
CPU Fan Stopped
CPU Fan Stopped (Service Process
CPU Fan Stopped (V2R2 Agent)
CPU Spiked
CPU Utilization
Critical Events
Disk Utilization
Environmental sensor events
Fatal Events
Filter for spooler stopped event
Hardware Predictive Failure Alert eve
Harmless Events
IBM Director Agent offline
IBM Director Agent online
Inventory
IRES Printer OK
IRES Printer Out of Paper
Actions
Add/Remove 'event' system to Static Group
Add/Remove source group members to target static group
Add a Message to the Console Ticker Tape
Add to the Event Log
Define a Timed Alarm to Generate an Event
Define a Timed Alarm to Start a Program on the Server
Log to Textual Log File
Post to a News Group (NNTP)
Resend Modified Event
Send an Alphanumeric Page (via TAP)
Send an E-mail to a Mobile Phone
Send an Event Message to a Console User
Send an Internet (SMTP) E-mail
Send an SNMP Inform to an IP Host
Send an SNMP Trap to a NetView Host
Send an SNMP Trap to an IP Host
Send a Numeric Page
Send a TEC Event to a TEC Server
Set an Event System Variable
Start a Program on a System
Start a Program on the "event" System
Start a Program on the Server
Start a Task on the "event" System
Update the Status of the "event" System
Flag Security Warning
Flag System Information
Flag System Warning
Set system warning flag
IBM
Ready

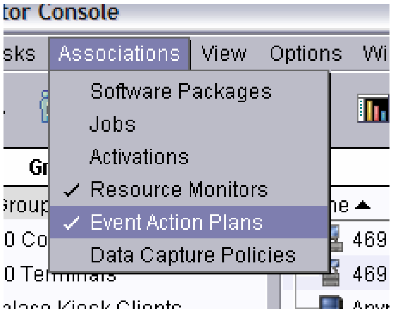
27. When finished, your event action plan should look similar to the following:



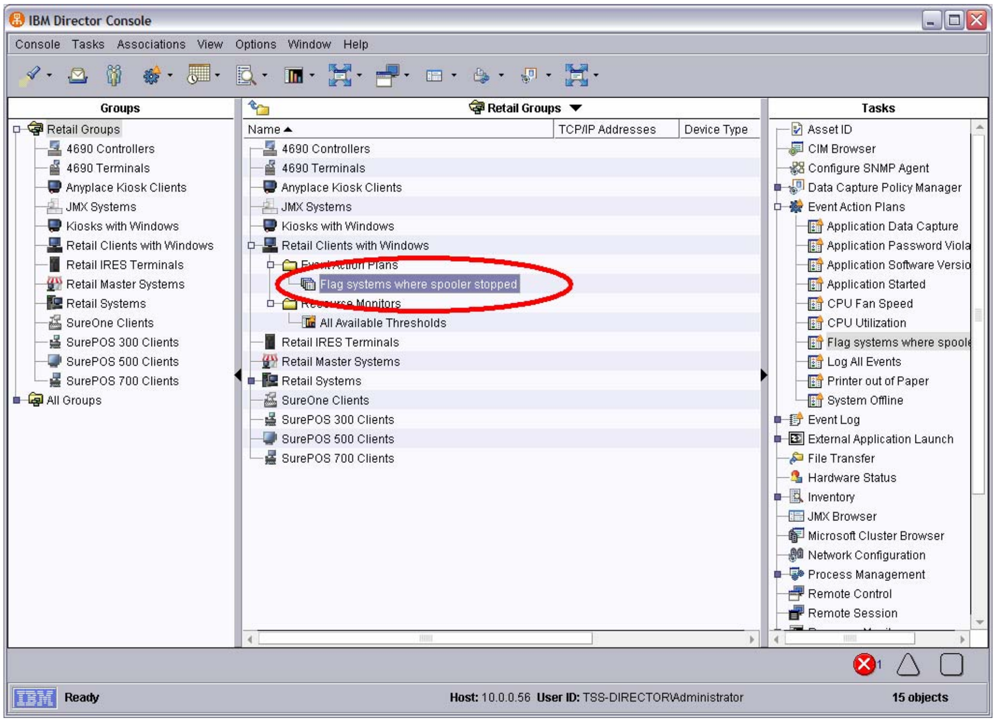
28. Close the event action plans task. In the main Director view, if you expand the "Event Action Plans" task, you should now see your new event action plan. In the groups pane, select "Retail Groups". You should now drag your event action plan to the group "Retail Clients with Windows".



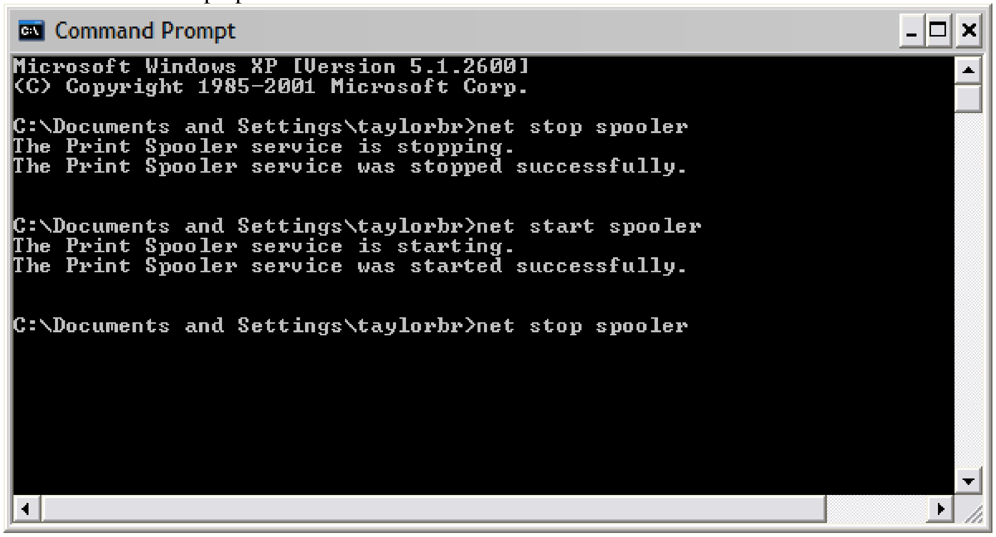
29. To make sure your event action plan is now associated to that group, first use the "Associations" menu to ensure that "Event Action Plans" is checked.



30. If you expand the tree, you will now see your event action plan displayed underneath the group.

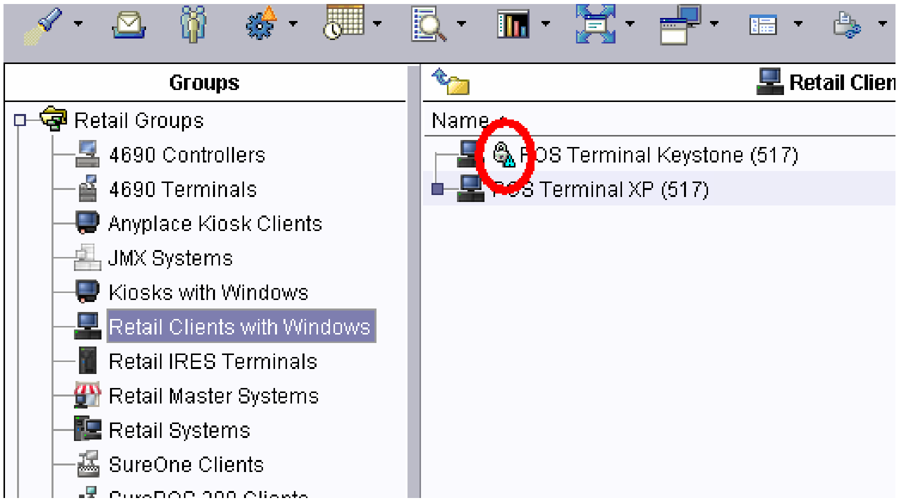


31. To test your finished event action plan, issue the command “net start spooler” on your system with the general agent, then wait about 10 seconds. Then issue the command “net stop spooler”.

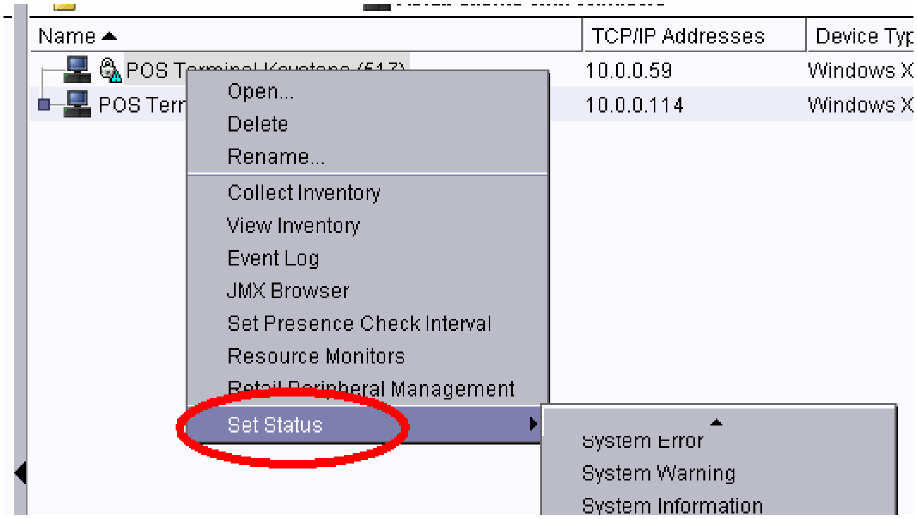


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\taylorbr>net stop spooler
The Print Spooler service is stopping.
The Print Spooler service was stopped successfully.


C:\Documents and Settings\taylorbr>net start spooler
The Print Spooler service is starting.
The Print Spooler service was started successfully.


C:\Documents and Settings\taylorbr>net stop spooler
```

32. After 5 seconds, in Director, you should see the status icon change as shown below.



33. You can manually clear the status icon by right-clicking the system and choosing "Set Status".



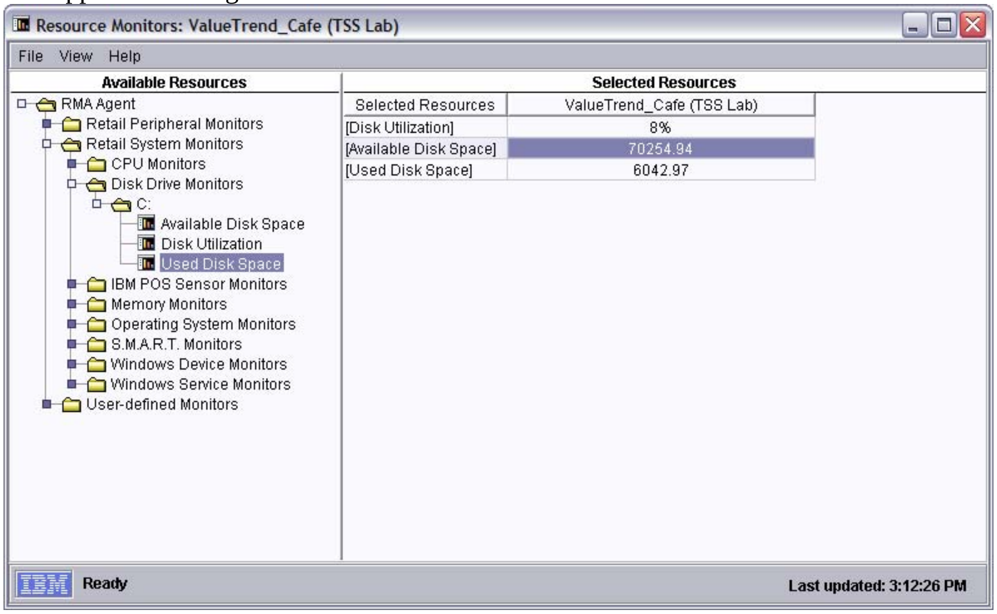
Example: Monitoring disk space available

In this example, we will set up a resource monitor that monitors the available disk space on a system (or selection of multiple systems, or group(s) of systems). When the available disk space gets too low (either as a percentage or as a number of MB), then an event will be generated which can be handled via event action plans.

Note: This example assumes you've already become familiar with the basics of creating a resource monitor and event action plan. If not, you should first try

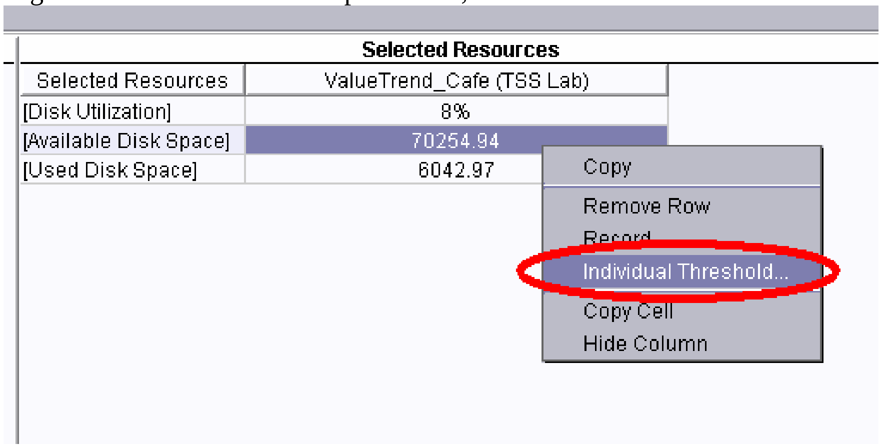
"**Example: Monitoring a Windows Service**", and read the introduction to resource monitors, before proceeding with this example.

1. First, launch the Resource Monitors task, and expand the tree to "RMA Agent / Retail System Monitors / Disk Drive Monitors". Choose the "C:" drive for a Windows system, and double-click on the "Available Disk Space" attribute so it will appear on the right-hand side of the screen.



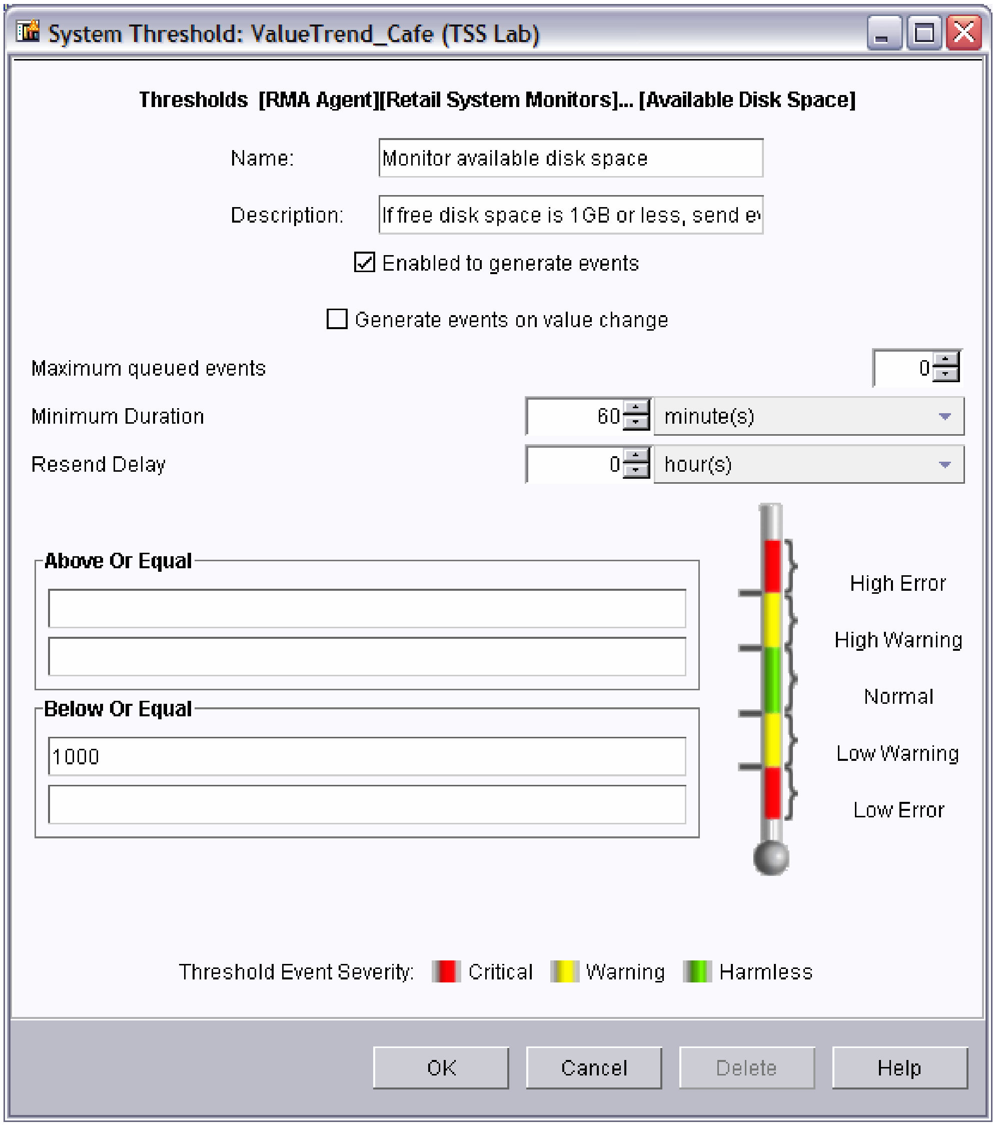
Selected Resources	ValueTrend_Cafe (TSS Lab)
[Disk Utilization]	8%
[Available Disk Space]	70254.94
[Used Disk Space]	6042.97

2. Right-click the available disk space value, and select "Individual Threshold".



Selected Resources	ValueTrend_Cafe (TSS Lab)
[Disk Utilization]	8%
[Available Disk Space]	70254.94
[Used Disk Space]	6042.97

3. In this example, the resource monitor will be configured to send a "Warning" event if the available disk space goes below 1000 MB (i.e. 1 GB) for 60 minutes.



System Threshold: ValueTrend_Cafe (TSS Lab)

Thresholds [RMA Agent][Retail System Monitors]... [Available Disk Space]

Name: Monitor available disk space

Description: If free disk space is 1GB or less, send ev

☑ Enabled to generate events

□ Generate events on value change

Maximum queued events: 0

Minimum Duration: 60 minute(s)

Resend Delay: 0 hour(s)

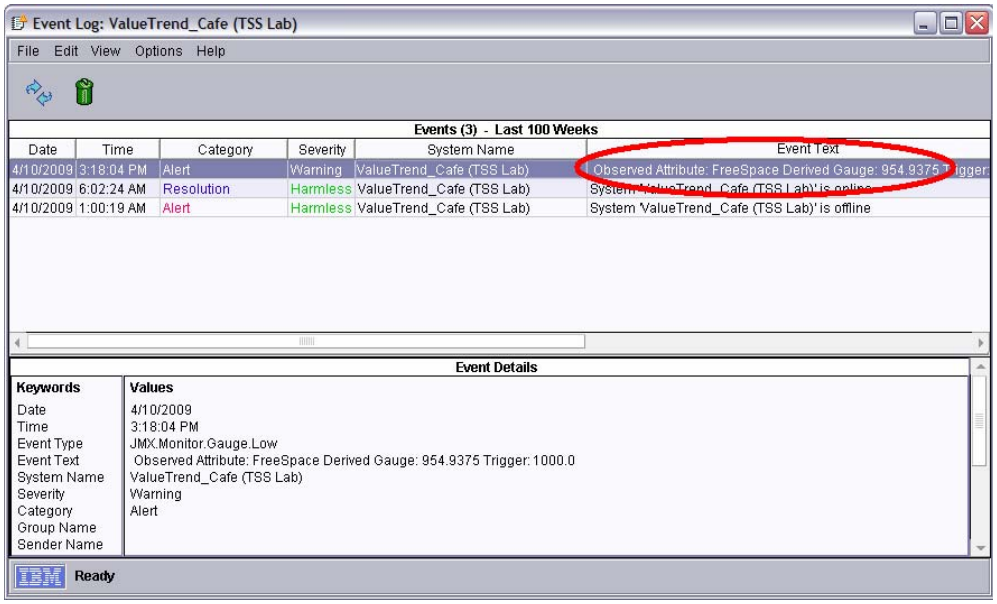
Above Or Equal

Below Or Equal

1000

Threshold Event Severity: 🟥 Critical 🟨 Warning 🟩 Harmless

4. You can test your threshold plan by creating a very large file on the target system that takes up most of the available disk space. (You could also set the threshold higher for initial testing, which is much easier to do.) Once the threshold triggers an event, you will see the event in the event log for the system:



Events (3) - Last 100 Weeks

Date	Time	Category	Severity	System Name	Event Text
4/10/2009	3:18:04 PM	Alert	Warning	ValueTrend_Cafe (TSS Lab)	Observed Attribute: FreeSpace Derived Gauge: 954.9375 Trigger:
4/10/2009	6:02:24 AM	Resolution	Harmless	ValueTrend_Cafe (TSS Lab)	System 'ValueTrend_Cafe (TSS Lab)' is online
4/10/2009	1:00:19 AM	Alert	Harmless	ValueTrend_Cafe (TSS Lab)	System 'ValueTrend_Cafe (TSS Lab)' is offline

Event Details

Keywords	Values
Date	4/10/2009
Time	3:18:04 PM
Event Type	JMX.Monitor.Gauge.Low
Event Text	Observed Attribute: FreeSpace Derived Gauge: 954.9375 Trigger: 1000.0
System Name	ValueTrend_Cafe (TSS Lab)
Severity	Warning
Category	Alert
Group Name	
Sender Name	

5. You can now right-click the event from the event-log, and begin creating your event filter and your event action plans. (Note: Be careful about the extended attributes, because they will, by default, be too exclusive/specific for monitoring a large number of systems.) For more information, see "**Chapter 6 – Event Management**".

6. You can also organize your new resource monitor into a threshold plan, then apply it to a wider range of systems and/or groups.

Example: Monitoring CPU temperature and fan speed

In this example, we'll show you how to create a resource monitor that alerts when the CPU temperature is too high for too long, or when the fan speed is too low for a long period of time.

Before continuing with this example, you should check to see whether the system you are monitoring has pre-configured thresholds at the following URL: http://www-01.ibm.com/support/docview.wss?rs=219&uid=pos1R1004330

If possible, you should download and apply the thresholds from the URL above, which will save you considerable time as you configure Director for hardware monitoring via RMA.

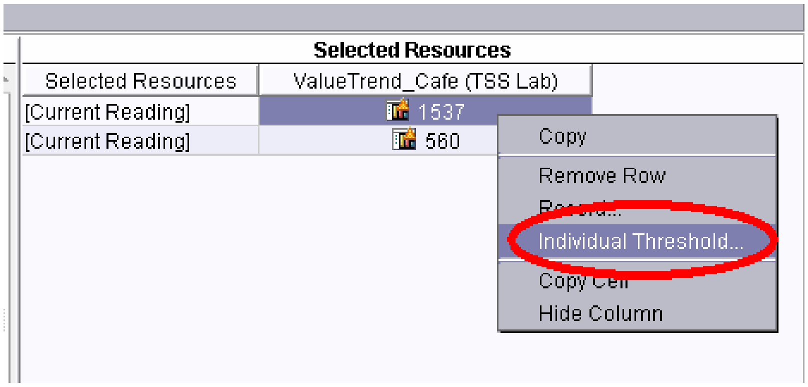
1. Before you can use RMA to monitor the CPU temperature or fan speed on IBM POS hardware, you need to first download and install the POS Sensor Drivers for IBM POS systems, which can be found here:

http://www-01.ibm.com/support/docview.wss?rs=219&uid=pos1R4000167

2. Launch the Resource Monitors task, and expand the tree to “RMA Agent / Retail System Monitors / IBM POS Sensor Monitors”. If you are using a system that has an on-board service processor (with light-path management), then you should use the “Service Processor Sensor Monitors”. If your system does not have a service processor, then use “Numeric POS Sensor Monitors”.

3. Locate the CPU temperature and CPU fan speed attributes, and double-click them to display the current value on the right-hand side of the screen.

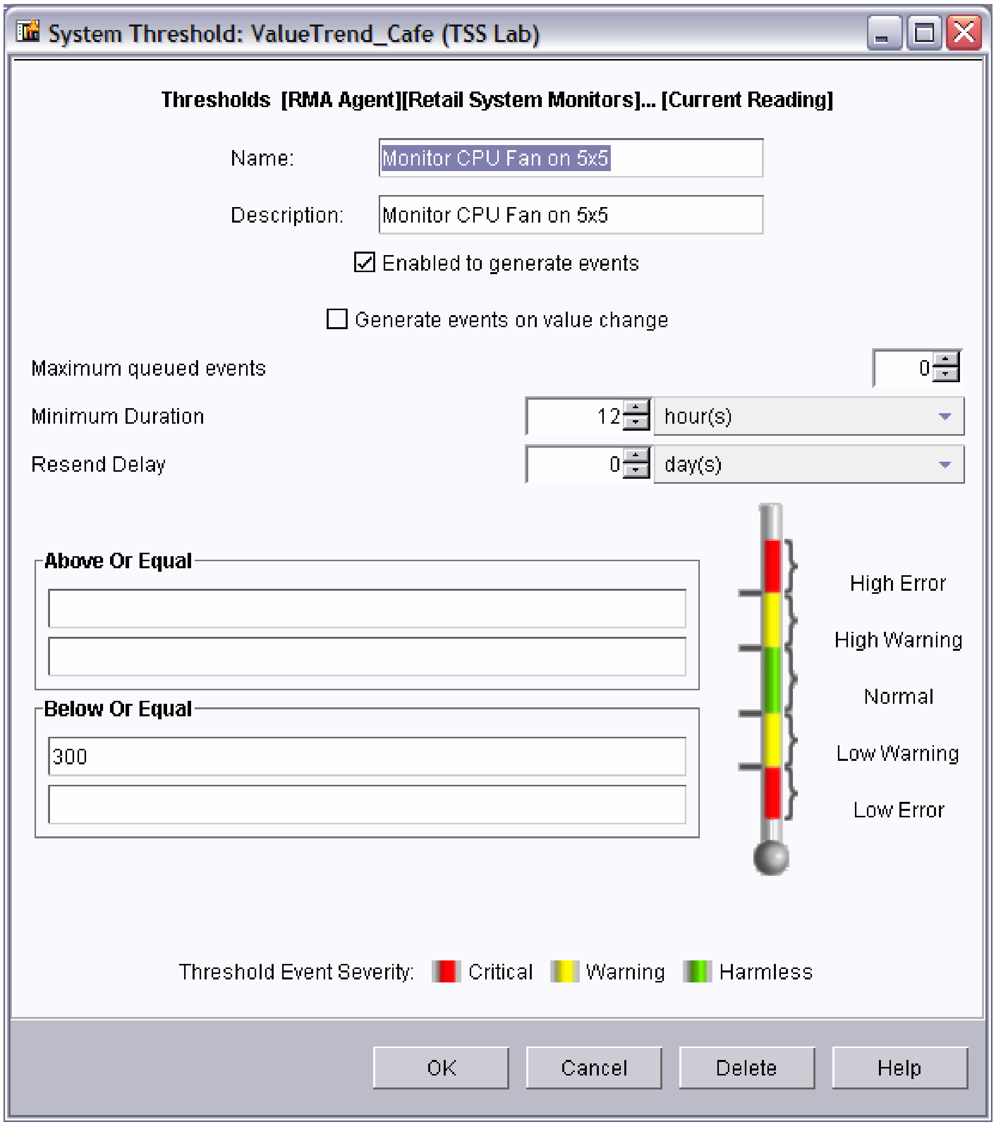
4. Left-click the first value (in this example the first value is the CPU temperature). Select “Individual Threshold”.



Selected Resources

Selected Resources	ValueTrend_Cafe (TSS Lab)
[Current Reading]	1537
[Current Reading]	560

5. In this example, we are monitoring a 4840-5x5 system, and we will configure the monitor to send a “Warning” event when the CPU fan drops below 300 RPM’s for 12 hours or more.


System Threshold: ValueTrend_Cafe (TSS Lab)

Thresholds [RMA Agent][Retail System Monitors]... [Current Reading]

Name: Monitor CPU Fan on 5x5

Description: Monitor CPU Fan on 5x5

☑ Enabled to generate events

□ Generate events on value change

Maximum queued events: 0

Minimum Duration: 12 hour(s)

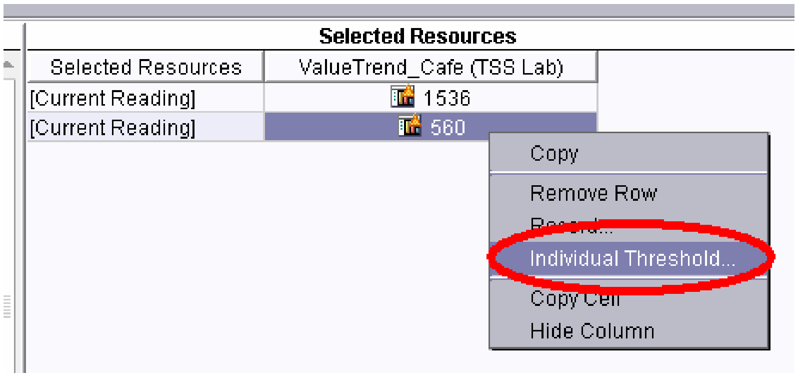
Resend Delay: 0 day(s)

Above Or Equal

Below Or Equal: 300

Threshold Event Severity: 🟥 Critical 🟨 Warning 🟩 Harmless

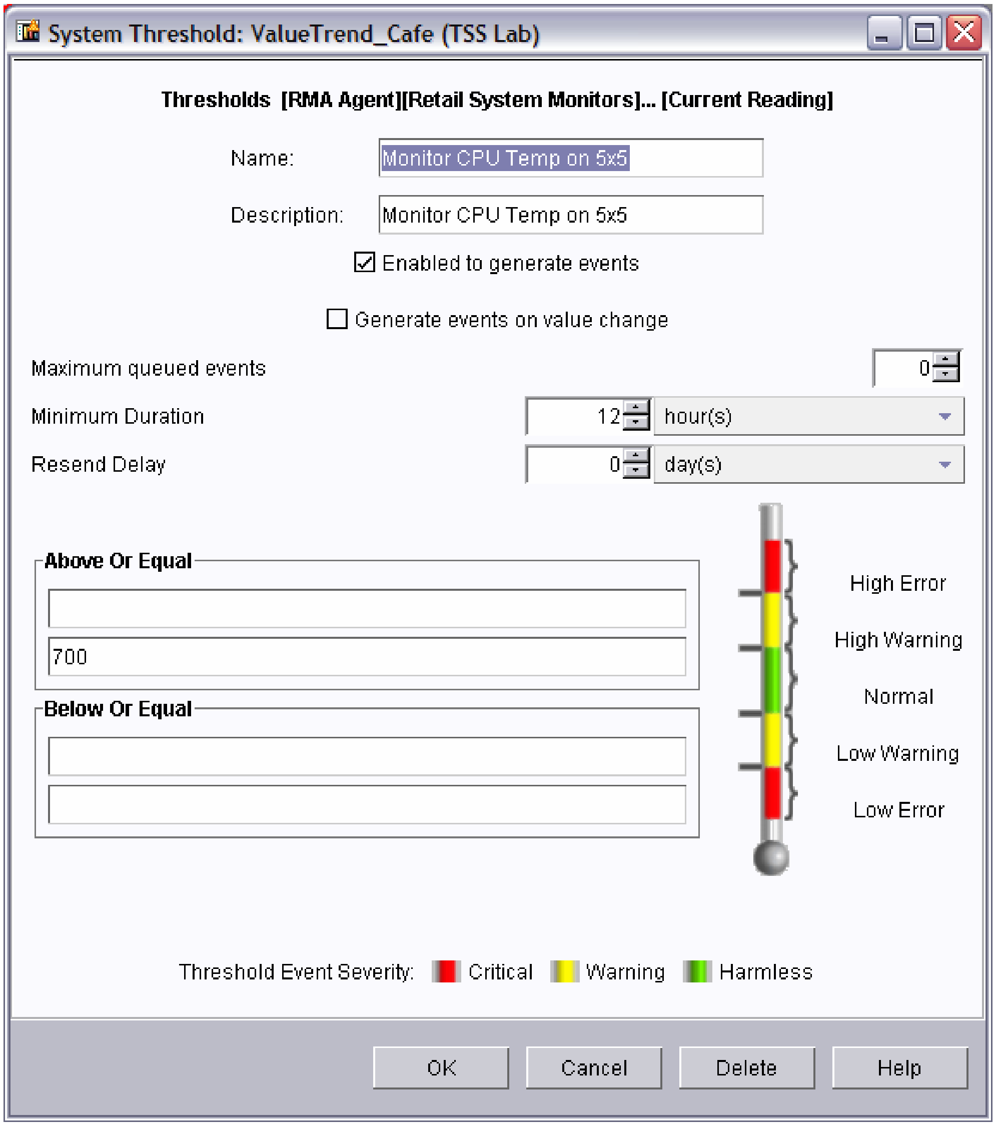
6. Click OK, then right-click the value that represents the CPU temperature.



Selected Resources

Selected Resources	ValueTrend_Cafe (TSS Lab)
[Current Reading]	1536
[Current Reading]	560

7. In this example, we will configure the monitor to send a “Warning” event if the CPU temperature remains above 70-degrees Celsius for more than 12 hours.


System Threshold: ValueTrend_Cafe (TSS Lab)

Thresholds [RMA Agent][Retail System Monitors]... [Current Reading]

Name: Monitor CPU Temp on 5x5

Description: Monitor CPU Temp on 5x5

☑ Enabled to generate events

□ Generate events on value change

Maximum queued events: 0

Minimum Duration: 12 hour(s)

Resend Delay: 0 day(s)

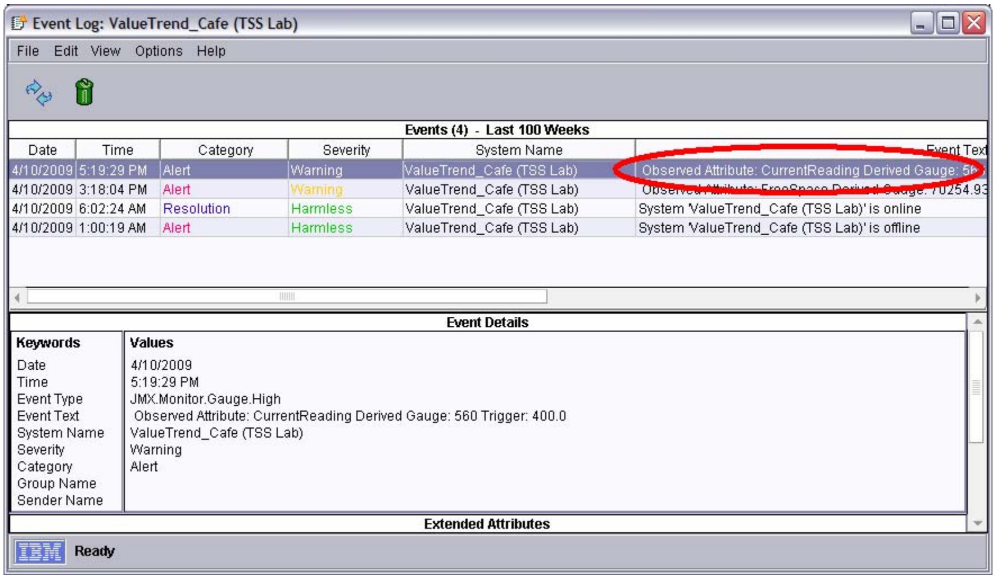
Above Or Equal

700

Below Or Equal

Threshold Event Severity: 🟥 Critical 🟨 Warning 🟩 Harmless

8. To test your resource monitors, you can either modify the resource monitor with different values (i.e. a low temperature and a high fan speed, both with smaller minimum durations), or you can physically attempt to cause the problem, for example, by blocking the CPU fan on a running system. Once the threshold triggers an event, you will see the event in the event log for the system:


Event Log: ValueTrend_Cafe (TSS Lab)
File Edit View Options Help
Ready

Events (4) - Last 100 Weeks

Date	Time	Category	Severity	System Name	Event Text
4/10/2009	5:19:29 PM	Alert	Warning	ValueTrend_Cafe (TSS Lab)	Observed Attribute: CurrentReading Derived Gauge: 5
4/10/2009	3:18:04 PM	Alert	Warning	ValueTrend_Cafe (TSS Lab)	Observed Attribute: FreeSpace Derived Gauge: 70254.93
4/10/2009	6:02:24 AM	Resolution	Harmless	ValueTrend_Cafe (TSS Lab)	System 'ValueTrend_Cafe (TSS Lab)' is online
4/10/2009	1:00:19 AM	Alert	Harmless	ValueTrend_Cafe (TSS Lab)	System 'ValueTrend_Cafe (TSS Lab)' is offline

Event Details

Keywords	Values
Date	4/10/2009
Time	5:19:29 PM
Event Type	JMX.Monitor.Gauge.High
Event Text	Observed Attribute: CurrentReading Derived Gauge: 560 Trigger: 400.0
System Name	ValueTrend_Cafe (TSS Lab)
Severity	Warning
Category	Alert
Group Name	
Sender Name	

Extended Attributes

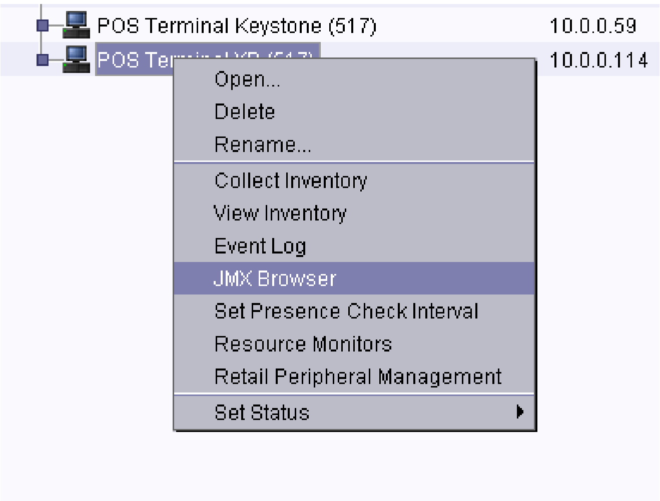
9. You can now right-click the event from the event-log, and begin creating your event filter and your event action plans. (Note: Be careful about the extended attributes, because they will, by default, be too exclusive/specific for monitoring a large number of systems.) For more information, see "**Chapter 6 – Event Management**".

10. You can also organize your new resource monitor into a threshold plan, then apply it to a wider range of systems and/or groups.

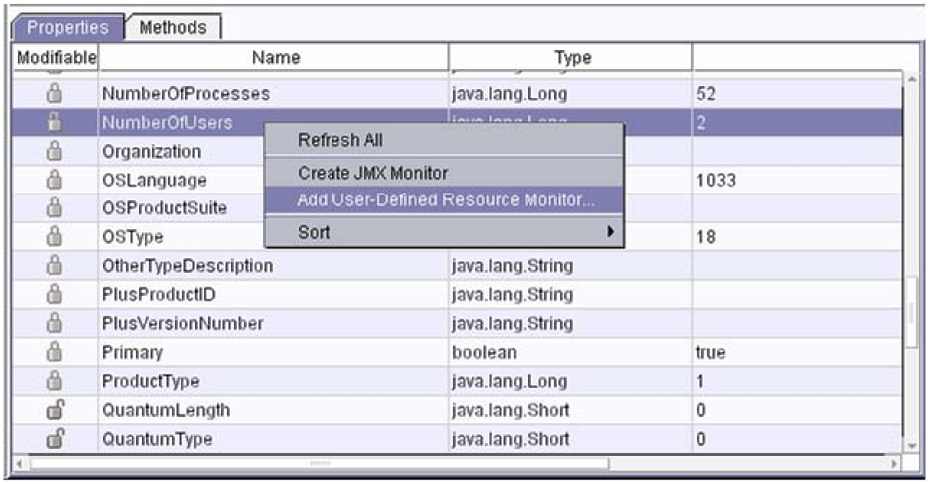
Example: Creating a "user-defined" resource monitor

If you can't find the value that you're looking for in the "Resource Monitors" task, you can create a custom (user-defined) monitor based on any value available in the JMX browser.

1. To create a custom-monitor, first open the JMX Browser for a system.

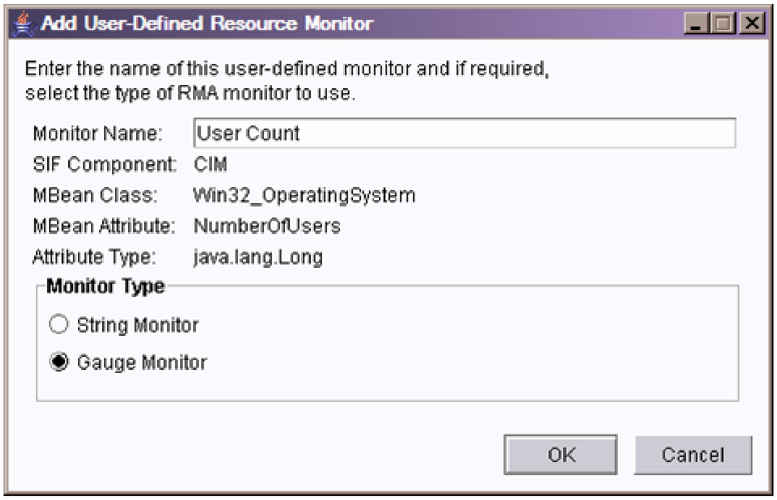


2. Within the JMX Browser, locate the value you want to monitor, then right-click and select "Add User-Defined Resource Monitor".



Modifiable	Name	Type	
🔒	NumberOfProcesses	java.lang.Long	52
🔒	NumberOfUsers		2
🔒	Organization		
🔒	OSLanguage		1033
🔒	OSProductSuite		
🔒	OSType		18
🔒	OtherTypeDescription	java.lang.String	
🔒	PlusProductID	java.lang.String	
🔒	PlusVersionNumber	java.lang.String	
🔒	Primary	boolean	true
🔒	ProductType	java.lang.Long	1
🔓	QuantumLength	java.lang.Short	0
🔓	QuantumType	java.lang.Short	0

3. Give it a name and click OK.



Enter the name of this user-defined monitor and if required, select the type of RMA monitor to use.

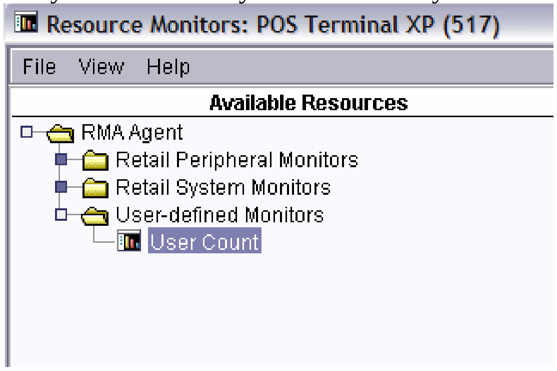
Monitor Name:	User Count
SIF Component:	CIM
MBean Class:	Win32_OperatingSystem
MBean Attribute:	NumberOfUsers
Attribute Type:	java.lang.Long

Monitor Type

○ String Monitor

● Gauge Monitor

4. Your custom resource monitor will now appear in the “Resource Monitors” UI, and you can use it as you would use any other resource monitor.



Chapter 8 – Software Distribution

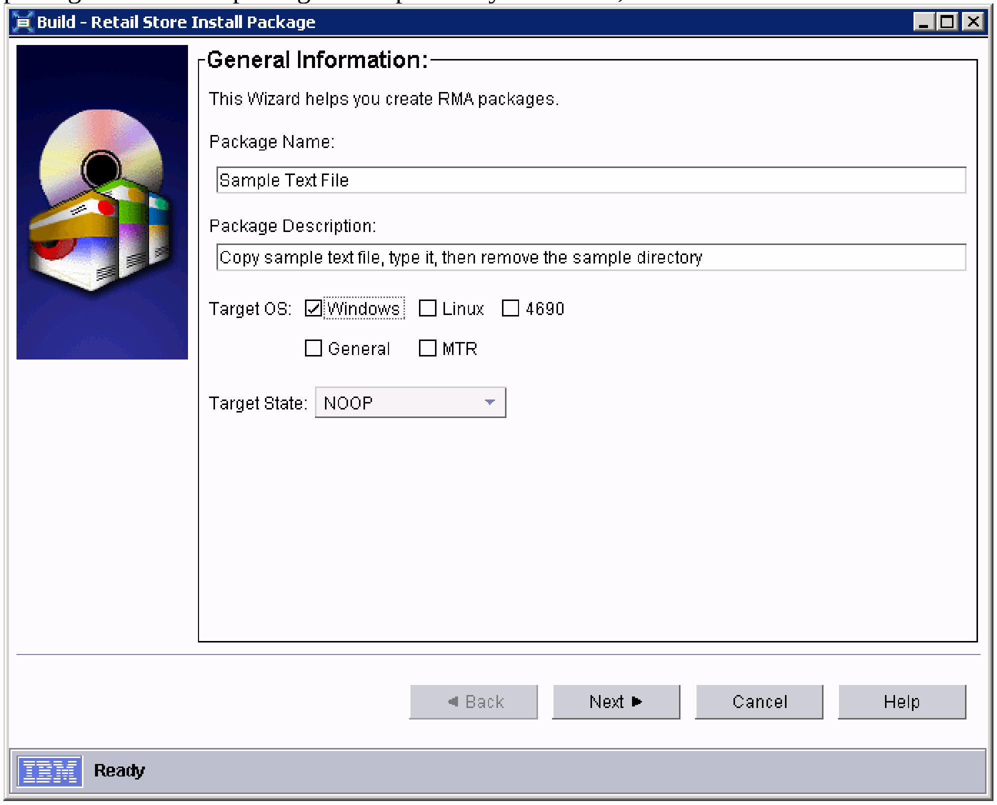
Example: Basic/Generic RMA Software Distribution

In this exercise, you will create a simple text file, distribute that text file to the master agent, and execute a command that outputs the contents of the text file. This will illustrate how to use RMA software distribution to deploy files and execute remote commands.

1. On the Director Server machine, create a simple text file (using the Microsoft “notepad” application). Type “hello” in the text file, and save it as “C:\sample.txt”.

2. Start by right-clicking the “**RMA Software Distribution**” task (in the tasks pane), and select “**Create Install Package**”.

3. Select “Windows” for the target OS, and “NOOP” for the target state. Enter a package name and a package description of your choice, then click “Next”.



Build - Retail Store Install Package

General Information:

This Wizard helps you create RMA packages.

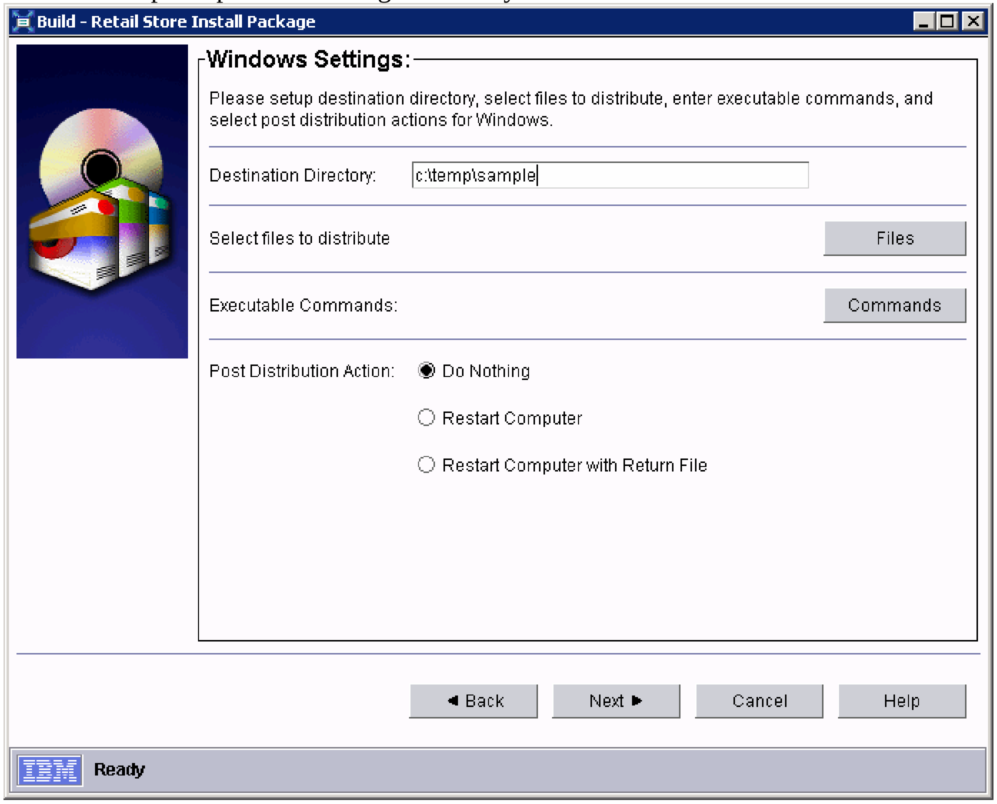
Package Name: Sample Text File

Package Description: Copy sample text file, type it, then remove the sample directory

Target OS: ☑ Windows ☐ Linux ☐ 4690 ☐ General ☐ MTR

Target State: NOOP

4. Enter “c:\temp\sample” for the target directory.



Build - Retail Store Install Package

Windows Settings:

Please setup destination directory, select files to distribute, enter executable commands, and select post distribution actions for Windows.

Destination Directory: c:\temp\sample

Select files to distribute

Executable Commands:

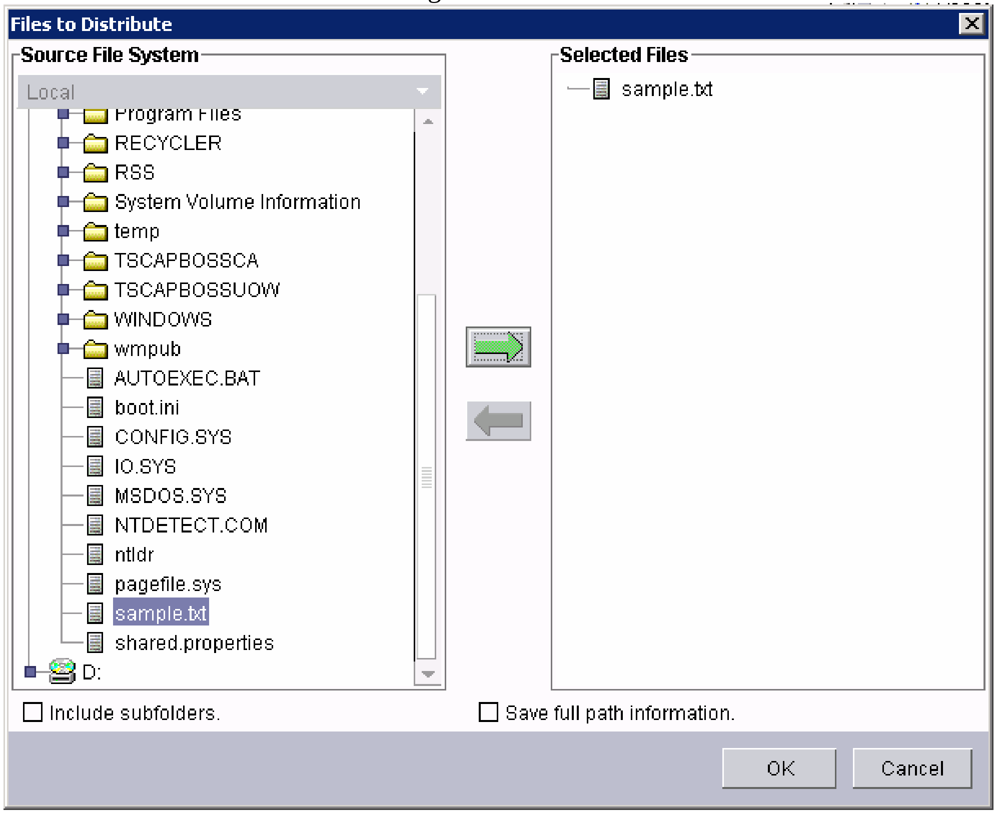
Post Distribution Action:

● Do Nothing

○ Restart Computer

○ Restart Computer with Return File

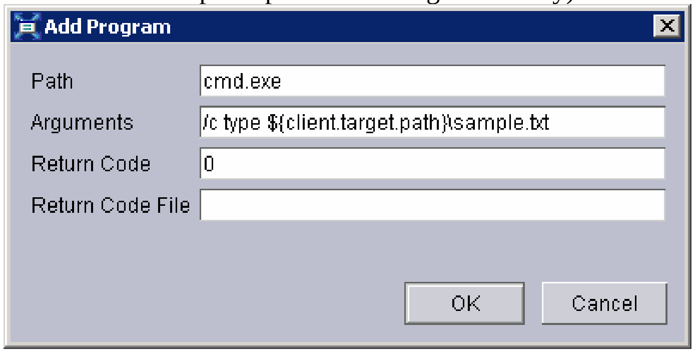
5. Click “Files” and select your sample.txt file, then click the “→” button to add the file to the list of selected files on the right. Click OK.



☐ Include subfolders.

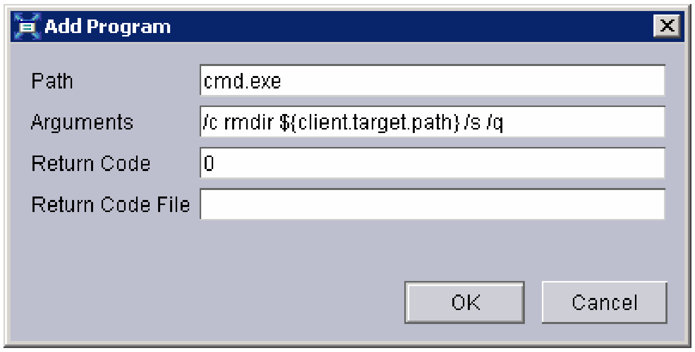
☐ Save full path information.

6. Click “Commands”, then “Add” to enter your first command. Use the “cmd.exe /c” command to execute your command (you can use “${client.target.path}” instead of “c:\temp\sample” for the target directory).



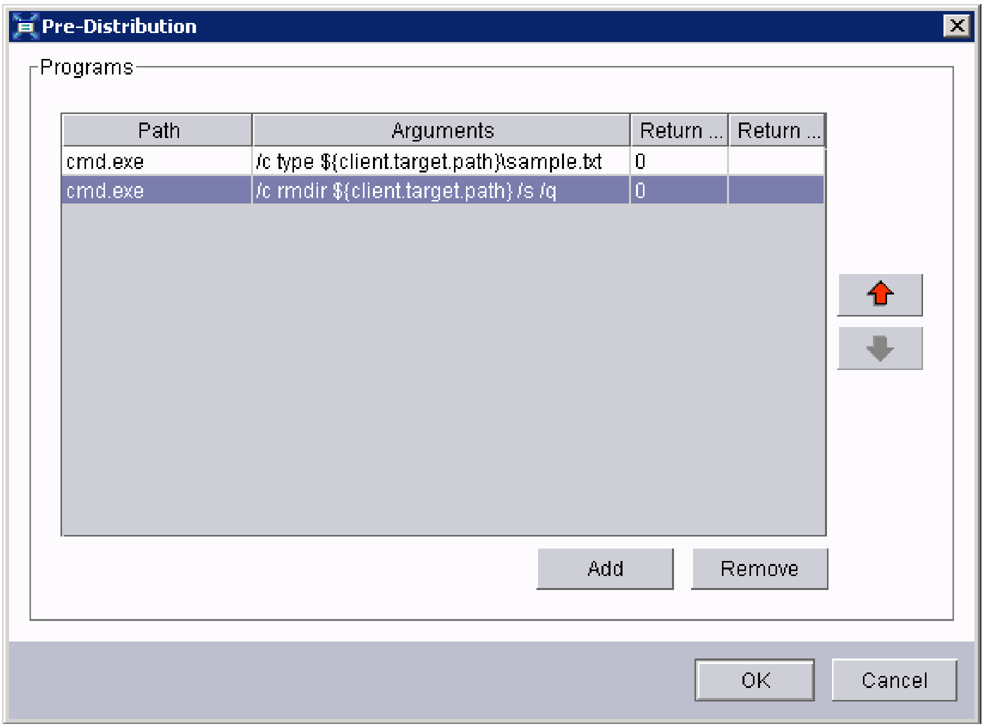
Path	cmd.exe
Arguments	/c type ${client.target.path}\sample.txt
Return Code	0
Return Code File	

7. Click "Add" again to enter a second command. Remove the target directory using "cmd.exe" also.



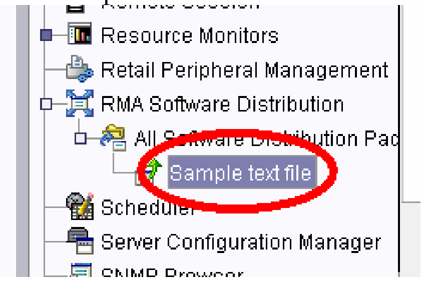
Path	cmd.exe
Arguments	/c rmdir ${client.target.path} /s /q
Return Code	0
Return Code File	

8. Your two commands should now look like this:

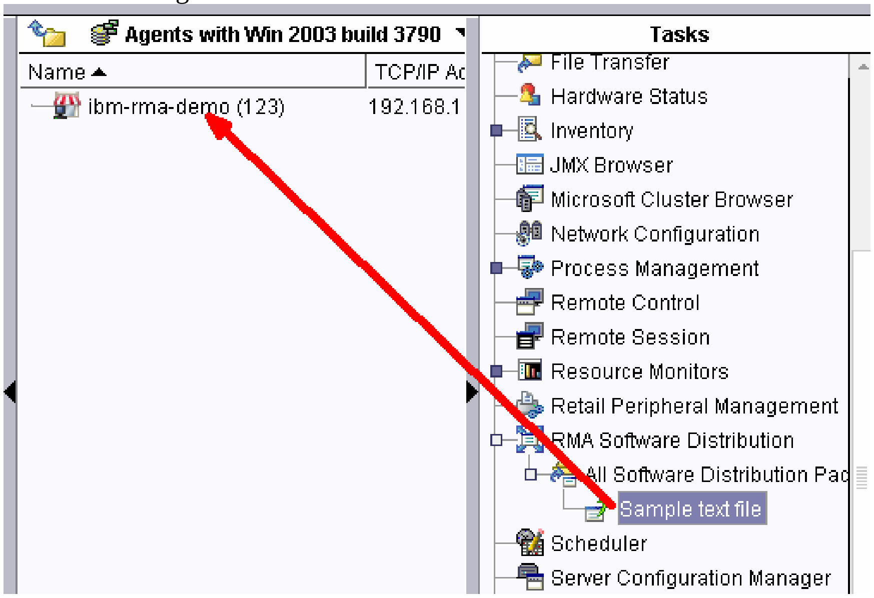


Path	Arguments	Return ...	Return ...
cmd.exe	/c type ${client.target.path}\sample.txt	0	
cmd.exe	/c rmdir ${client.target.path} /s /q	0	

9. Now, finish creating the software distribution package. After the software distribution package is created, you will see the new software package listed under “**RMA Software Distribution / All Software Distribution Packages**” in the tasks pane.


Resource Monitors
Retail Peripheral Management
RMA Software Distribution
All Software Distribution Pac
Sample text file
Scheduler
Server Configuration Manager
SNMP Browser

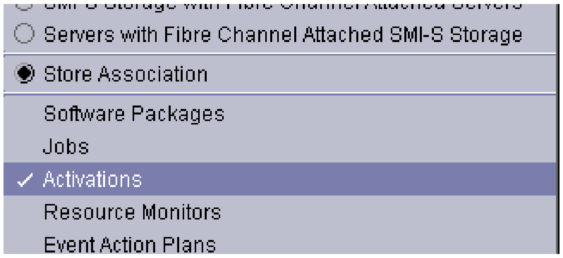
10. To apply the package to the master agent, drag-and-drop this package to the MO for the master agent.



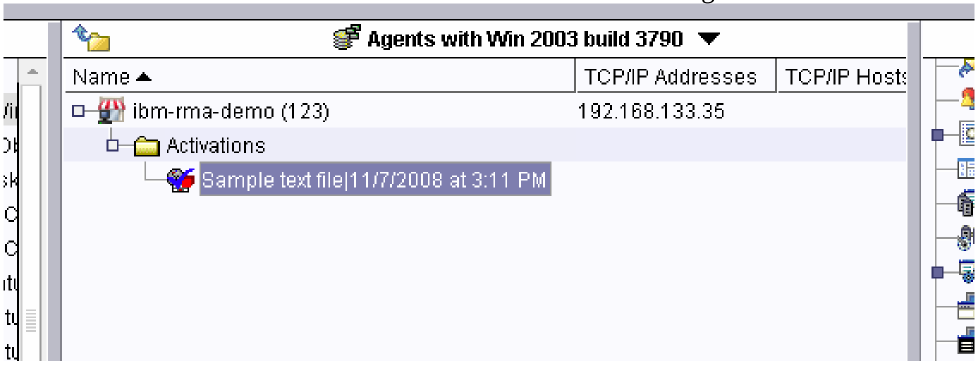
11. Select “**Execute Now**” when prompted.

12. You should see the execution history window appear. For now, you can close the execution history window.

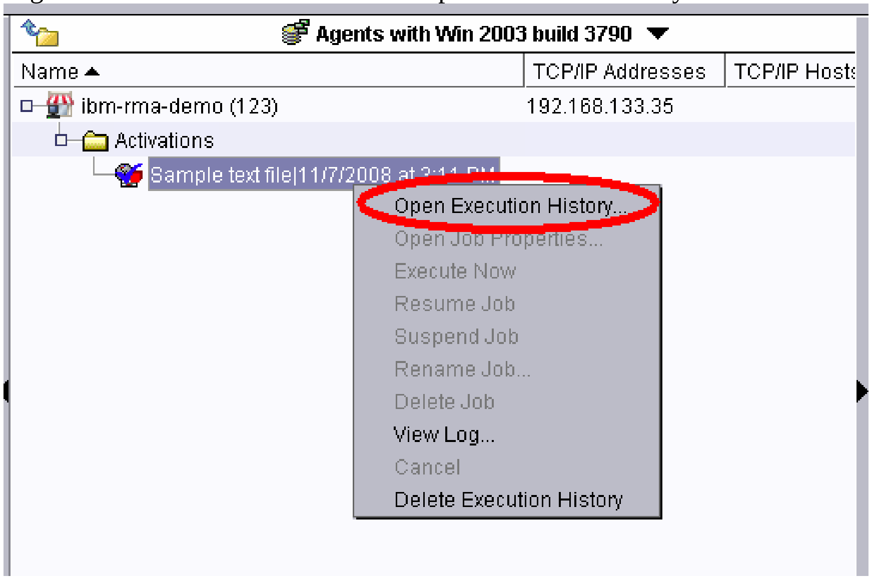
13. Make sure that “**Activations**” is checked in the “**Associations**” menu of the Director Console.


○ SMI-S Storage with Fibre Channel Attached Servers
○ Servers with Fibre Channel Attached SMI-S Storage
● Store Association
Software Packages
Jobs
✓ Activations
Resource Monitors
Event Action Plans

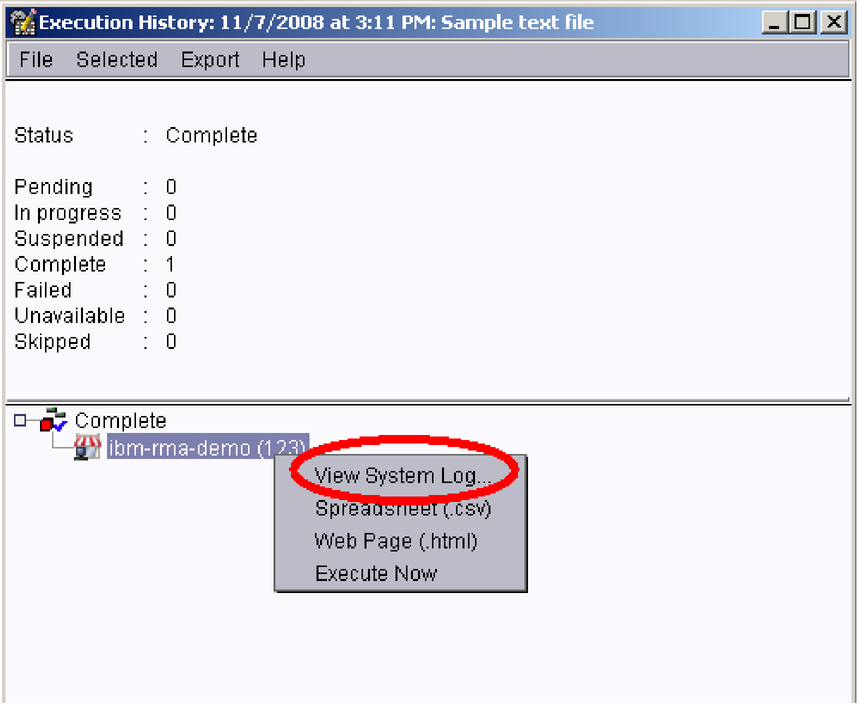
14. Expand the tree in the center pane, so that you can see the execution history icon underneath the “Activations” folder on the MO for the master agent.



15. Right-click the activation and select “Open Execution History”.

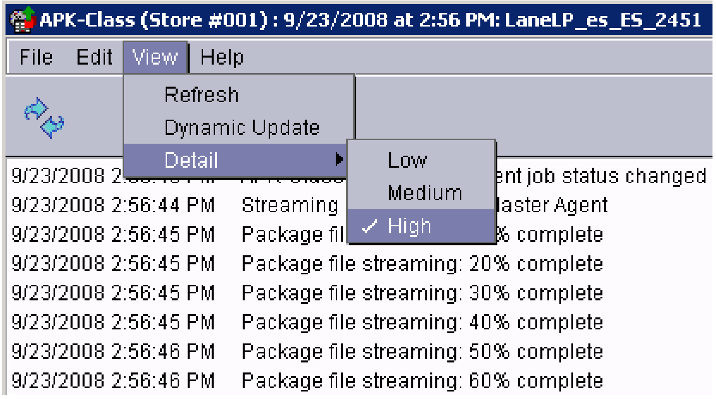


16. You can see the detailed logs for the execution by right-clicking an entry in the execution history and selecting “**View System Log**”.



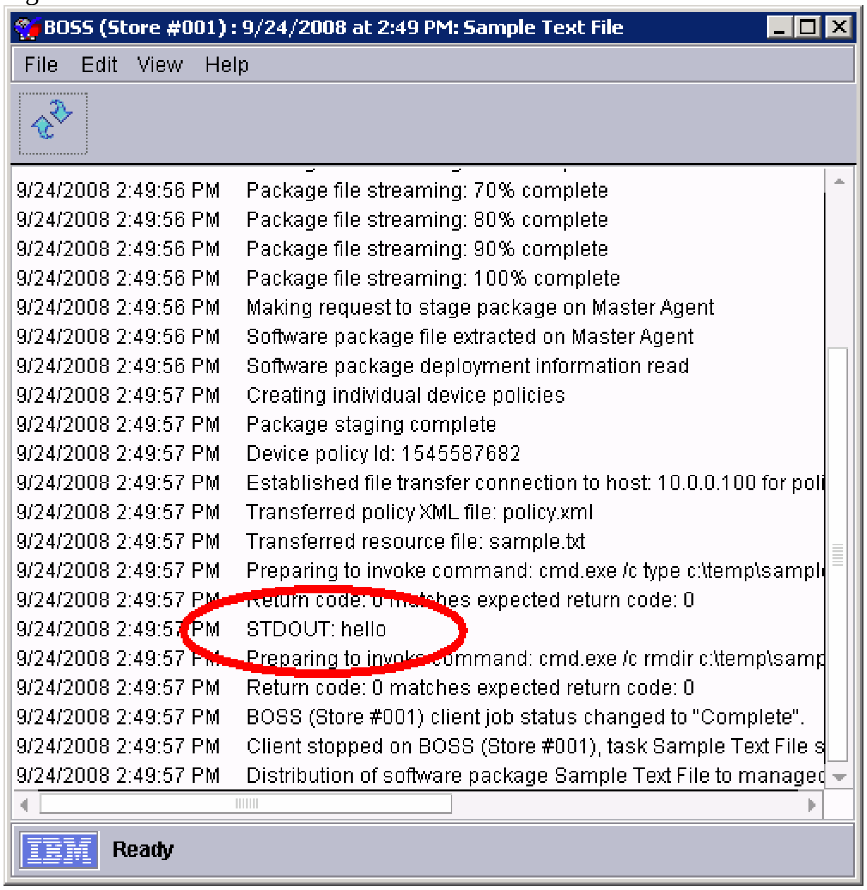
```
Status      :  Complete

Pending     :  0
In progress :  0
Suspended   :  0
Complete    :  1
Failed      :  0
Unavailable :  0
Skipped     :  0
```

17. When the system log appears for this system, click “**View / Detail / High**” to see the detailed logs.


APK-Class (Store #001) : 9/23/2008 at 2:56 PM: LaneLP_es_ES_2451
File
Edit
View
Help
Refresh
Dynamic Update
Detail
Low
Medium
✓ High

```
9/23/2008 2                                 ent job status changed
9/23/2008 2:56:44 PM   Streaming            laster Agent
9/23/2008 2:56:45 PM   Package fil          % complete
9/23/2008 2:56:45 PM   Package file streaming: 20% complete
9/23/2008 2:56:45 PM   Package file streaming: 30% complete
9/23/2008 2:56:45 PM   Package file streaming: 40% complete
9/23/2008 2:56:46 PM   Package file streaming: 50% complete
9/23/2008 2:56:46 PM   Package file streaming: 60% complete
```

18. Since you executed the “type” command in your package, the entire contents of your “sample.txt” file should be displayed in the detailed software distribution logs.



```
9/24/2008 2:49:56 PM    Package file streaming: 70% complete
9/24/2008 2:49:56 PM    Package file streaming: 80% complete
9/24/2008 2:49:56 PM    Package file streaming: 90% complete
9/24/2008 2:49:56 PM    Package file streaming: 100% complete
9/24/2008 2:49:56 PM    Making request to stage package on Master Agent
9/24/2008 2:49:56 PM    Software package file extracted on Master Agent
9/24/2008 2:49:56 PM    Software package deployment information read
9/24/2008 2:49:57 PM    Creating individual device policies
9/24/2008 2:49:57 PM    Package staging complete
9/24/2008 2:49:57 PM    Device policy Id: 1545587682
9/24/2008 2:49:57 PM    Established file transfer connection to host: 10.0.0.100 for poli
9/24/2008 2:49:57 PM    Transferred policy XML file: policy.xml
9/24/2008 2:49:57 PM    Transferred resource file: sample.txt
9/24/2008 2:49:57 PM    Preparing to invoke command: cmd.exe /c type c:\temp\sampl
9/24/2008 2:49:57 PM    Return code: 0 matches expected return code: 0
9/24/2008 2:49:57 PM    STDOUT: hello
9/24/2008 2:49:57 PM    Preparing to invoke command: cmd.exe /c rmdir c:\temp\samp
9/24/2008 2:49:57 PM    Return code: 0 matches expected return code: 0
9/24/2008 2:49:57 PM    BOSS (Store #001) client job status changed to "Complete".
9/24/2008 2:49:57 PM    Client stopped on BOSS (Store #001), task Sample Text File s
9/24/2008 2:49:57 PM    Distribution of software package Sample Text File to managed
```

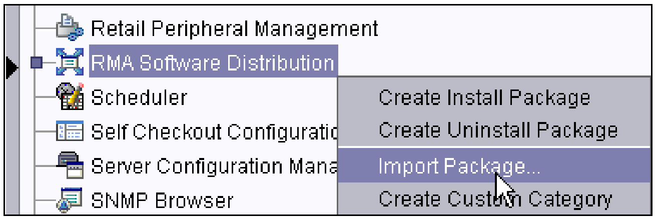
Example: Updating RMA via RMA Software Distribution

These instructions describe how the RMA master agent and/or general agent can be updated using RMA software distribution and the IBM Director Console. The RMA software CD includes packages that are available to be imported into IBM Director. These packages contain all the files and commands needed to update RMA automatically.

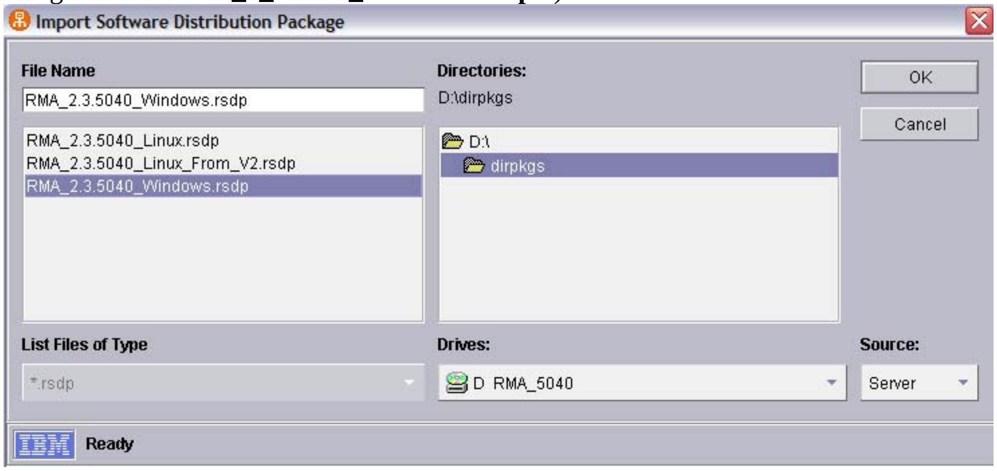
1. Logon to the IBM Director Console.

2. Insert the RMA software CD.

3. Right click on the RMA Software Distribution Task and Select Import Package



4. Browse the RMA software CD to the **dirpkgs** directory and select the package to use for the update and select **OK.** (The example below is for a Windows update, using the file "**RMA_2_3.5040_Windows.rsdp**".)



Import Software Distribution Package

File Name: RMA_2.3.5040_Windows.rsdp

RMA_2.3.5040_Linux.rsdp
RMA_2.3.5040_Linux_From_V2.rsdp
RMA_2.3.5040_Windows.rsdp

Directories: D:\dirpkgs

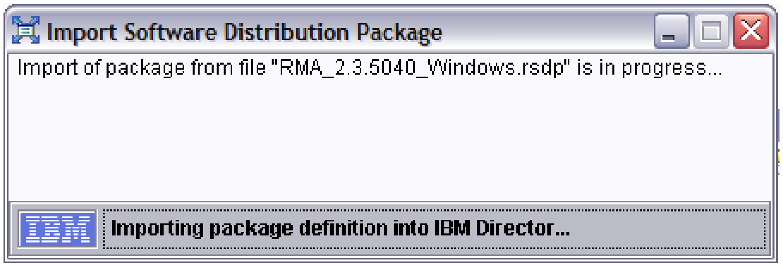
D:\
dirpkgs

List Files of Type: *.rsdp

Drives: D RMA_5040

Source: Server

Ready

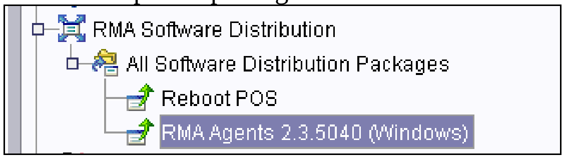


Import Software Distribution Package

Import of package from file "RMA_2.3.5040_Windows.rsdp" is in progress...

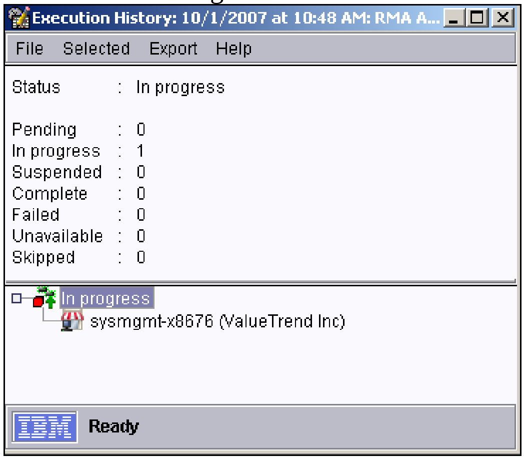
Importing package definition into IBM Director...

5. After the package is imported expand the RMA Software Distribution Task to view the imported package.


RMA Software Distribution
All Software Distribution Packages
Reboot POS
RMA Agents 2.3.5040 (Windows)

6. Drag the RMA update packages to the Agents that require an update and select Execute Now. (**Note**: You can drag it to a single system, a selection of multiple systems, a group, or you can schedule it to occur at a later time.)

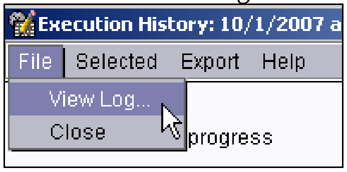
7. Installation will begin.


Execution History: 10/1/2007 at 10:48 AM: RMA A...
File Selected Export Help
In progress
IBM
Ready

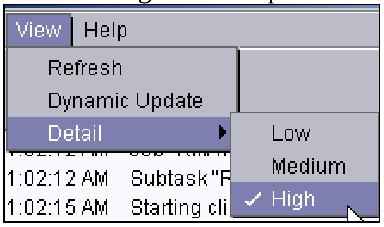
```
Status      :  In progress

Pending     :  0
In progress :  1
Suspended   :  0
Complete    :  0
Failed      :  0
Unavailable :  0
Skipped     :  0
```

sysmgmt-x8676 (ValueTrend Inc)

8. To view a detailed log of the installation select File > View Log.

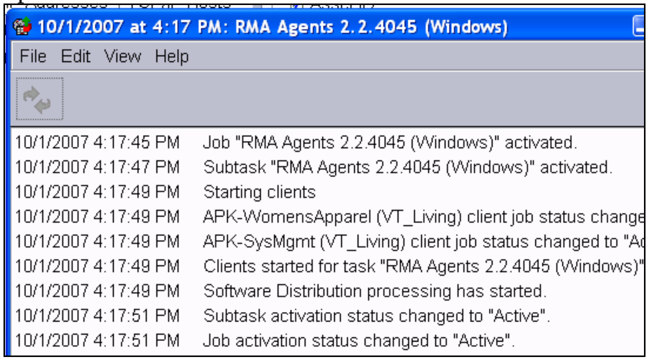


9. When the log window opens select View > Detail > High



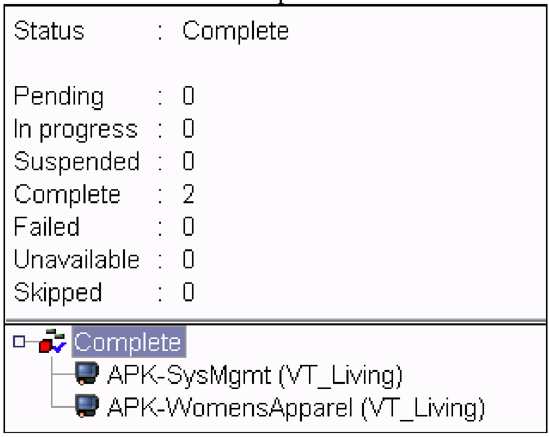
```
1:02:12 AM   Subtask "F
1:02:15 AM   Starting cli
```

10. On the log window select View > Dynamic Update to have the log automatically updated



```
10/1/2007 4:17:45 PM   Job "RMA Agents 2.2.4045 (Windows)" activated.
10/1/2007 4:17:47 PM   Subtask "RMA Agents 2.2.4045 (Windows)" activated.
10/1/2007 4:17:49 PM   Starting clients
10/1/2007 4:17:49 PM   APK-WomensApparel (VT_Living) client job status change
10/1/2007 4:17:49 PM   APK-SysMgmt (VT_Living) client job status changed to "A
10/1/2007 4:17:49 PM   Clients started for task "RMA Agents 2.2.4045 (Windows)"
10/1/2007 4:17:49 PM   Software Distribution processing has started.
10/1/2007 4:17:51 PM   Subtask activation status changed to "Active".
10/1/2007 4:17:51 PM   Job activation status changed to "Active".
```

11. When installation is complete there will be a complete status.



```
Status      :  Complete

Pending     :  0
In progress :  0
Suspended   :  0
Complete    :  2
Failed      :  0
Unavailable :  0
Skipped     :  0
```

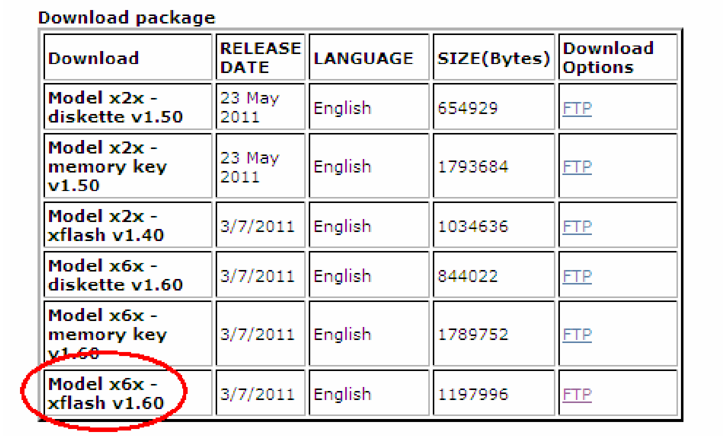
```
Complete
 ├─ APK-SysMgmt (VT_Living)
 └─ APK-WomensApparel (VT_Living)
```

Example: Deploying an xFlash BIOS Update via RMA Software Distribution

These instructions describe how you can use RMA to remotely deploy an xFlash BIOS update on a system using RMA Software Distribution. Currently (at the time of thise writing) xFlash BIOS updates are only available for Windows Systems. In the future they may be made available for SuSE Linux systems as well. 4690 Terminal BIOS updates can be applied remotely without xFlash.

> **Note:** All remote BIOS updates should be tested **thoroughly** in a lab prior to being mass deployed in a production environment to prevent any unforeseen issues.

1. First, download the xFlash BIOS update executable for your system type from the IBM Retail Store Solutions Support site: http://www2.clearlake.ibm.com/store/support/index.html

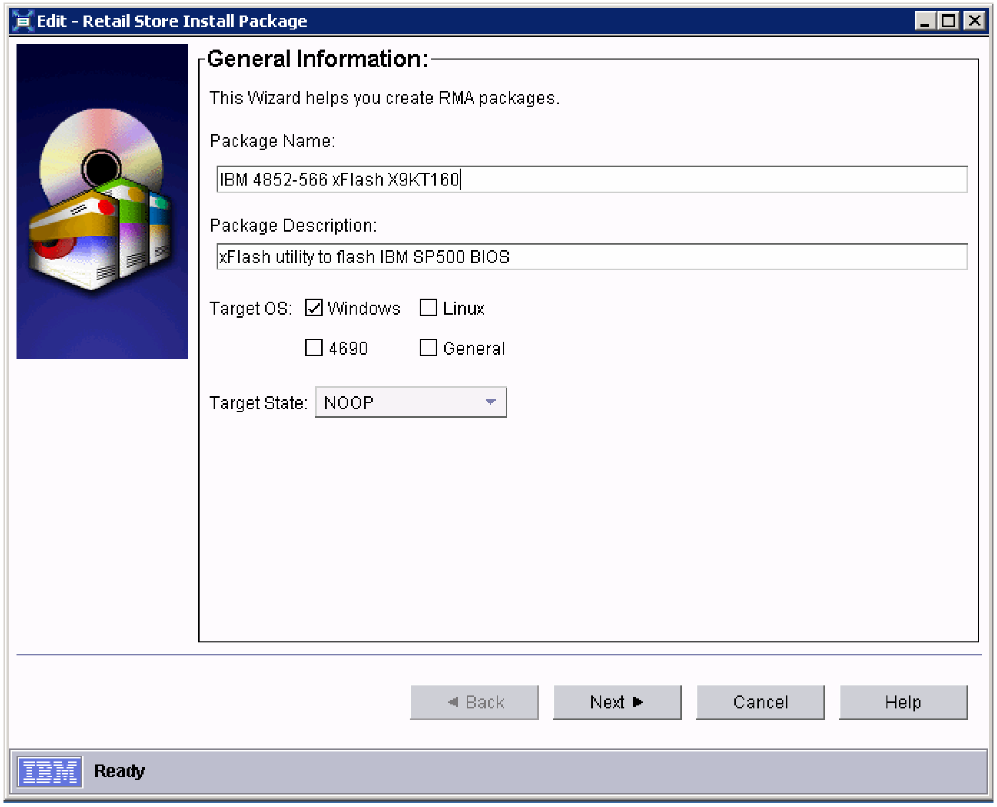


Download package

Download	RELEASE DATE	LANGUAGE	SIZE(Bytes)	Download Options
Model x2x - diskette v1.50	23 May 2011	English	654929	FTP
Model x2x - memory key v1.50	23 May 2011	English	1793684	FTP
Model x2x - xflash v1.40	3/7/2011	English	1034636	FTP
Model x6x - diskette v1.60	3/7/2011	English	844022	FTP
Model x6x - memory key v1.60	3/7/2011	English	1789752	FTP
Model x6x - xflash v1.60	3/7/2011	English	1197996	FTP

2. Right-click on the “RMA Software Distribution” task on the IBM Director Console and select “Create Install Package”.

3. On the first page of the Wizard, give the package a useful name and description, ensure the “Target OS” is set to “Windows”, and the “Target State” is set to “NOOP”. Click “Next” to continue:


Edit - Retail Store Install Package

General Information:

This Wizard helps you create RMA packages.

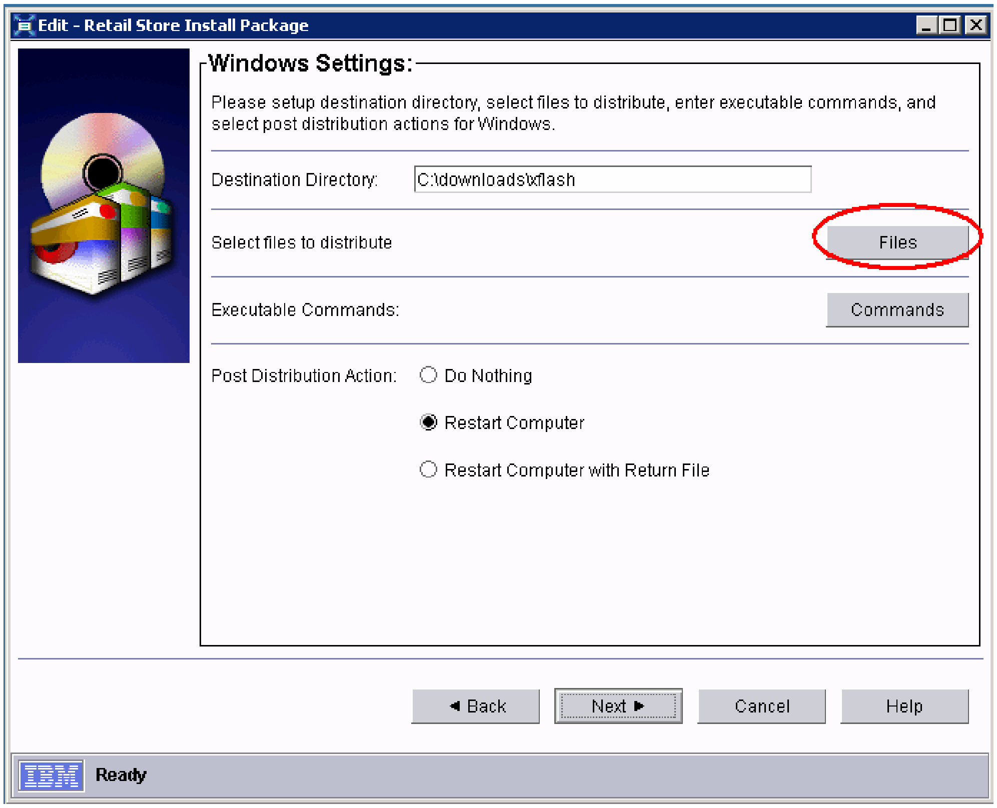
Package Name: IBM 4852-566 xFlash X9KT160

Package Description: xFlash utility to flash IBM SP500 BIOS

Target OS: ☑ Windows □ Linux □ 4690 □ General

Target State: NOOP

4. On the next screen, specify a Destination Directory for the xFlash executable on the target system. Click the “Files” button to continue:



Edit - Retail Store Install Package

Windows Settings:

Please setup destination directory, select files to distribute, enter executable commands, and select post distribution actions for Windows.

Destination Directory: C:\downloads\xflash

Select files to distribute

Executable Commands:

Post Distribution Action:

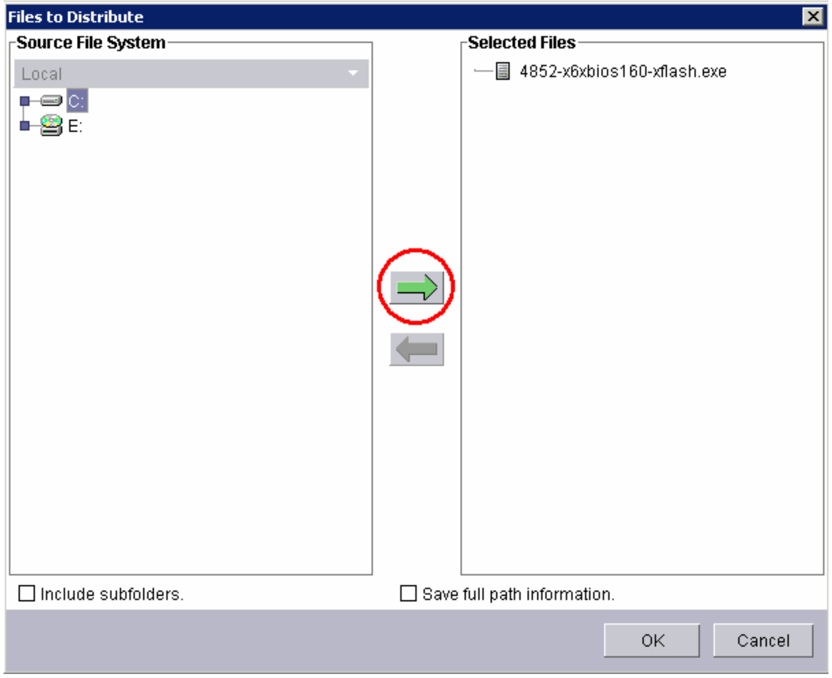
○ Do Nothing

● Restart Computer

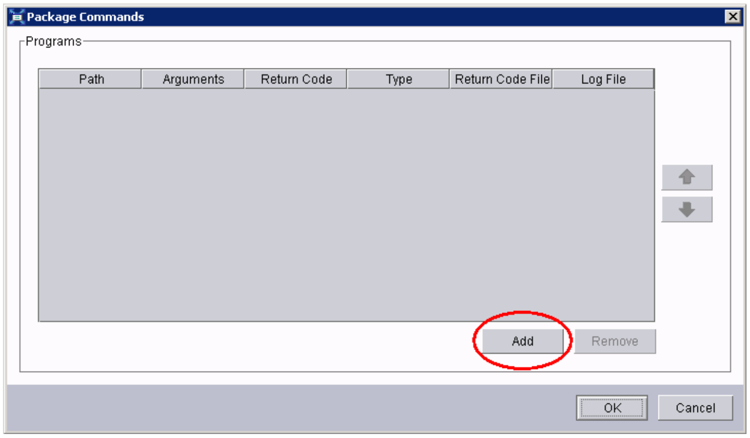
○ Restart Computer with Return File

Ready

5. In the “Files to Distribute” screen, find the downloaded xFlash executable on the “Source File System”, and click the green arrow to move it to the “Selected Files” list. Click “OK” to continue:



6. Back on the “Windows Settings” screen, click on the “Commands” button to add commands to the package. Inside the “Package Commands” screen, click on the “Add” button to add the first command:



7. The first command needed is to stop the POS Sensor Driver service from running on the target system. To stop the POS Sensor Driver service you will need to enter one of the following two commands based on if the system has a service processor.

   If the system has a service processor then enter the following command syntax:

“**cmd.exe /c net stop IPSDWSPSvc**”.

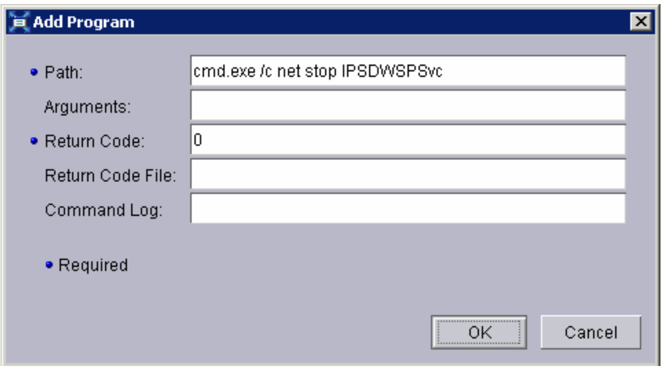
If the system does not have a service processor then enter the following command syntax: “**cmd.exe /c net stop IPSDWSvc**”.

The download link for the two sensor drivers explains which systems have the service processors and which systems do not:

IBM POS Sensor Drivers for Systems With Service Processors: http://www-01.ibm.com/support/docview.wss?rs=219&context=SW880&context=HW196&q1=pos+sensor&uid=pos1R4000167&loc=en_US&cs=utf-8&lang=en

IBM POS Sensor Drivers for Systems Without Service Processors: http://www-01.ibm.com/support/docview.wss?rs=219&context=SW880&context=HW196&q1=pos+sensor&uid=pos1R4000247&loc=en_US&cs=utf-8&lang=en

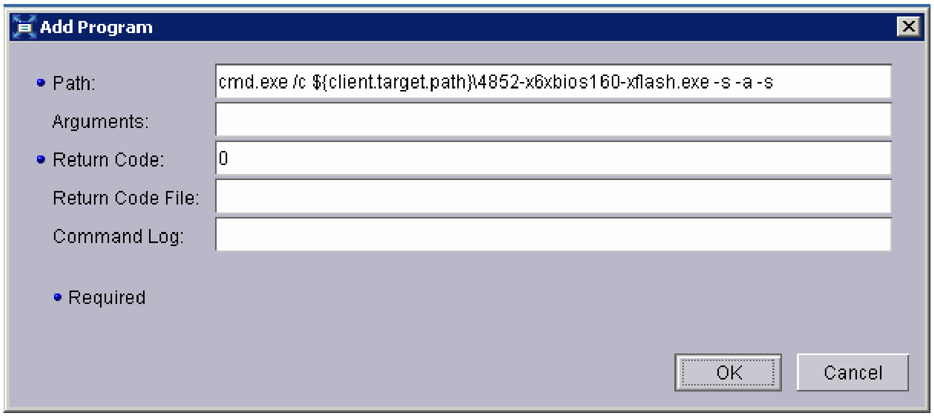
Click “OK” to continue:



• Path:	cmd.exe /c net stop IPSDWSPSvc
Arguments:	
• Return Code:	0
Return Code File:	
Command Log:	

Note: This command is not needed if the POS Sensor Drivers are not installed on the target system that will be getting the xFlash BIOS Update.

8. Click the “Add” button on the “Package Commands” screen to add a second command to the package. The second command will execute the xFlash BIOS Utility with the correct parameters to run the utility silently. To do so, enter the following: “**cmd.exe /c ${client.target.path}\4852-x6xbios160-xflash.exe –s –a –s**”. Click “OK” to continue:

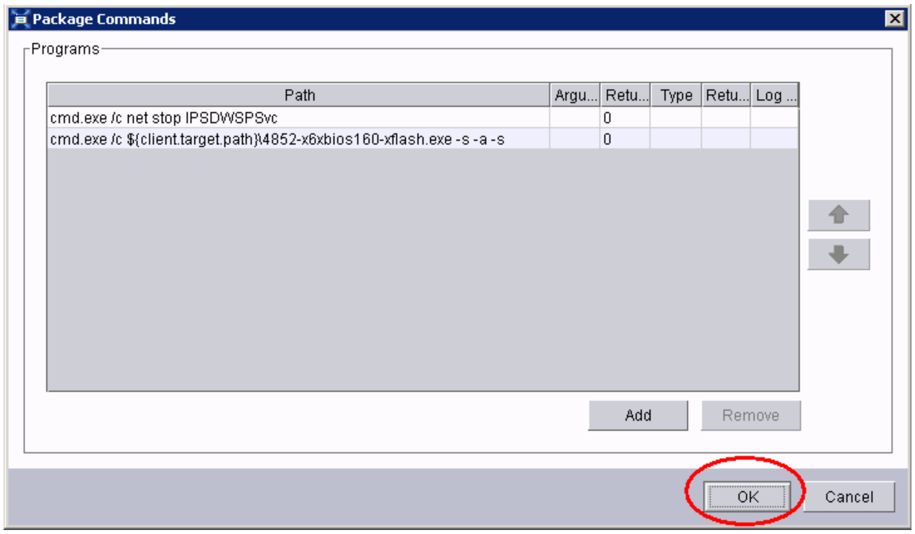


- Path: cmd.exe /c ${client.target.path}\4852-x6xbios160-xflash.exe -s -a -s
- Arguments:
- Return Code: 0
- Return Code File:
- Command Log:

● Required

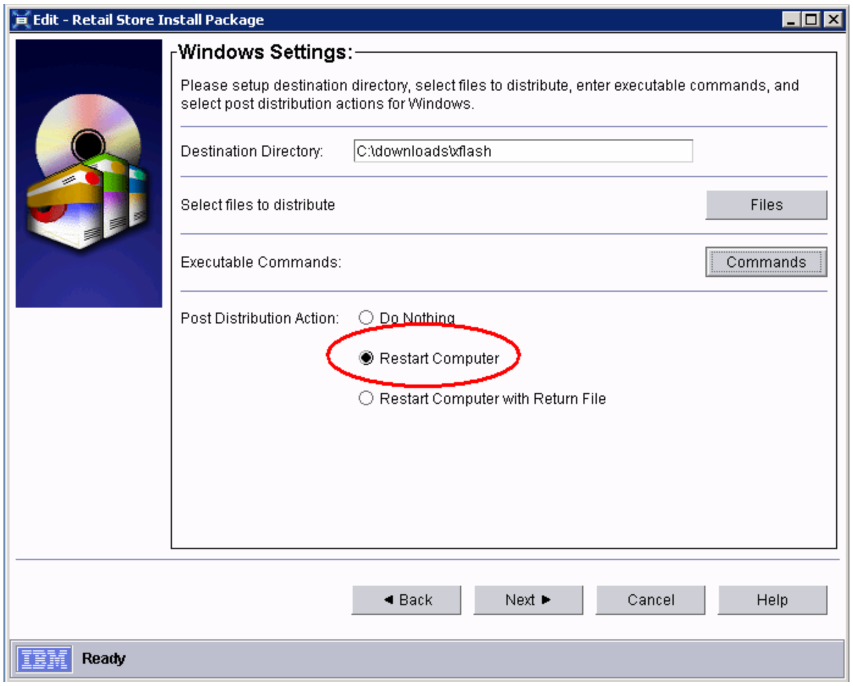
Note: The ${client.target.path} substitution variable will automatically substitute the destination directory that you specified when creating the package. Also note that the xFlash executable name will be different pending on the system type and BIOS level that is being applied. The "–s –a –s" parameters will always be required.

9. The completed "Package Commands" screen should look like the following. Click the "OK" button to continue:



Path	Argu...	Retu...	Type	Retu...	Log ...
cmd.exe /c net stop IPSDWSPSvc		0			
cmd.exe /c ${client.target.path}\4852-x6xbios160-xflash.exe -s -a -s		0			

10. Back on the "Windows Settings" page, ensure that "Restart Computer" is selected in the "Post Distribution Action" section and click "Next" to continue. On the last page, click "Finish" to build the package:



Windows Settings:

Please setup destination directory, select files to distribute, enter executable commands, and select post distribution actions for Windows.

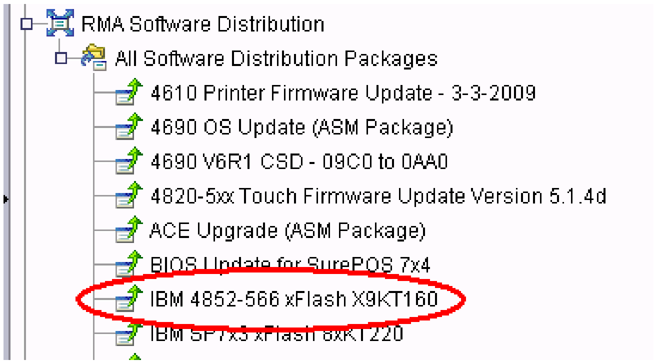
Destination Directory: C:\downloads\xflash

Select files to distribute

Executable Commands:

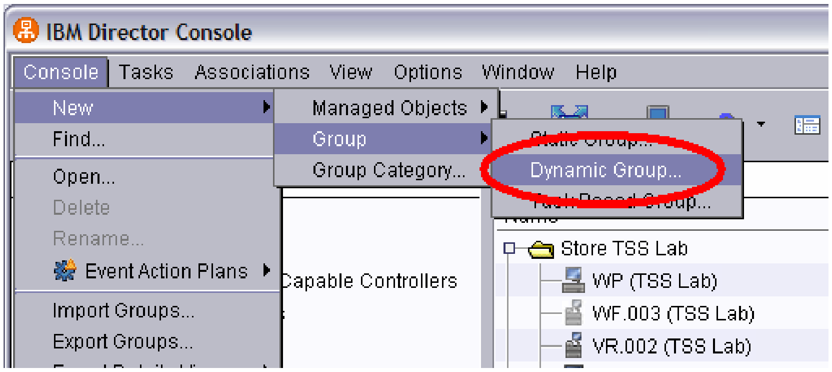
Post Distribution Action:
○ Do Nothing
● Restart Computer
○ Restart Computer with Return File

11. When finished, the BIOS Update package will appear under the “RMA Software Distribution” task on the IBM Director Console. From there, you can drag and drop to apply the package to a single system, multiple systems, or a group of systems.

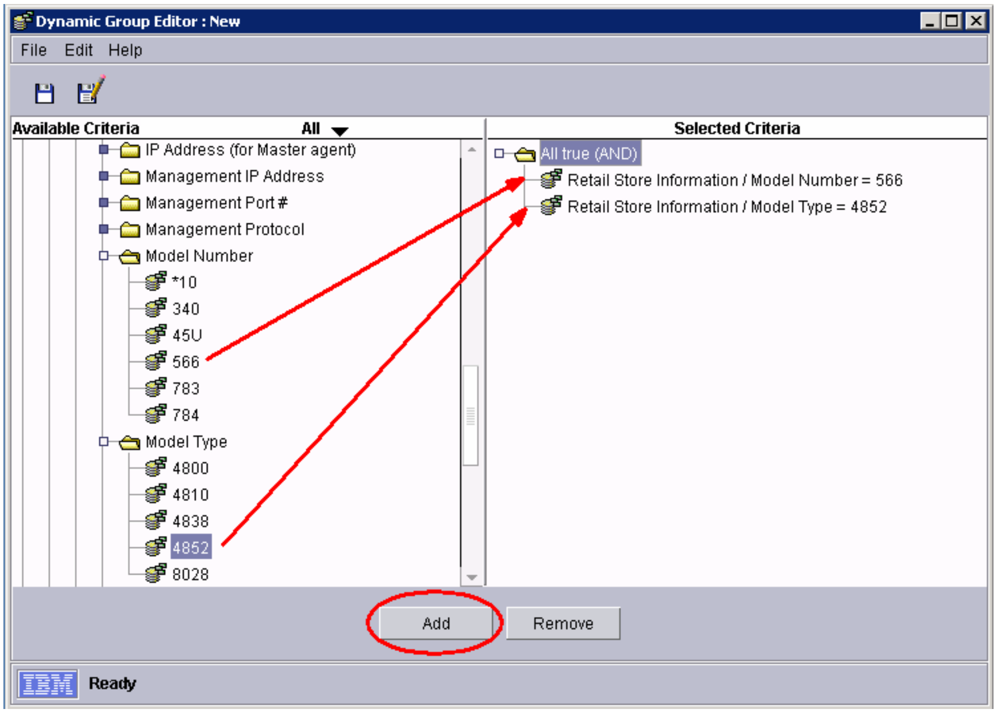


RMA Software Distribution
- All Software Distribution Packages
  - 4610 Printer Firmware Update - 3-3-2009
  - 4690 OS Update (ASM Package)
  - 4690 V6R1 CSD - 09C0 to 0AA0
  - 4820-5xx Touch Firmware Update Version 5.1.4d
  - ACE Upgrade (ASM Package)
  - BIOS Update for SurePOS 7x4
  - IBM 4852-566 xFlash X9KT160
  - IBM SP7x3 xFlash 8xKT220

12. The next set of steps are optional steps that will show you how to create a “Dynamic Group” of systems that need the BIOS Update Package. This example is assuming the system in question is an IBM SurePOS 500, 4852-566. To start, select “Console / New / Group / Dynamic Group” from the console’s main menu.

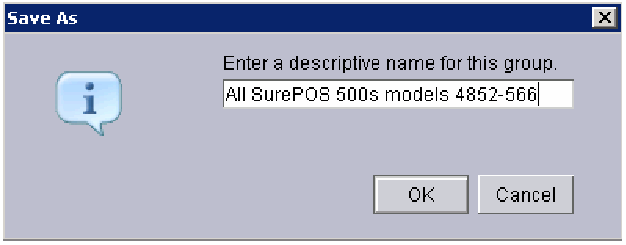


13. Expand the available criteria to "Hardware / Settings / Retail Store Information / Model Type", and select the "4852" entry. Either drag and drop or click "Add" to move it to the selected criteria on the right. Repeat the same with the "566" entry under "Hardware / Settings / Retail Store Information / Model Type". Select "All True (AND)" on the popup that gets displayed:



All true (AND)
Retail Store Information / Model Number = 566
Retail Store Information / Model Type = 4852

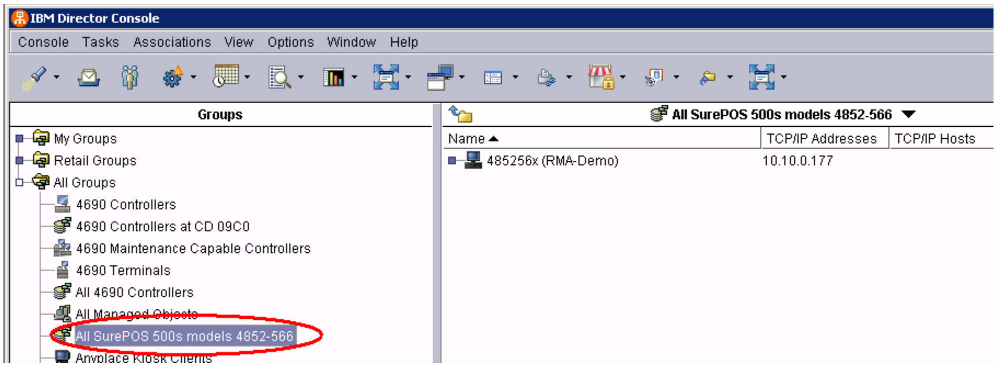
14. Click "Save As" and give the group a descriptive name. Click "OK" to create the group:



Enter a descriptive name for this group.

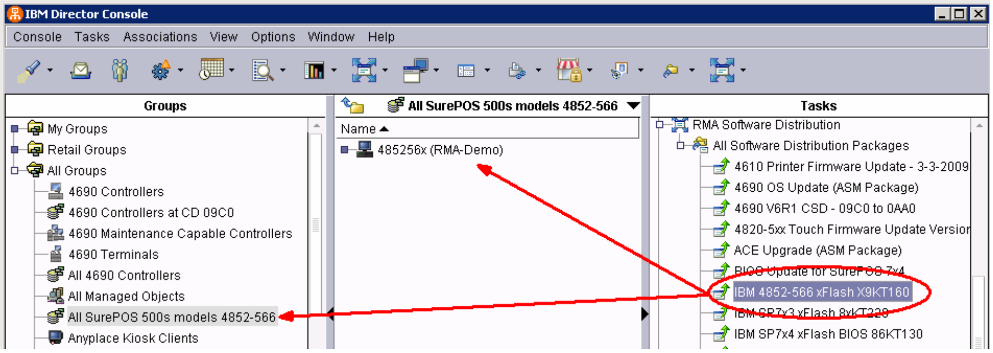
All SurePOS 500s models 4852-566

15. The group will now appear on the IBM Director Console under the “All Groups” section. You can click on the group to verify that it displays all of your SurePOS 500, 4852-566 systems:

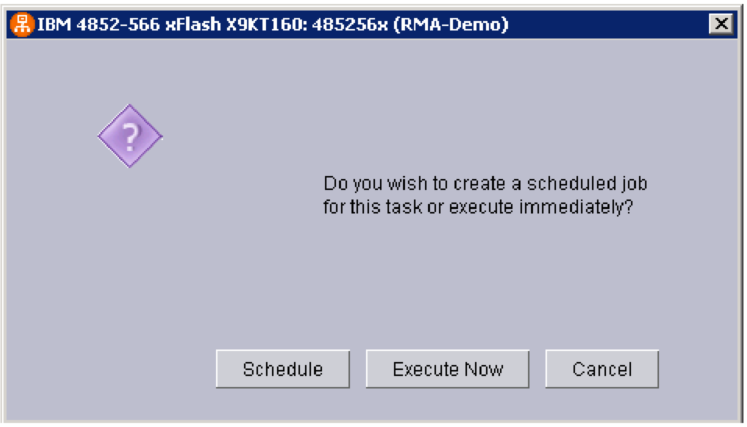

IBM Director Console
Console Tasks Associations View Options Window Help
Groups
My Groups
Retail Groups
All Groups
4690 Controllers
4690 Controllers at CD 09C0
4690 Maintenance Capable Controllers
4690 Terminals
All 4690 Controllers
All Managed Objects
All SurePOS 500s models 4852-566
Anyplace Kiosk Clients
All SurePOS 500s models 4852-566

Name	TCP/IP Addresses	TCP/IP Hosts
485256x (RMA-Demo)	10.10.0.177	

16. Now, to apply the BIOS update package, you can either drag and drop to apply the package to ALL of the systems within the group, or a number of systems within the group:

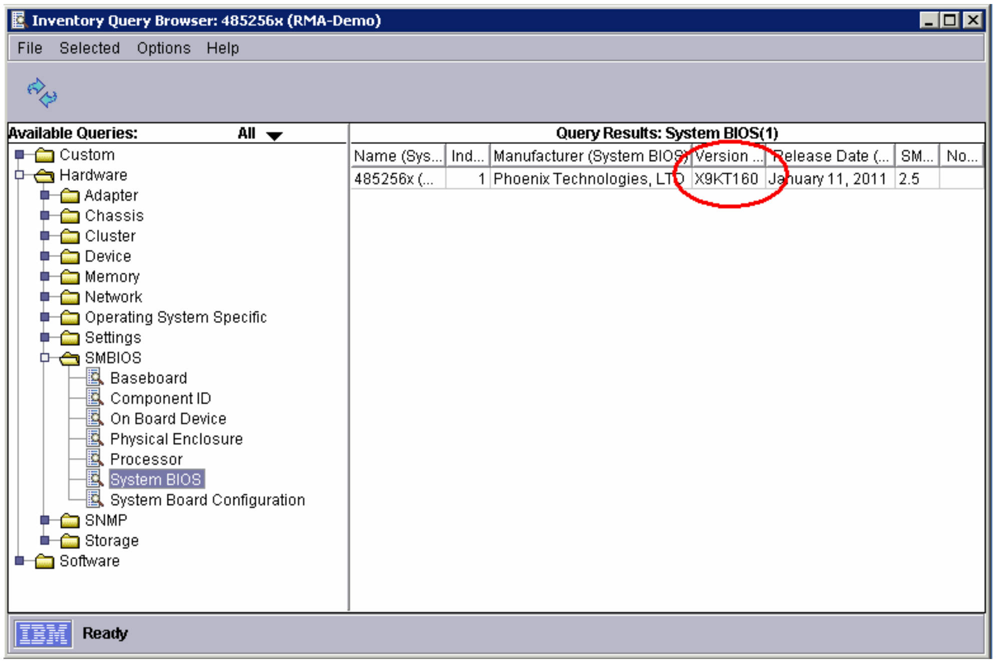

IBM Director Console
Console Tasks Associations View Options Window Help
Groups
My Groups
Retail Groups
All Groups
4690 Controllers
4690 Controllers at CD 09C0
4690 Maintenance Capable Controllers
4690 Terminals
All 4690 Controllers
All Managed Objects
All SurePOS 500s models 4852-566
Anyplace Kiosk Clients
All SurePOS 500s models 4852-566
Name
485256x (RMA-Demo)
Tasks
RMA Software Distribution
All Software Distribution Packages
4610 Printer Firmware Update - 3-3-2009
4690 OS Update (ASM Package)
4690 V6R1 CSD - 09C0 to 0AA0
4820-5xx Touch Firmware Update Versior
ACE Upgrade (ASM Package)
BIOS Update for SurePOS 7x4
IBM 4852-566 xFlash X9KT160
IBM SP7x3 xFlash 8xKT220
IBM SP7x4 xFlash BIOS 86KT130

17. After dragging and dropping, you will have the ability to “Execute Now” or “Schedule” the package for future deployment:



Do you wish to create a scheduled job for this task or execute immediately?

18. After the update finishes, you should re-collect Inventory on the systems units that received the update. Then you can verify that the new BIOS level is correct by looking at the "Hardware -> SMBIOS -> System BIOS" table:



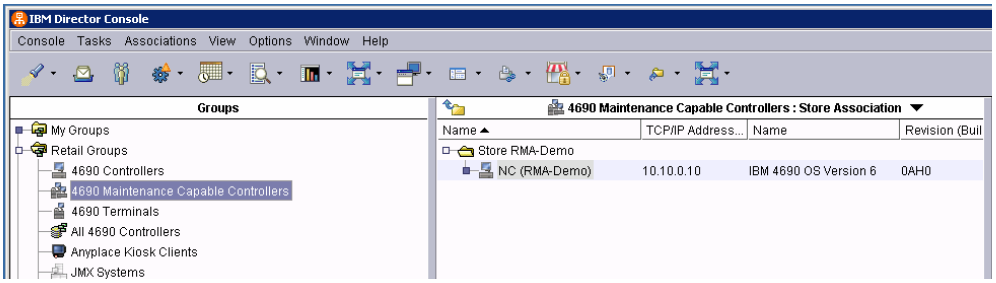
Query Results: System BIOS(1)

Name (Sys...	Ind...	Manufacturer (System BIOS)	Version ...	Release Date (...	SM...	No...
485256x (...	1	Phoenix Technologies, LTD	X9KT160	January 11, 2011	2.5	

RMA Software Distribution on 4690

RMA Software Distribution is supported on 4690 V6R1 and greater levels. It is similar to software distribution on Windows and Linux with two key differences.

The first is that software distribution to 4690 systems is only allowed on the Master Controller. To simplify that process, there is a pre-defined group for “4690 Maintenance Capable Controllers”. This group will only display the 4690 systems that are eligible for Software Distribution.



Groups

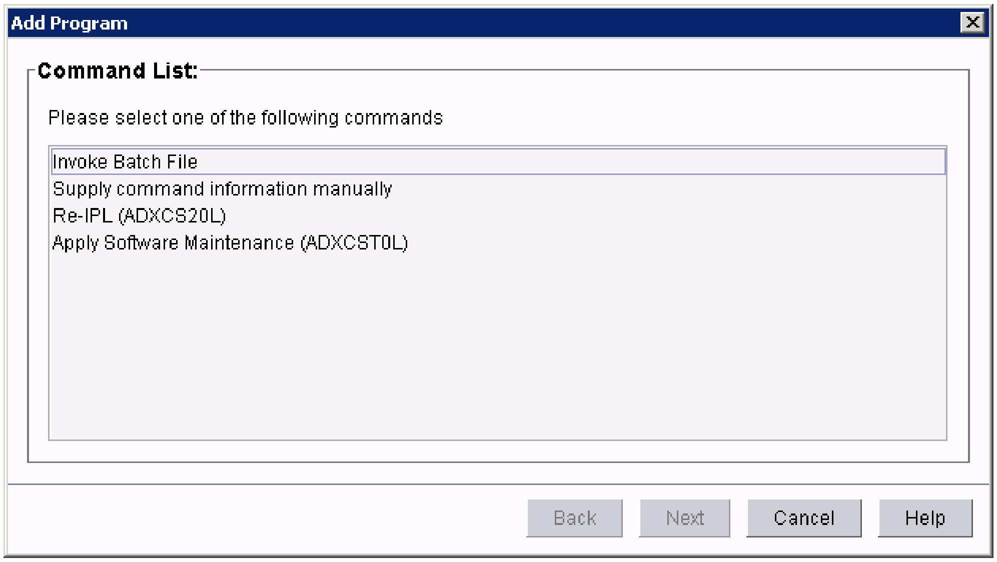
- My Groups
- Retail Groups
  - 4690 Controllers
  - 4690 Maintenance Capable Controllers
  - 4690 Terminals
  - All 4690 Controllers
  - Anyplace Kiosk Clients
  - JMX Systems

4690 Maintenance Capable Controllers : Store Association

Name ▲	TCP/IP Address...	Name	Revision (Buil
Store RMA-Demo			
NC (RMA-Demo)	10.10.0.10	IBM 4690 OS Version 6	0AH0

The second difference between 4690 and other operating systems are the options for adding commands to the Software Distribution package.

When you click on the “Commands” button for a 4690 package, it will display several command options specific to 4690:



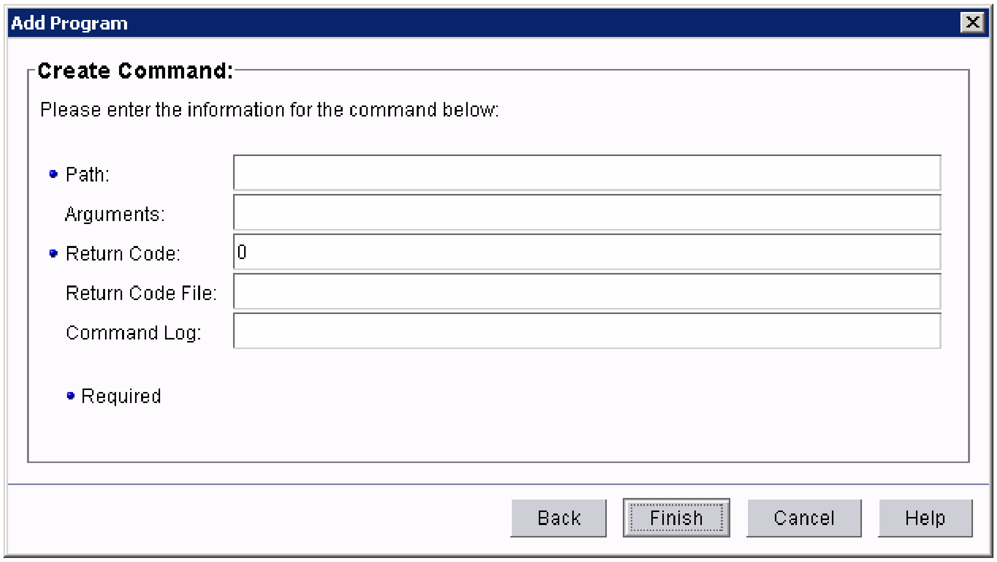
Command List:

Please select one of the following commands

Invoke Batch File
Supply command information manually
Re-IPL (ADXCS20L)
Apply Software Maintenance (ADXCST0L)

The “Supply Command Information Manually” option launches a command window very similar to the dialog launched for Windows. It allows you to specify the path to the command you want to run, arguments for that command, the expected return code, and optionally a return code file or command log.

RMA uses RCP as its means to run commands on 4690, so any RCP commands available on 4690 may be entered in this dialog.



Add Program

Create Command:

Please enter the information for the command below:

● Path:

Arguments:

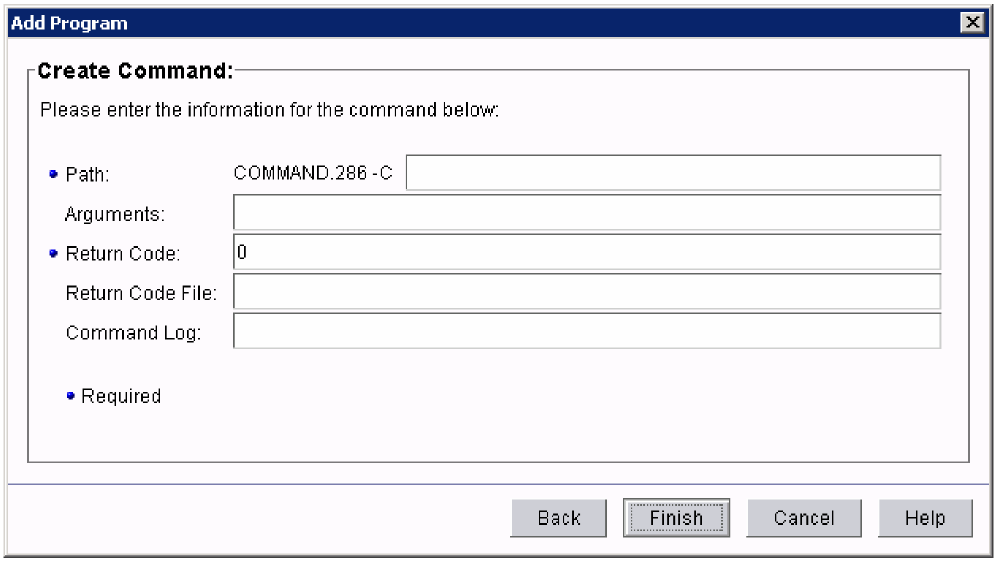
● Return Code: 0

Return Code File:

Command Log:

● Required

The “Invoke Batch File” option also launches a similar window, but prepends the path with “COMMAND.286 –C” to ensure the command is issued from a command window on the 4690 controller. You would use this to execute batch files or commands that are available on the 4690 file system, but not standard RCP commands.



Add Program

Create Command:

Please enter the information for the command below:

● Path: COMMAND.286 -C

Arguments:

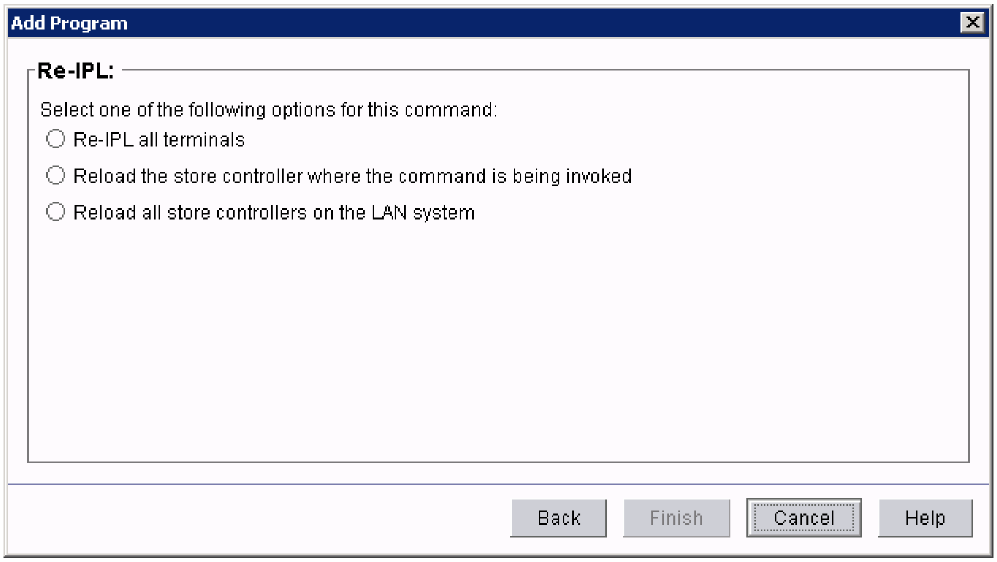
● Return Code: 0

Return Code File:

Command Log:

● Required

The “Re-IPL (ADXCS20L)” option generates a command string to issue the ADXCS20L command on a 4690 controller. The options displayed let you specify the arguments for Re-IPL command:



Re-IPL:

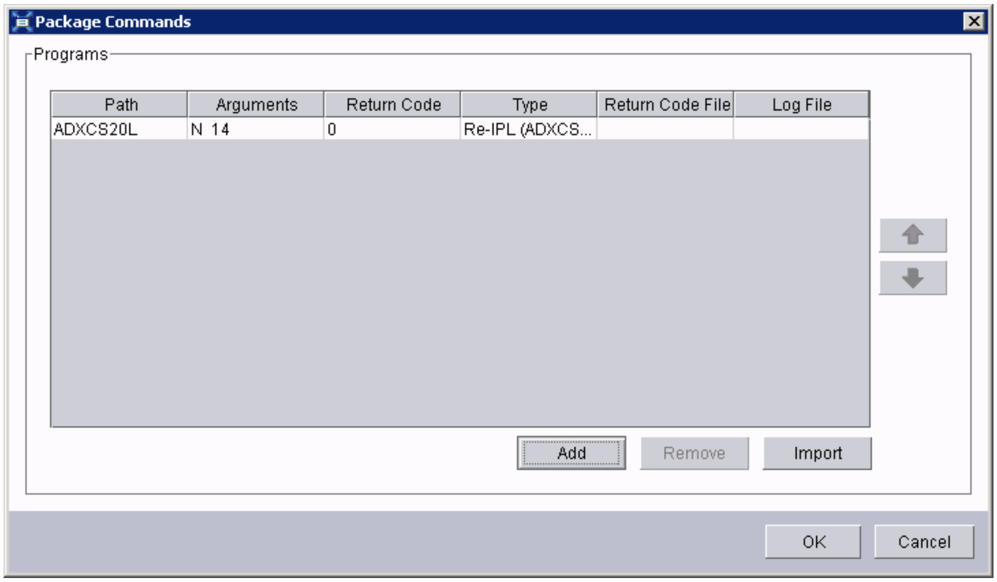
Select one of the following options for this command:

○ Re-IPL all terminals

○ Reload the store controller where the command is being invoked

○ Reload all store controllers on the LAN system

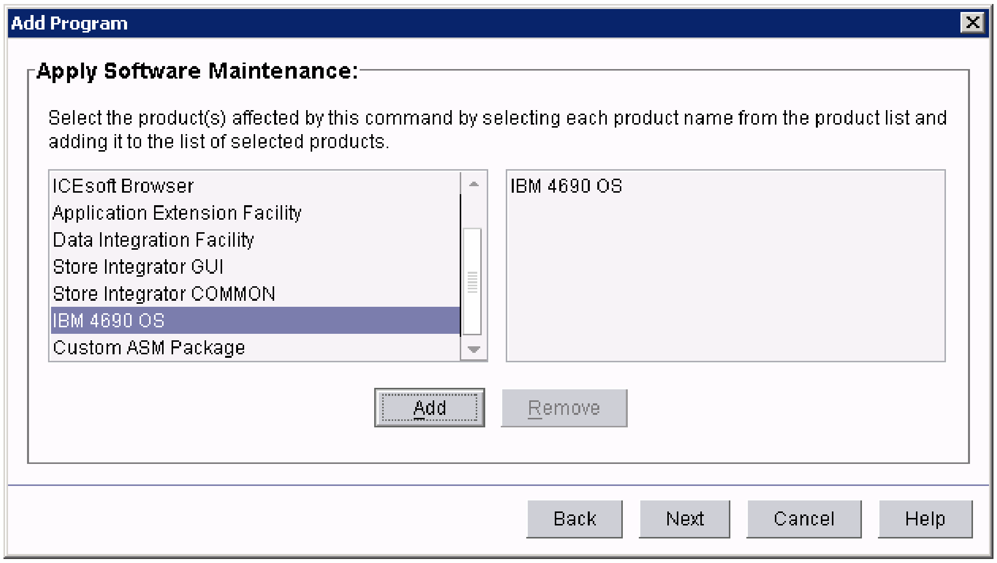
When finished, the wizard will generate the ADXCS20L command with the proper arguments based on what you selected:



Path	Arguments	Return Code	Type	Return Code File	Log File
ADXCS20L	N 14	0	Re-IPL (ADXCS...		

The “Apply Software Maintenance (ADXCST0L) option is what is used to issue ASM commands on 4690. The wizard will prompt you for all of the information necessary to issue the ADXCST0L command as desired.

The first screen allows you to select which ASM products you would like to work with. The available list of products is pre-populated with the known products within RSS:



Add Program

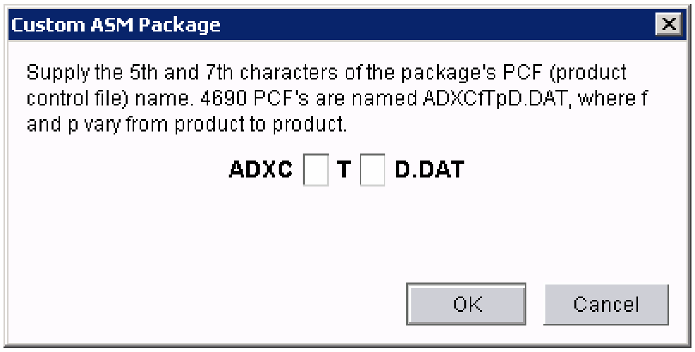
Apply Software Maintenance:

Select the product(s) affected by this command by selecting each product name from the product list and adding it to the list of selected products.

- ICEsoft Browser
- Application Extension Facility
- Data Integration Facility
- Store Integrator GUI
- Store Integrator COMMON
- IBM 4690 OS
- Custom ASM Package

IBM 4690 OS

If you have a custom built package with a unique product control file, then simply select the “Custom ASM Package” option. This will allow you to enter the unique characters to represent that product control file:

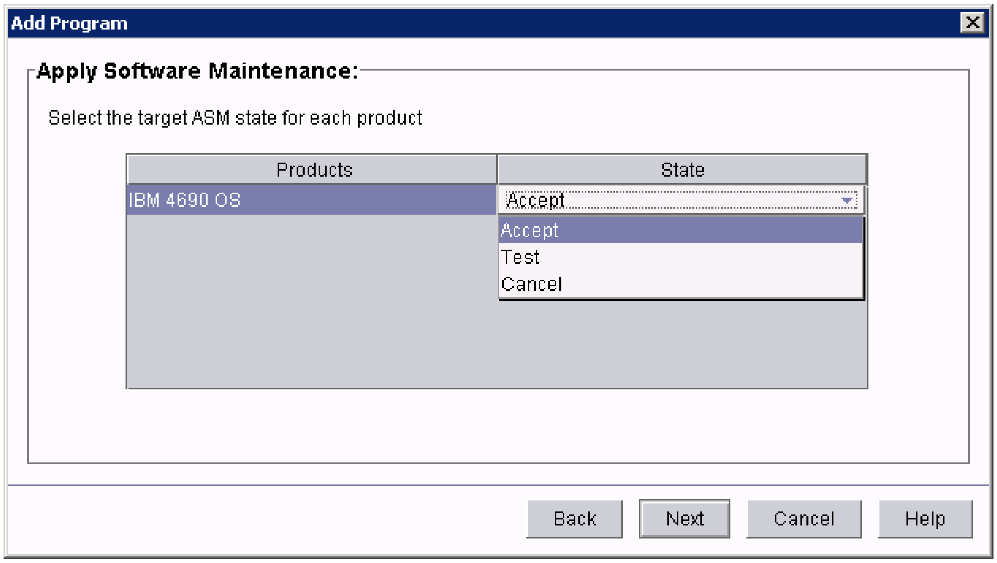


Custom ASM Package

Supply the 5th and 7th characters of the package's PCF (product control file) name. 4690 PCF's are named ADXCfTpD.DAT, where f and p vary from product to product.

ADXC □ T □ D.DAT

The next screen will display each of the products that you selected along with a drop box for the desired ASM package state. When the RMA Software Distribution Package is executed, it will attempt to move the ASM package to the state that is selected (Accept, Test, or Cancel):



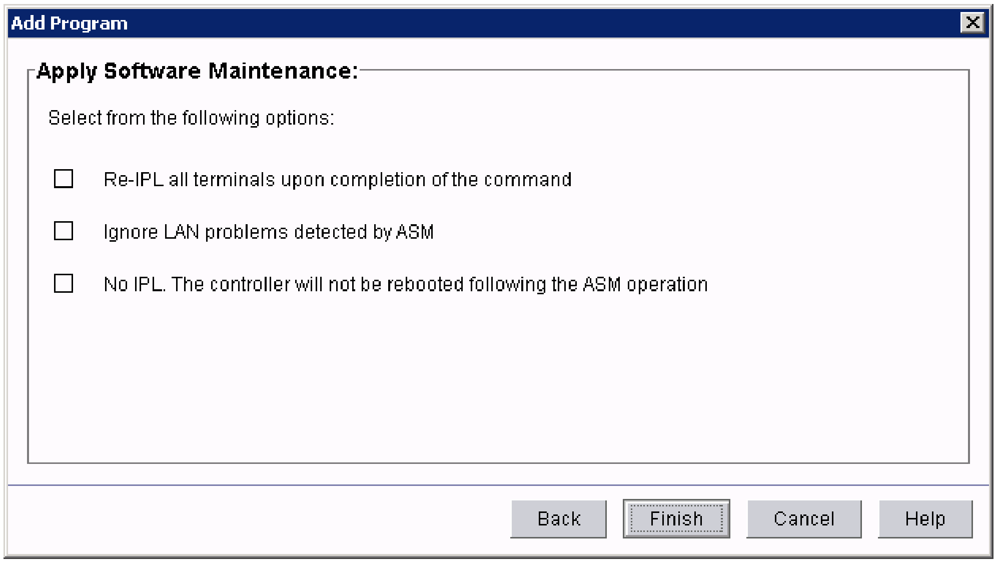
Add Program

Apply Software Maintenance:

Select the target ASM state for each product

Products	State
IBM 4690 OS	Accept

Finally, the last screen lists all of the options available when issuing the ASM update command:



Add Program

Apply Software Maintenance:

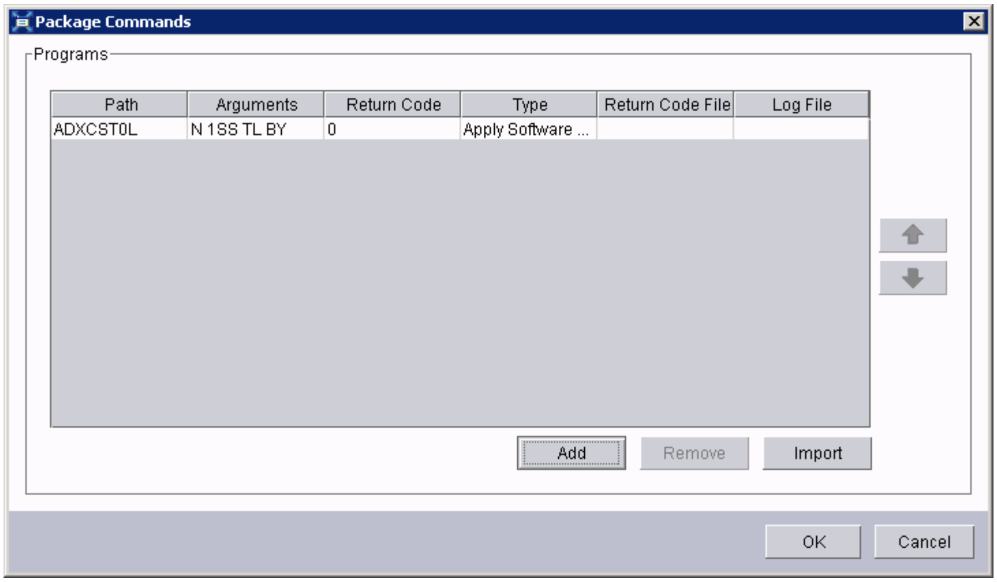
Select from the following options:

□ Re-IPL all terminals upon completion of the command

□ Ignore LAN problems detected by ASM

□ No IPL. The controller will not be rebooted following the ASM operation

When you click “Finish”, the command string for your ASM package will be built along with the options specified:



Path	Arguments	Return Code	Type	Return Code File	Log File
ADXCST0L	N 1SS TL BY	0	Apply Software ...		

Please refer to the 4690 publications for more detail about the available RCP commands and their options.

Example: Upgrading 4690 Levels Using RMA Software Distribution

Using RMA Software Distribution to upgrade 4690 Levels is very similar to the standard RCP process that you would use to do the same. This example will walk you through all of the steps necessary to:

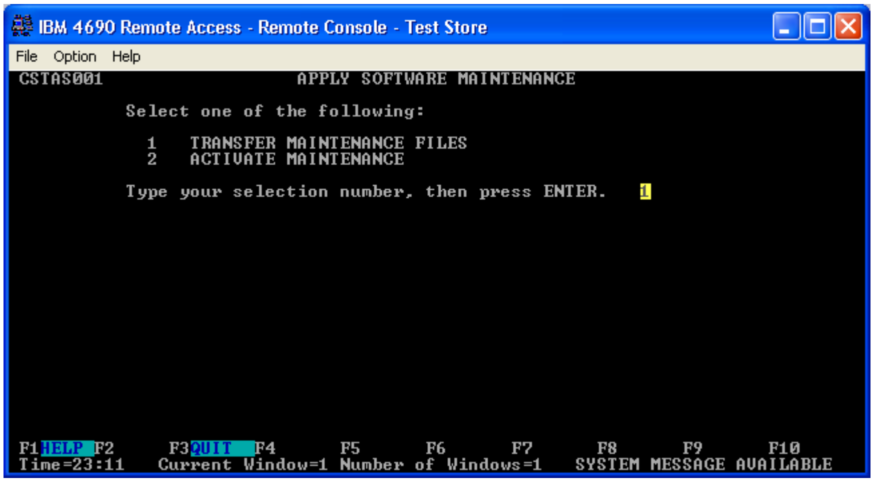
- Prepare the files needed for the upgrade
- Build a software distribution package for the upgrade
- Target the systems for the upgrade
- Deploy the upgrade to the targeted systems

> **Note:** Please refer to the 4690 User's Guide for more detail on the upgrade process while using RCP

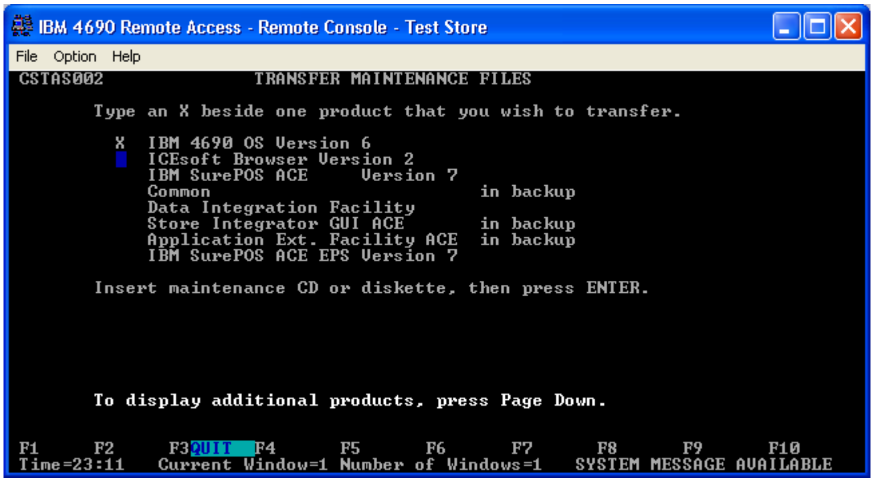
Preparing the Files Needed for a 4690 Upgrade

1. Use the ASM process to transfer the maintenance for the OS update on a master controller at your host site:

   > **Note:** The update package files **must** be generated on a system that is at the same OS level as the system that will be receiving the update in the field.

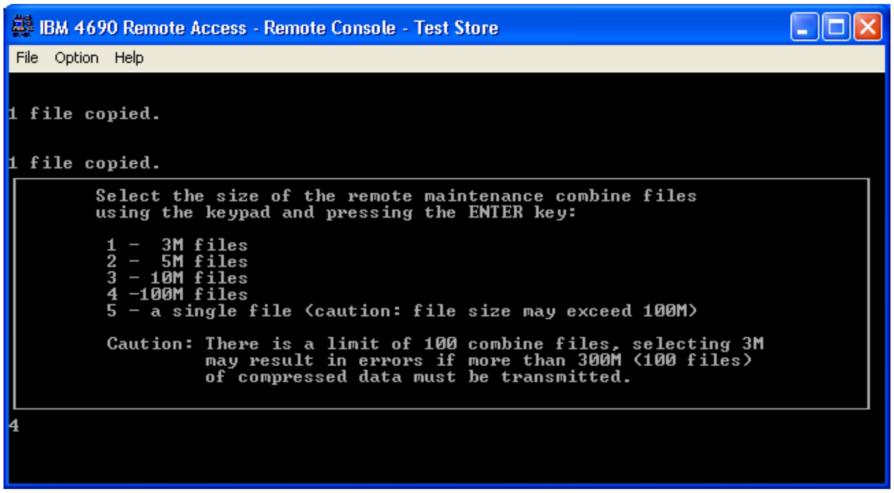


```
CSTAS001                    APPLY SOFTWARE MAINTENANCE

           Select one of the following:

             1   TRANSFER MAINTENANCE FILES
             2   ACTIVATE MAINTENANCE

           Type your selection number, then press ENTER.    1

F1HELP  F2      F3QUIT  F4      F5      F6      F7      F8      F9      F10
Time=23:11   Current Window=1 Number of Windows=1   SYSTEM MESSAGE AVAILABLE
```



```
CSTAS002                TRANSFER MAINTENANCE FILES

        Type an X beside one product that you wish to transfer.

          X  IBM 4690 OS Version 6
             ICEsoft Browser Version 2
             IBM SurePOS ACE     Version 7
             Common                         in backup
             Data Integration Facility
             Store Integrator GUI ACE       in backup
             Application Ext. Facility ACE  in backup
             IBM SurePOS ACE EPS Version 7

        Insert maintenance CD or diskette, then press ENTER.



        To display additional products, press Page Down.

F1      F2      F3QUIT  F4      F5      F6      F7      F8      F9      F10
Time=23:11   Current Window=1 Number of Windows=1   SYSTEM MESSAGE AVAILABLE
```

2. Without activating the maintenance, open a command window and run the ASMBUNDL command from the ADX_SMNT directory. Select the desired file size for the bundle files and wait for the command to complete:

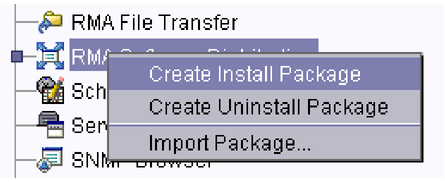


```
1 file copied.

1 file copied.
        Select the size of the remote maintenance combine files
        using the keypad and pressing the ENTER key:

         1 -  3M files
         2 -  5M files
         3 - 10M files
         4 -100M files
         5 - a single file (caution: file size may exceed 100M)

         Caution: There is a limit of 100 combine files, selecting 3M
                  may result in errors if more than 300M (100 files)
                  of compressed data must be transmitted.

4
```

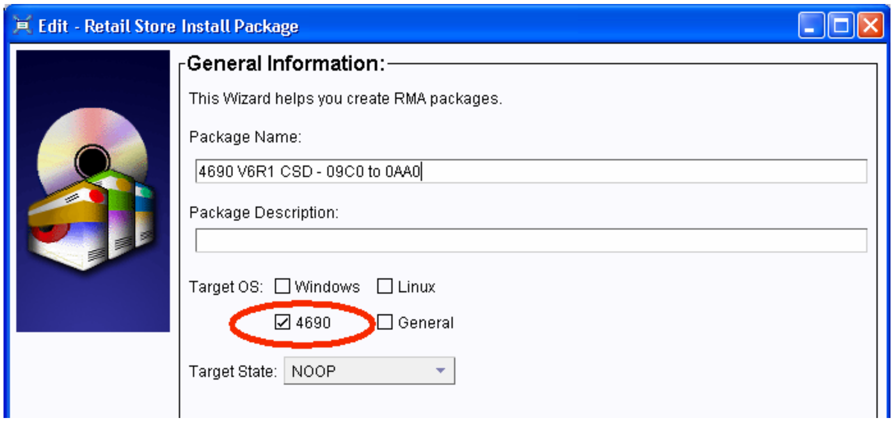
3. After the ASMBUNDL command completes, transfer all of the completed bundle files from your Master Controller to your IBM Director Server system. The following files should be transferred:
    - c:\adx_smnt\adxhj??f.dat (i.e. the bundle files)
    - c:\adx_smnt\adxhjlcl.286
    - c:\adx_smnt\adxnsxzl.286

Building the RMA Software Distribution Package for the Upgrade

1. On the IBM Director Console, right click on the “RMA Software Distribution” task and select “Create Install Package”:



2. Give your package a descriptive name and check “4690” for the target OS:



Edit - Retail Store Install Package

General Information:

This Wizard helps you create RMA packages.

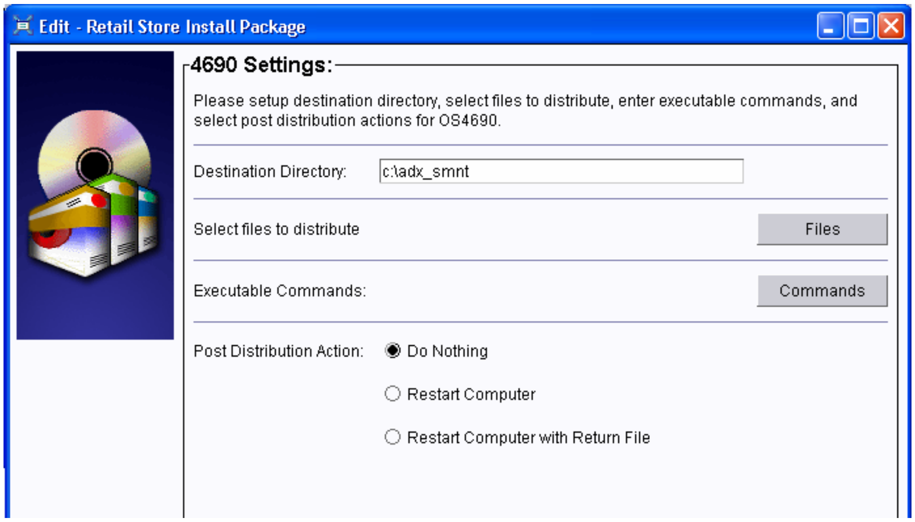
Package Name: 4690 V6R1 CSD - 09C0 to 0AA0

Package Description:

Target OS: □ Windows □ Linux ☑ 4690 □ General

Target State: NOOP

3. Enter “c:\adx_smnt” for the destination directory:



Edit - Retail Store Install Package

4690 Settings:

Please setup destination directory, select files to distribute, enter executable commands, and select post distribution actions for OS4690.

Destination Directory: c:\adx_smnt

Select files to distribute

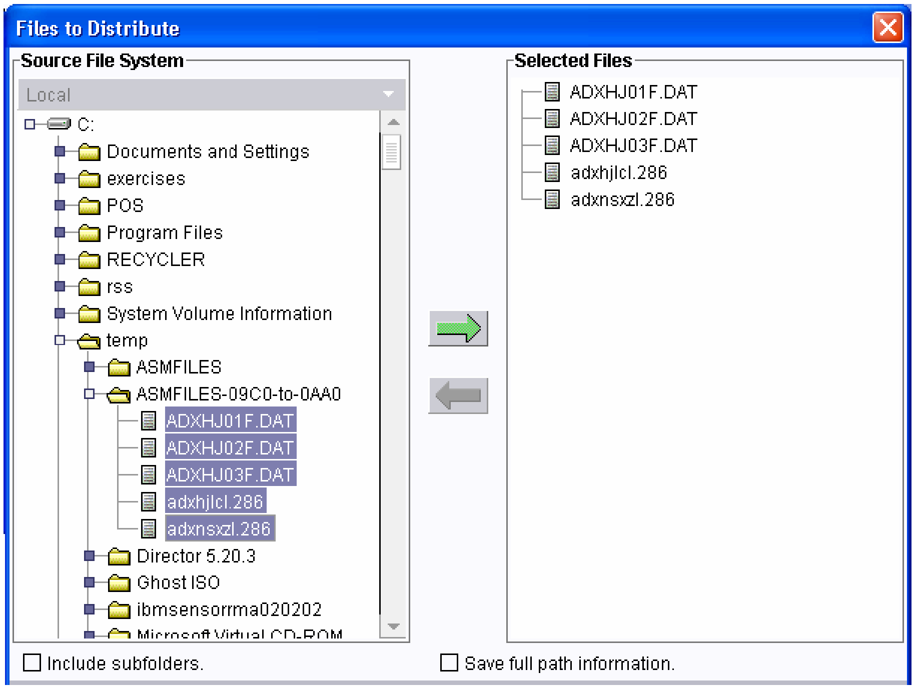
Executable Commands:

Post Distribution Action: ● Do Nothing

○ Restart Computer

○ Restart Computer with Return File

4. Click the “Files” button, and add the transferred DAT files and the 286 files to the package. Click “OK” when finished:



Files to Distribute

Source File System

Local

- C:
  - Documents and Settings
  - exercises
  - POS
  - Program Files
  - RECYCLER
  - rss
  - System Volume Information
  - temp
    - ASMFILES
    - ASMFILES-09C0-to-0AA0
      - ADXHJ01F.DAT
      - ADXHJ02F.DAT
      - ADXHJ03F.DAT
      - adxhjlcl.286
      - adxnsxzl.286
    - Director 5.20.3
    - Ghost ISO
    - ibmsensorrma020202
    - Microsoft Virtual CD-ROM

Selected Files

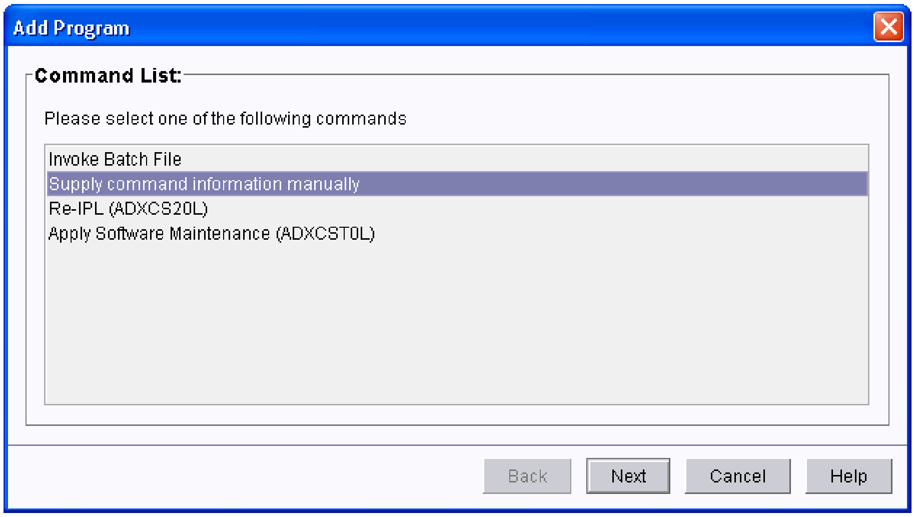
- ADXHJ01F.DAT
- ADXHJ02F.DAT
- ADXHJ03F.DAT
- adxhjlcl.286
- adxnsxzl.286

□ Include subfolders.

□ Save full path information.

5. Click on the “Commands” button to bring up the command list for this package.

6. The first command needed will be to un-bundle the bundle files created by the ASMBUNDL process. To add this command, click the “Add” button and select “Supply Command Information Manually”:



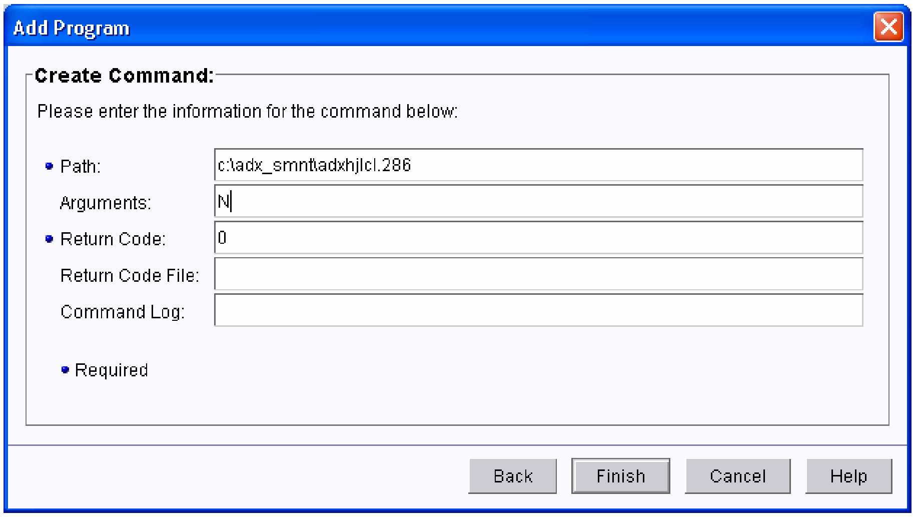
Add Program

Command List:

Please select one of the following commands

Invoke Batch File
Supply command information manually
Re-IPL (ADXCS20L)
Apply Software Maintenance (ADXCST0L)

7. On the next screen, add the adx_smnt\adxhjlcl.286 command with the N argument as shown below. Click "Finish" when completed:



Add Program

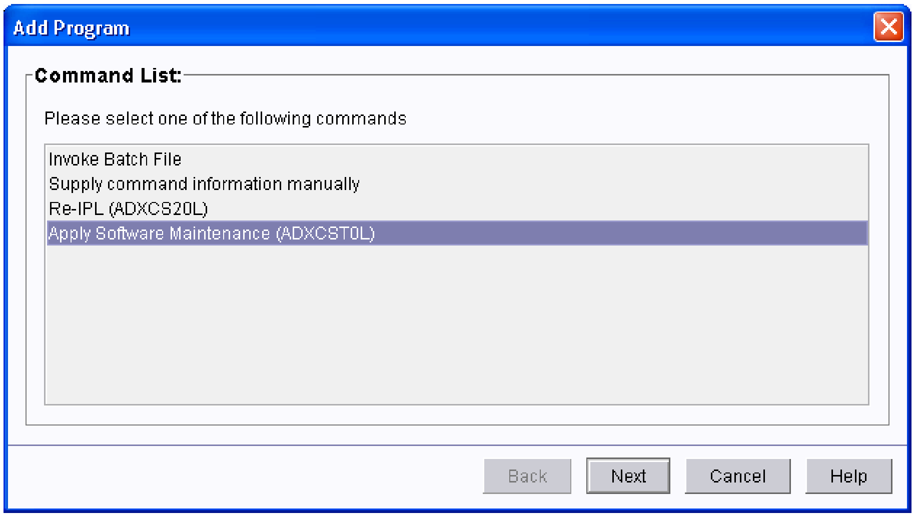
Create Command:

Please enter the information for the command below:

- Path: c:\adx_smnt\adxhjlcl.286
- Arguments: N
- Return Code: 0
- Return Code File:
- Command Log:

Required

8. The second command needed for the package will be the ASM command to move the maintenance level into either the "Test" or "Accept" state. To add the ASM command, click the "Add" button and select "Apply Software Maintenance (ADXCST0L)". Click "Next" to continue:



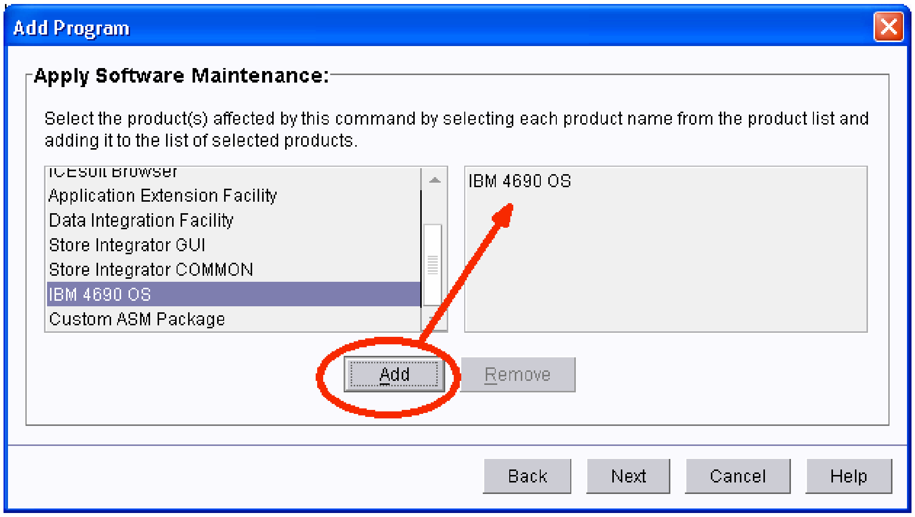
Add Program

Command List:

Please select one of the following commands

Invoke Batch File
Supply command information manually
Re-IPL (ADXCS20L)
Apply Software Maintenance (ADXCST0L)

9. Select “IBM 4690 OS” from the list of ASM packages and click “Add” to add it to the selected package list. Click “Next” to continue:



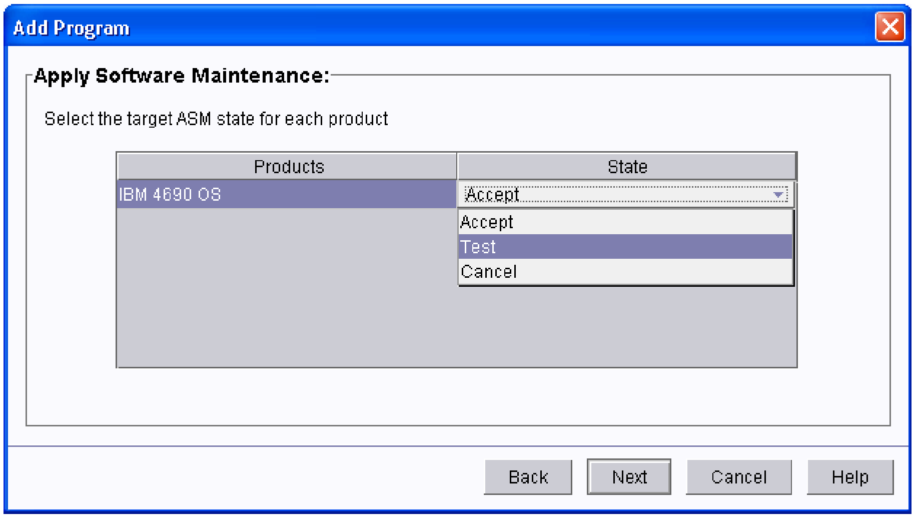
Apply Software Maintenance:

Select the product(s) affected by this command by selecting each product name from the product list and adding it to the list of selected products.

- ICESoft Browser
- Application Extension Facility
- Data Integration Facility
- Store Integrator GUI
- Store Integrator COMMON
- IBM 4690 OS
- Custom ASM Package

IBM 4690 OS

10. On the next page, use the drop box to select the desired ASM package state after the upgrade (Test or Accept). Click “Next” to continue:

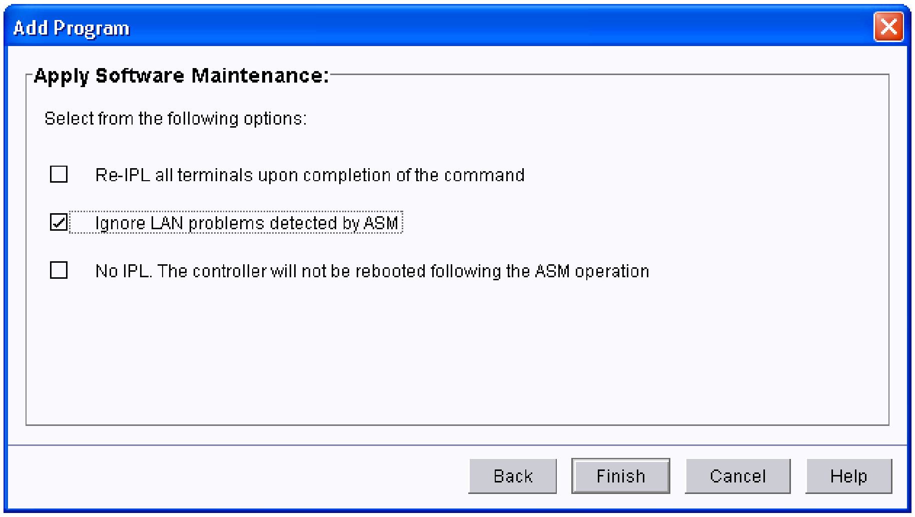


Apply Software Maintenance:

Select the target ASM state for each product

Products	State
IBM 4690 OS	Accept

11. Finally, decide if you want to apply and of the ASM options on the last screen and click “Finish” to add the command:



Apply Software Maintenance:

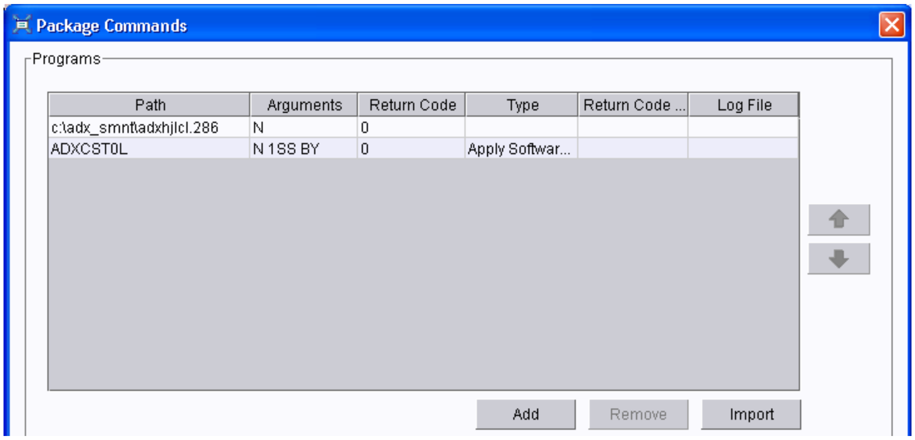
Select from the following options:

☐ Re-IPL all terminals upon completion of the command

☑ Ignore LAN problems detected by ASM

☐ No IPL. The controller will not be rebooted following the ASM operation

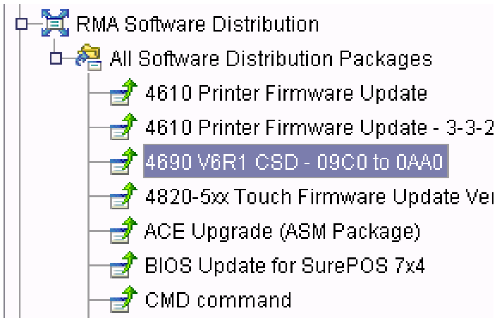
12. After verifying that your commands look correct, click the “OK” button to close the Package Commands Window.



Programs

Path	Arguments	Return Code	Type	Return Code ...	Log File
c:\adx_smnt\adxhjlcl.286	N	0			
ADXCST0L	N 1SS BY	0	Apply Softwar...		

13. Click “Next” and then “Finish” to build the RMA Software Distribution Package. When finished, the package should appear under the “RMA Software Distribution” task:



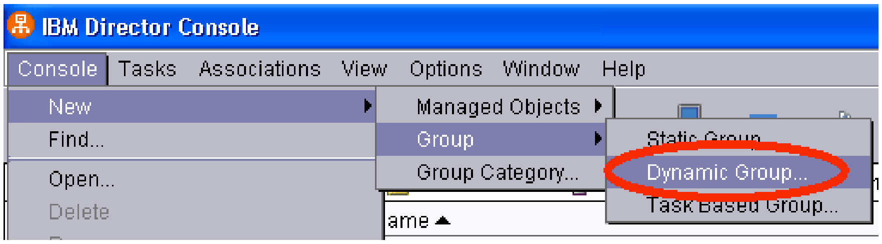
RMA Software Distribution
All Software Distribution Packages
4610 Printer Firmware Update
4610 Printer Firmware Update - 3-3-2
4690 V6R1 CSD - 09C0 to 0AA0
4820-5xx Touch Firmware Update Vei
ACE Upgrade (ASM Package)
BIOS Update for SurePOS 7x4
CMD command

Targeting the Systems for the Upgrade

To target the proper systems to deploy an upgrade to, it is recommended that you create a dynamic group showing all of the 4690 controllers that are at the level that needs to be upgraded (ie, 09C0).

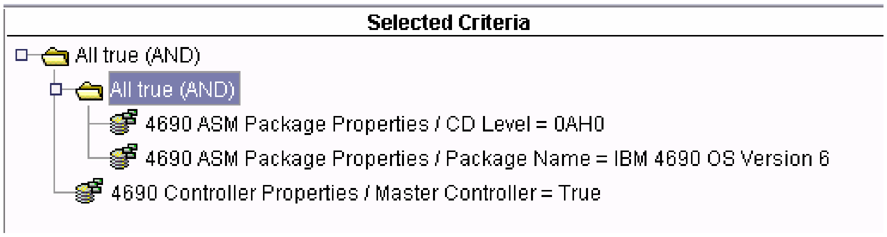
To create this group:

1. Right-click on the groups column on the IBM Director Console, or use the Menu tree to create a Dynamic group:



2. In the Dynamic Group Editor, add the following conditions:
   - Software -> 4690 ASM Package Properties -> Package Name -> IBM 4690 OS Version 6
   - Software -> 4690 ASM Package Properties -> CD Level -> ** 4690 Base level to be upgraded **
   - Hardware -> Settings -> 4690 Controller Properties -> Master Controller -> TRUE

   Make sure the conditions are set to “All true (AND)”. The final group tree should look something like:



Selected Criteria

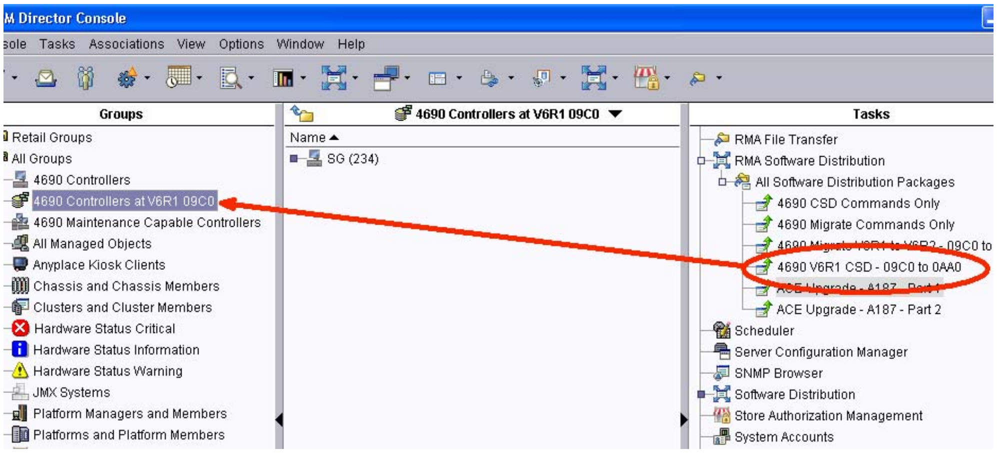
All true (AND)
- All true (AND)
  - 4690 ASM Package Properties / CD Level = 0AH0
  - 4690 ASM Package Properties / Package Name = IBM 4690 OS Version 6
- 4690 Controller Properties / Master Controller = True

3. Click “Save-As” and give a descriptive name for the group.

4. When finished, the group will appear under the “All Groups” section on the Director Console. Click on the group and verify it contains the systems you are looking for.

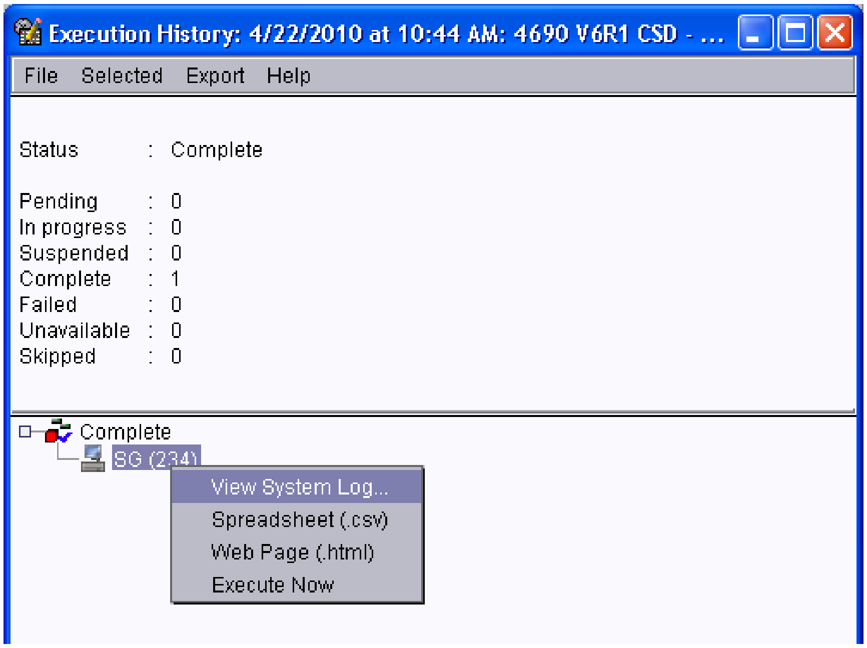
Deploying the Upgrade to the Targeted Systems

To deploy the upgrade to all of your stores, you simply have to drag and drop the package that was created to the dynamic group containing all of the systems as the required level.


M Director Console
sole Tasks Associations View Options Window Help
Groups
Retail Groups
All Groups
4690 Controllers
4690 Controllers at V6R1 09C0
4690 Maintenance Capable Controllers
All Managed Objects
Anyplace Kiosk Clients
Chassis and Chassis Members
Clusters and Cluster Members
Hardware Status Critical
Hardware Status Information
Hardware Status Warning
JMX Systems
Platform Managers and Members
Platforms and Platform Members
4690 Controllers at V6R1 09C0
Name
SG (234)
Tasks
RMA File Transfer
RMA Software Distribution
All Software Distribution Packages
4690 CSD Commands Only
4690 Migrate Commands Only
4690 Migrate V6R1 to V6R2 - 09C0 to
4690 V6R1 CSD - 09C0 to 0AA0
ACE Upgrade - A187 - Part 1
ACE Upgrade - A187 - Part 2
Scheduler
Server Configuration Manager
SNMP Browser
Software Distribution
Store Authorization Management
System Accounts

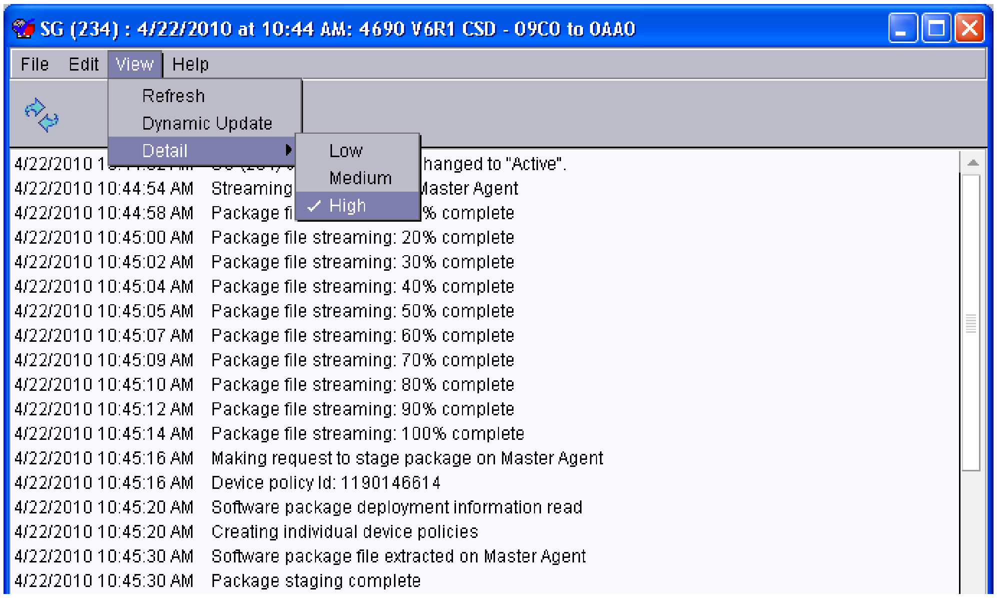
As the package is running, the Execution History will show you the status of the systems as they are running the upgrade.

To view detailed logs for any system, right-click and select “View System Log”



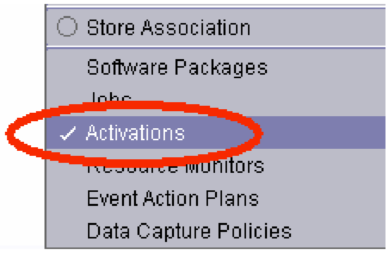
```
Status       :  Complete

Pending      :  0
In progress  :  0
Suspended    :  0
Complete     :  1
Failed       :  0
Unavailable  :  0
Skipped      :  0
```

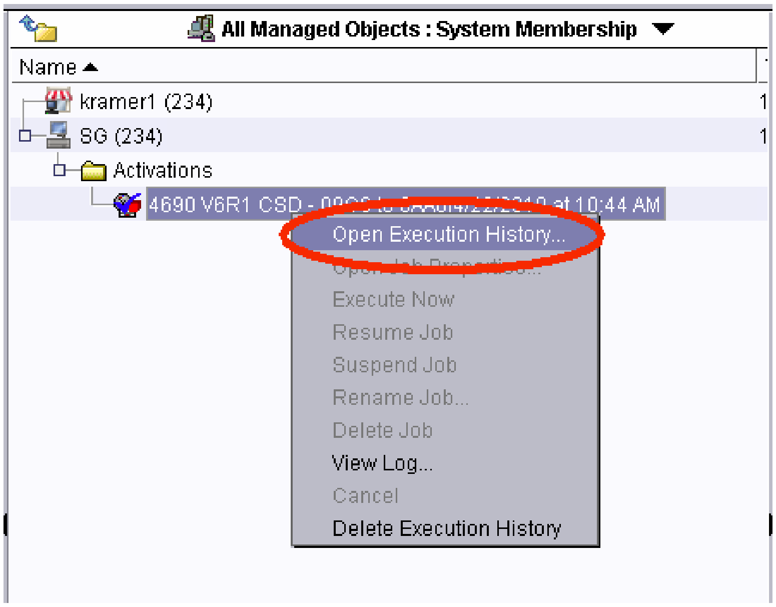
After the log is displayed, set it to "High" detail, and scan the logs for any errors. Information from the RCP status file will be populated in these logs:


SG (234) : 4/22/2010 at 10:44 AM: 4690 V6R1 CSD - 09C0 to 0AA0
File
Edit
View
Help
Refresh
Dynamic Update
Detail
Low
Medium
✓ High

```
4/22/2010 1                                    hanged to "Active".
4/22/2010 10:44:54 AM   Streaming              laster Agent
4/22/2010 10:44:58 AM   Package fi             % complete
4/22/2010 10:45:00 AM   Package file streaming: 20% complete
4/22/2010 10:45:02 AM   Package file streaming: 30% complete
4/22/2010 10:45:04 AM   Package file streaming: 40% complete
4/22/2010 10:45:05 AM   Package file streaming: 50% complete
4/22/2010 10:45:07 AM   Package file streaming: 60% complete
4/22/2010 10:45:09 AM   Package file streaming: 70% complete
4/22/2010 10:45:10 AM   Package file streaming: 80% complete
4/22/2010 10:45:12 AM   Package file streaming: 90% complete
4/22/2010 10:45:14 AM   Package file streaming: 100% complete
4/22/2010 10:45:16 AM   Making request to stage package on Master Agent
4/22/2010 10:45:16 AM   Device policy Id: 1190146614
4/22/2010 10:45:20 AM   Software package deployment information read
4/22/2010 10:45:20 AM   Creating individual device policies
4/22/2010 10:45:30 AM   Software package file extracted on Master Agent
4/22/2010 10:45:30 AM   Package staging complete
```

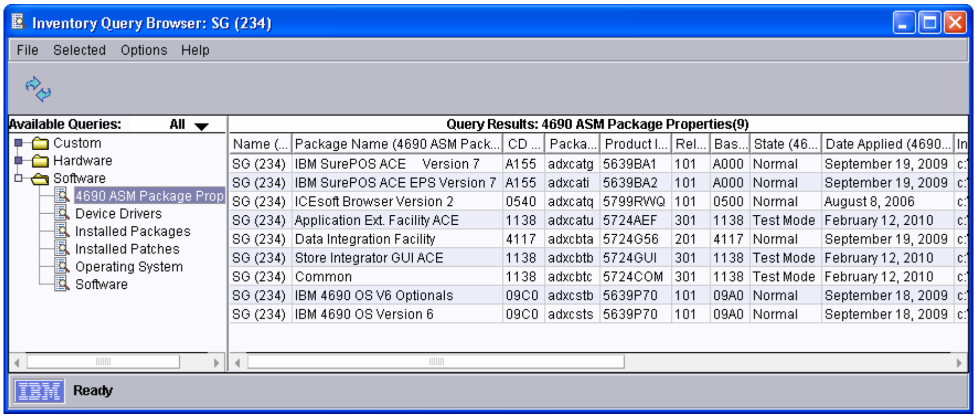
You can view software distribution history data from previous distributions by enabling the "Activations" association and right-clicking on the particular activation:





When the Software Distribution is complete, you can re-collect inventory on all of your 4690 systems to ensure they are all at the proper level.

To view the ASM Package levels, look in the “Software -> 4690 ASM Package Properties” table:



Query Results: 4690 ASM Package Properties(9)

Name (...	Package Name (4690 ASM Pack...	CD ...	Packa...	Product I...	Rel...	Bas...	State (46...	Date Applied (4690...	In
SG (234)	IBM SurePOS ACE Version 7	A155	adxcatg	5639BA1	101	A000	Normal	September 19, 2009	c:
SG (234)	IBM SurePOS ACE EPS Version 7	A155	adxcati	5639BA2	101	A000	Normal	September 19, 2009	c:
SG (234)	ICEsoft Browser Version 2	0540	adxcatq	5799RWQ	101	0500	Normal	August 8, 2006	c:
SG (234)	Application Ext. Facility ACE	1138	adxcatu	5724AEF	301	1138	Test Mode	February 12, 2010	c:
SG (234)	Data Integration Facility	4117	adxcbta	5724G56	201	4117	Normal	September 19, 2009	c:
SG (234)	Store Integrator GUI ACE	1138	adxcbtb	5724GUI	301	1138	Test Mode	February 12, 2010	c:
SG (234)	Common	1138	adxcbtc	5724COM	301	1138	Test Mode	February 12, 2010	c:
SG (234)	IBM 4690 OS V6 Optionals	09C0	adxcstb	5639P70	101	09A0	Normal	September 18, 2009	c:
SG (234)	IBM 4690 OS Version 6	09C0	adxcsts	5639P70	101	09A0	Normal	September 18, 2009	c:

You can also use this table to create a dynamic group of all of the systems that are, or are not at the new level.

Chapter 9 – Retail Peripheral Management

This chapter explains how to manage peripheral-attached devices (e.g. printers, cash drawers, etc.) using RMA. It teaches you how to setup your POS terminals for peripheral management, and how to use IBM Director for inventory, resource monitoring, and event management. It also explains how to use the "Retail Peripheral Management" task to simplify the presentation of the peripherals within Director.

Introduction to Retail Peripheral Management

There are several different ways to manage peripheral devices using RMA and IBM Director:

1. JavaPOS or OPOS (known together as "UPOS"). For remote systems running supported Windows or Linux-based operating systems, the IBM UPOS drivers provide rich instrumentation designed to enhance the remote manageability of supported peripheral devices. This instrumentation is made available to RMA through the Windows or Linux CIM repositories, allowing RMA to inventory and monitor the attached devices. On Windows, RMA can also relay status update events from the peripheral devices to IBM Director.

2. 4690 Operating System. For terminals running the 4690 operating system, the operating system provides built-in instrumentation for RMA, allowing inventory and monitoring of peripheral devices attached to the terminals.

3. Third-Party Drivers. Certain third-parties may provide support for RMA systems management through their own proprietary peripheral device drivers. For example, certain models of Honeywell (formerly Metrologic) scanners include "Remote Mastermind" software, which enables instrumentation for RMA peripheral management. Certain Symbol devices also include WMI-based instrumentation that allows RMA to manage those devices. This document does not cover these third-party drivers and devices.

The following table summarizes the peripheral management capabilities of RMA on the various platforms:

	Windows	Linux	4690
Drivers Needed	JavaPOS or OPOS	JavaPOS only	Built-in to OS
Inventory	**Yes**	**Yes**	**Yes**
Monitoring	**Yes**	**Yes**	**Yes**[1]
Event Forwarding	**Yes**	**Yes**	**No**

Notes:

- 1 – Monitoring on 4690 is only support on 4690 V6R1 and higher.

> **Note**: This document assumes that the UPOS drivers are at the 1.9.6b version or higher – older UPOS driver versions may not have the same level of functionality as described here. It is highly recommended to maintain a current version of the UPOS drivers when possible. The latest version as of the writing of this document is 1.13.1.

The instructions below will help you plan, install, configure, and effectively use the peripheral management capabilities of the RMA and IBM Director solution.

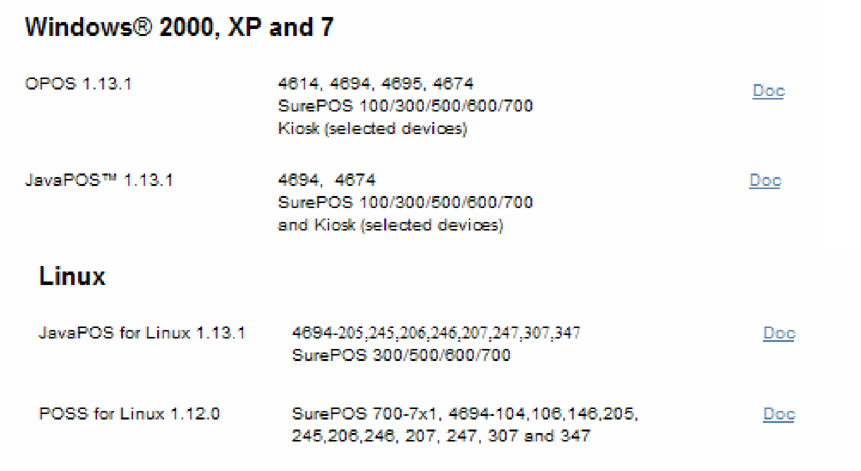
Planning for Peripheral Management via JavaPOS / OPOS

Supported Platforms, Devices, and Interfaces

The first step in planning for systems management of the peripheral-attached devices in your environment is to understand exactly which devices and configurations are supported by the drivers. You should be aware of the resources below, which can help you in the planning process.

The first resource is the UPOS download page on the RSS support website, which can be found here:
http://www2.clearlake.ibm.com/store/support/html/driverss.html

At the link above, you will find information about the operating systems and POS hardware units supported by the drivers. As of version 1.13.1, the website shows the following supported platforms:



Windows® 2000, XP and 7

OPOS 1.13.1	4614, 4694, 4695, 4674 SurePOS 100/300/500/600/700 Kiosk (selected devices)	Doc
JavaPOS™ 1.13.1	4694, 4674 SurePOS 100/300/500/600/700 and Kiosk (selected devices)	Doc

Linux

JavaPOS for Linux 1.13.1	4694-205,245,206,246,207,247,307,347 SurePOS 300/500/600/700	Doc
POSS for Linux 1.12.0	SurePOS 700-7x1, 4694-104,106,146,205, 245,206,246, 207, 247, 307 and 347	Doc

Note: The list of platforms shown above is for illustrative purposes only – please check with the website or the published UPOS documentation for the definitive support list for any particular version of UPOS. Also note that WEPOS (Windows Embedded for Point-of-Service) and POSReady are supported under the Windows XP umbrella.

The second resource is the JavaPOS user's guide, which can be found at the link below:
http://www-01.ibm.com/support/docview.wss?rs=219&uid=pos1R7000087

For detailed information about individual devices (such as the POS printer, the POS modular keyboards, etc.), look for the device-specific attributes in the UPOS user's guide. Also look at **Appendix A** in the UPOS user's guide, which details the systems management statistics properties available via RMA. The user's guide has a wealth of information about the systems management attributes, devices, and what to expect with various methods of connecting the peripheral device to the system unit (i.e. USB vs. RS232, etc.).

In general, the UPOS driver package supports systems management attributes on the following devices:

- Cash drawer
- Check scanner
- Fiscal printer
- Hard totals
- Keylock
- Line display
- MICR
- Motion sensor
- MSR
- POS keyboard
- POS printer
- Scale
- Scanner
- Tone Indicator

For more detailed descriptions of the various attributes supported on the above devices, consult the device-specific chapters, along with **Appendix A,** in the UPOS user's guide (as noted above).

You can also find information in the user's guide about the list of specific **StatusUpdateEvent**'s supported for each peripheral device, such as "PTR_SUE_COVER_OPEN" for the POS printer. This information is contained throughout the document, in the sections covering the various devices. On Windows and Linux, these events are forwarded through RMA to IBM Director.

Downloading and Installing the UPOS Drivers

Note: If you are installing JavaPOS for IRES, you should follow the setup instructions found in "**Chapter 4 – Setting Up RMA on IRES**".

If you are installing JavaPOS on SLEPOS 11, you should follow the setup instructions found in the following article: http://www-01.ibm.com/support/docview.wss?rs=0&uid=pos1R1004460

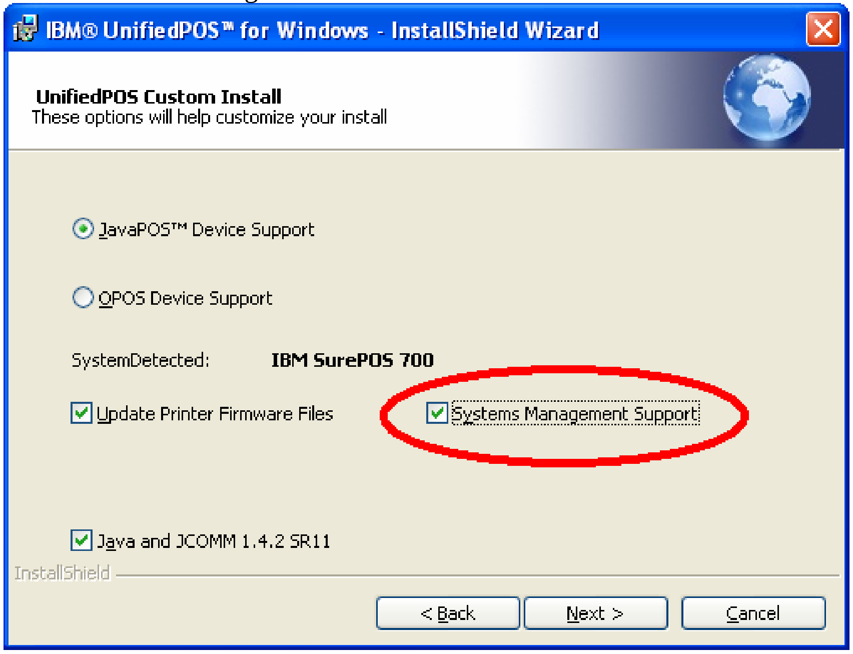
Before installing the UPOS drivers, you will need to download them from the UPOS download page. (See above for the URL to download the drivers).

Once you have downloaded the driver package, follow the instructions in the UPOS user's guide to install the drivers. (See above for the URL to the user's guide.)

Note: The UPOS user's guide contains valuable information about installing and using the UPOS (JavaPOS/OPOS) drivers. For example, if you are mass-deploying the drivers, you can refer to the "silent installation" section for information on how to perform an unattended installation.

JavaPOS

When you install JavaPOS, make sure to check the "Systems Management" checkbox, as shown in the following screenshot:



IBM® UnifiedPOS™ for Windows - InstallShield Wizard

UnifiedPOS Custom Install

These options will help customize your install

● JavaPOS™ Device Support

○ OPOS Device Support

SystemDetected: **IBM SurePOS 700**

☑ Update Printer Firmware Files

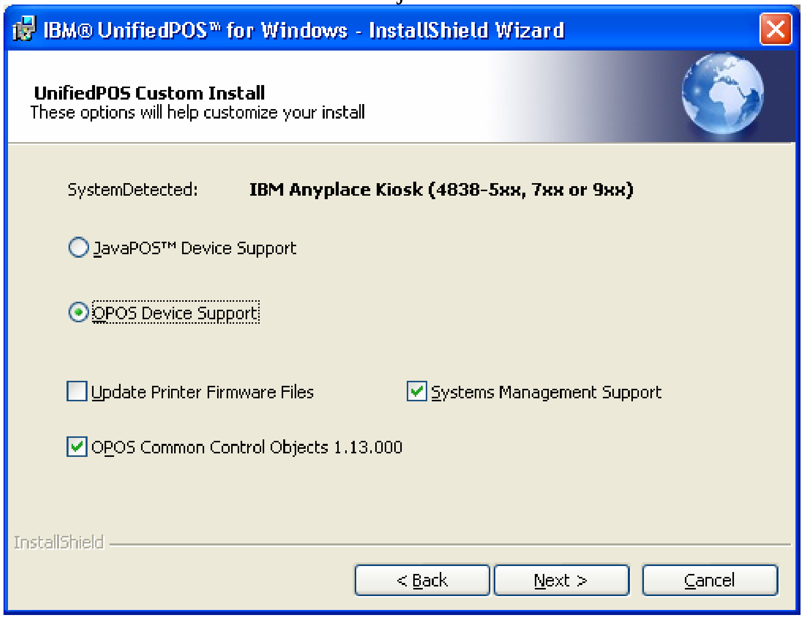
☑ Systems Management Support

☑ Java and JCOMM 1.4.2 SR11

OPOS

When you install OPOS, it is important that you check the following options:

- Systems Management Support
- OPOS Common Control Objects



IBM® UnifiedPOS™ for Windows - InstallShield Wizard

UnifiedPOS Custom Install
These options will help customize your install

SystemDetected: **IBM Anyplace Kiosk (4838-5xx, 7xx or 9xx)**

○ JavaPOS™ Device Support

● OPOS Device Support

□ Update Printer Firmware Files ☑ Systems Management Support

☑ OPOS Common Control Objects 1.13.000

In versions prior to 1.13.1, when you checked the "Systems Management Support" option for OPOS, it installed a JavaPOS Gateway that allowed OPOS to utilize the JavaPOS infrastructure behind the scenes.

As of version 1.13.1, OPOS systems management works directly without needing the JavaPOS interface. This is a much tighter integration with RMA, so it is highly recommend that you are on version 1.13.1 of the UPOS drivers if you want to enable OPOS Systems Management support.

Verifying Systems Management Capabilities of Devices

Starting with version 1.9.6b of JavaPOS, it's now possible to use a special "Systems Management" tab in the POS Control Center. This tab allows you to easily test your connection to the peripheral devices and verify the systems management capabilities of the device. This is a valuable resource for testing/evaluating the systems management solution, because it can help you determine quickly and easily what's possible for your specific configuration of drivers and peripheral-attached devices. Once you've verified the capabilities using the POS Control Center, then you can begin using RMA to leverage these capabilities remotely.

If you are using 1.9.6b, you need to download the "Systems Management" plug-in separately, from the RSS knowledge base. The URL is:
http://www-01.ibm.com/support/docview.wss?rs=219&uid=pos1R1004343

Note: After you've downloaded the plug-in from the URL above, follow the instructions in that article to learn how to launch the POS Control Center with the plug-in. The easiest method is to extract the contents of the ZIP file to any location on your hard drive, then launch the BAT file to start the POS Control Center.

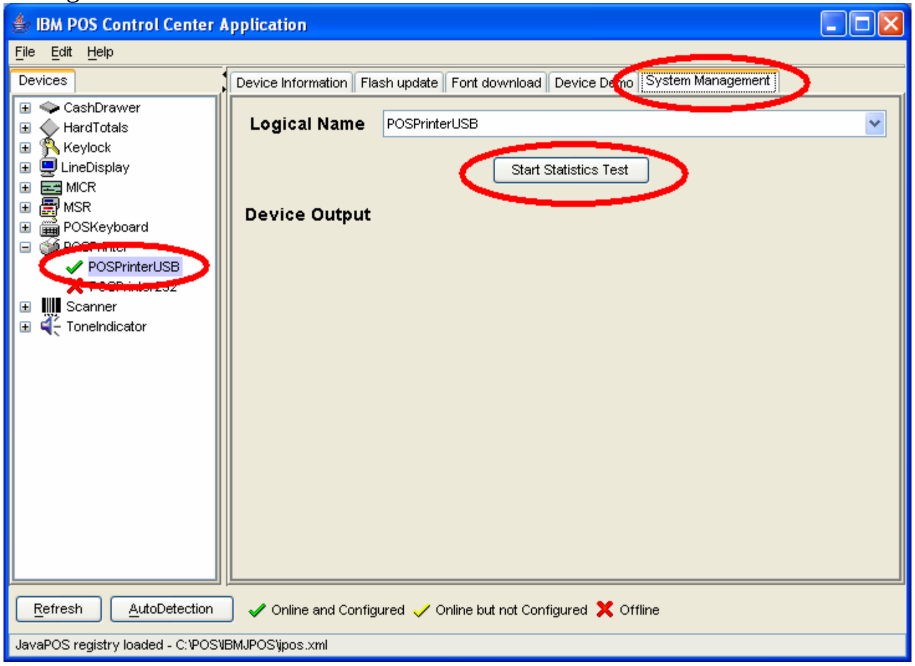
If you are using version 1.12 or higher, then the "Systems Management" tab is available by default in the released version of POS Control Center.

To use the "Systems Management" tab of the POS Control Center, follow the instructions below:

1. First, make sure your "jpos.xml" file is configured correctly. The "AutoDetection" feature can be used to auto-populate detected devices into the jpos.xml. (Refer to the UPOS user's guide for instructions.)

2. Launch the POS Control Center. (If using version 1.9.6b with the separate plug-in, make sure you launch it according to the instructions found in the knowledge base article for the plug-in.)

3. Select a peripheral-attached device on the left-hand side of the screen. In this example, we'll use the USB-attached 4610 POS printer. Then select the "Systems Management" tab. You should see a button labeled "Start Statistics Test".



IBM POS Control Center Application

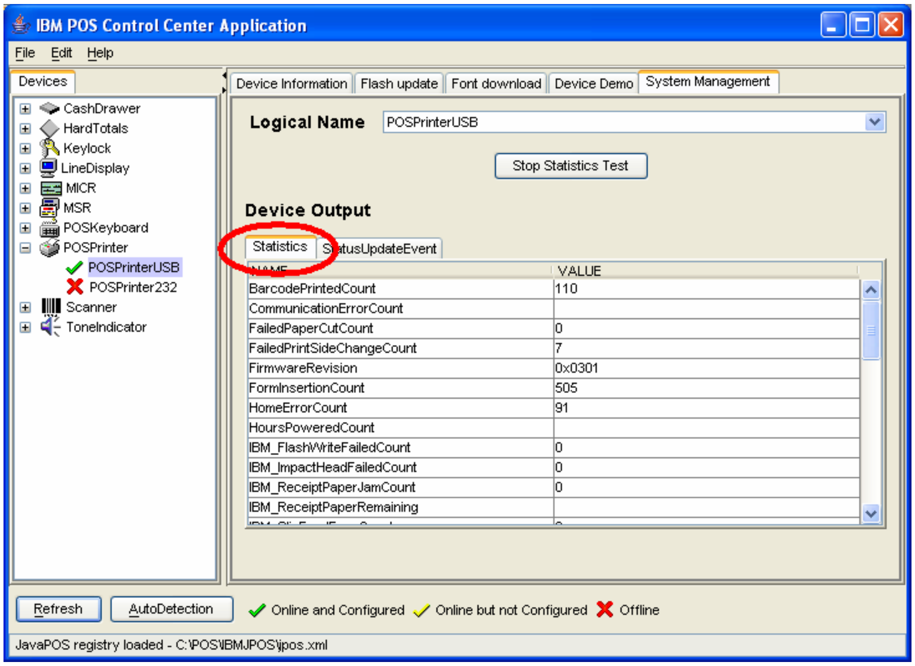
Logical Name: POSPrinterUSB

Device Output

JavaPOS registry loaded - C:\POS\IBMJPOS\jpos.xml

4. Click the "Start Statistics Test" button. **The POS Control Center will then open/claim/enable the device, and keep it opened/claimed/enabled until you**

click “Stop Statistics Test”. You will then see the list of systems management attributes that are available for that device:



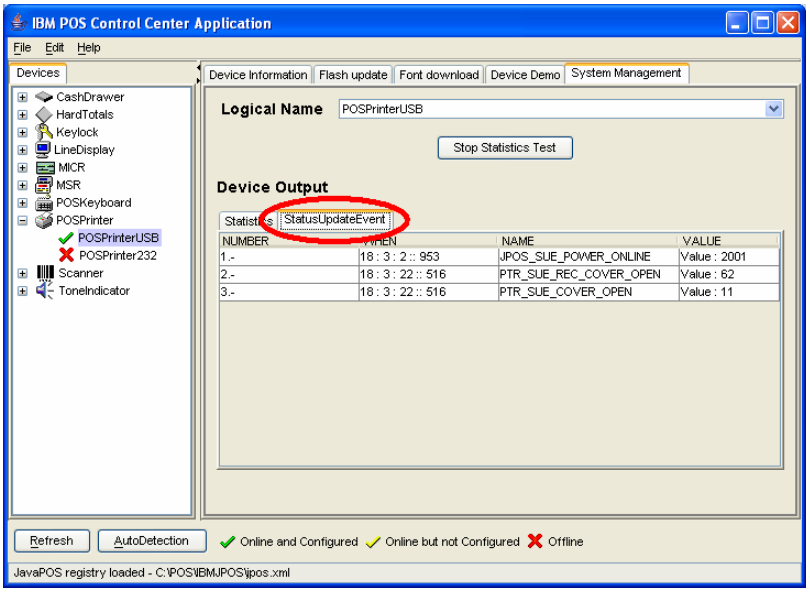
Logical Name: POSPrinterUSB

NAME	VALUE
BarcodePrintedCount	110
CommunicationErrorCount	
FailedPaperCutCount	0
FailedPrintSideChangeCount	7
FirmwareRevision	0x0301
FormInsertionCount	505
HomeErrorCount	91
HoursPoweredCount	
IBM_FlashWriteFailedCount	0
IBM_ImpactHeadFailedCount	0
IBM_ReceiptPaperJamCount	0
IBM_ReceiptPaperRemaining	

JavaPOS registry loaded - C:\POS\IBMJPOS\jpos.xml

Note: After you’ve clicked “Start Statistics Test”, you should also be able to view the device within RMA/Director via the JMX Browser (see instructions below), since the device is opened/claimed/enabled at that point. Once you click “Stop Statistics Test”, the device will no longer be visible because the device is no longer opened/claimed/enabled.

5. To test the status update events (which are forwarded to RMA on Windows installations), you can use the “StatusUpdateEvent” tab. For example, try lifting the cover open on a 4610 printer, and watch the status update events appear in the POS Control Center. This is a helpful diagnostic step when troubleshooting problems with event management via RMA/Director.



Logical Name: POSPrinterUSB

NUMBER	WHEN	NAME	VALUE
1.-	18 : 3 : 2 :: 953	JPOS_SUE_POWER_ONLINE	Value : 2001
2.-	18 : 3 : 22 :: 516	PTR_SUE_REC_COVER_OPEN	Value : 62
3.-	18 : 3 : 22 :: 516	PTR_SUE_COVER_OPEN	Value : 11

JavaPOS registry loaded - C:\POS\IBMJPOS\jpos.xml

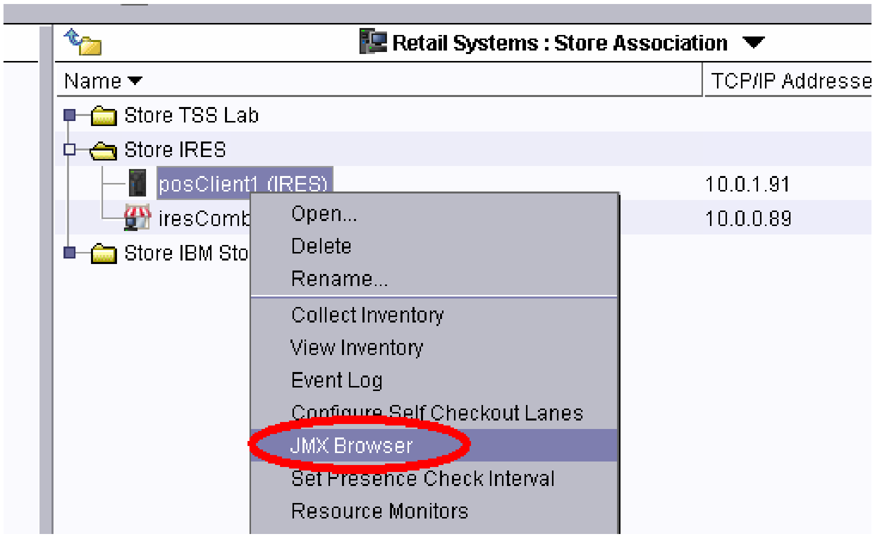
Verifying UPOS Device Mbeans in Director

To verify that the systems management instrumentation for your peripheral-attached device is working properly with RMA, follow the instructions below.

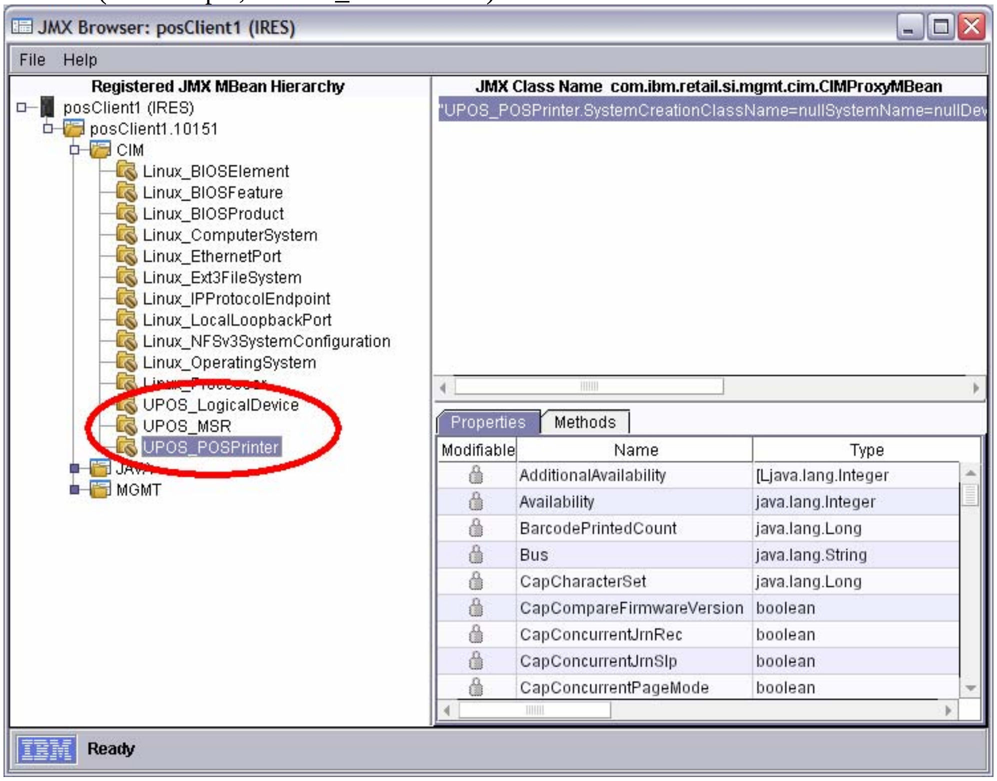
> **Note**: In JavaPOS or OPOS 1.9.6b, your application (or the POS Control Center, or some other application) must “open” the device before RMA will be able to see the instrumentation! If you follow the steps below and find that the instrumentation is not visible in IBM Director, verify that the application has the device opened in JavaPOS or OPOS. It’s also generally a good idea to test using the POS Control Center (see previous section of this document) before using your own application to test. Also note that *some* systems management attributes are only visible if the device is “opened/claimed/enabled” rather than just “opened”.

After you have made sure that the devices are at least “opened” via JavaPOS/OPOS, you can use the “JMX Browser” task within IBM Director to verify that the MBeans are properly registered with RMA.

1. Right-click the system in Director, and select “JMX Browser”.



2. Expand the tree on the left-hand side of the screen until you see the UPOS Mbeans (for example, "UPOS_POSPrinter").



JMX Class Name com.ibm.retail.si.mgmt.cim.CIMProxyMBean

"UPOS_POSPrinter.SystemCreationClassName=nullSystemName=nullDev

Modifiable	Name	Type
🔒	AdditionalAvailability	[Ljava.lang.Integer
🔒	Availability	java.lang.Integer
🔒	BarcodePrintedCount	java.lang.Long
🔒	Bus	java.lang.String
🔒	CapCharacterSet	java.lang.Long
🔒	CapCompareFirmwareVersion	boolean
🔒	CapConcurrentJrnRec	boolean
🔒	CapConcurrentJrnSlp	boolean
🔒	CapConcurrentPageMode	boolean

3. Once the UPOS Mbeans are appearing in JMX Browser (as shown above), you can begin working with the devices using the Director user interface. For example, you can collect inventory then use the retail peripheral management task in Director.

Planning for Peripheral Management via 4690 OS

Supported Platforms, Devices, and Interfaces

On 4690 V5R2, the following devices are instrumented for remote management:

- Keyboard
- Printer
- MICR
- Check scanner

On 4690 V6, the device instrumentation for terminals is as follows:

- MSR
- Line display
- Cash drawer
- Tone indicator
- Keylock
- Printer
- MICR
- Check scanner
- Keyboard

Initial Setup / Configuration

On both 4690 V5R2 and 4690 V6, RMA automatically has visibility to the terminal devices via the operating system (i.e. 4690 does not rely on the UPOS drivers, so there is no need to do anything special to make the devices appear in RMA).

Therefore, the steps to configure the peripheral devices in 4690 are much simpler than for UPOS. To set up the devices, you need to:

1. Set up RMA on 4690, and make sure the terminals appear within IBM Director. (For information on general RMA/4690 setup, see "**Chapter 2 – Setting Up RMA on 4690**".)

2. Verify that the MBeans appear in IBM Director (see section below).

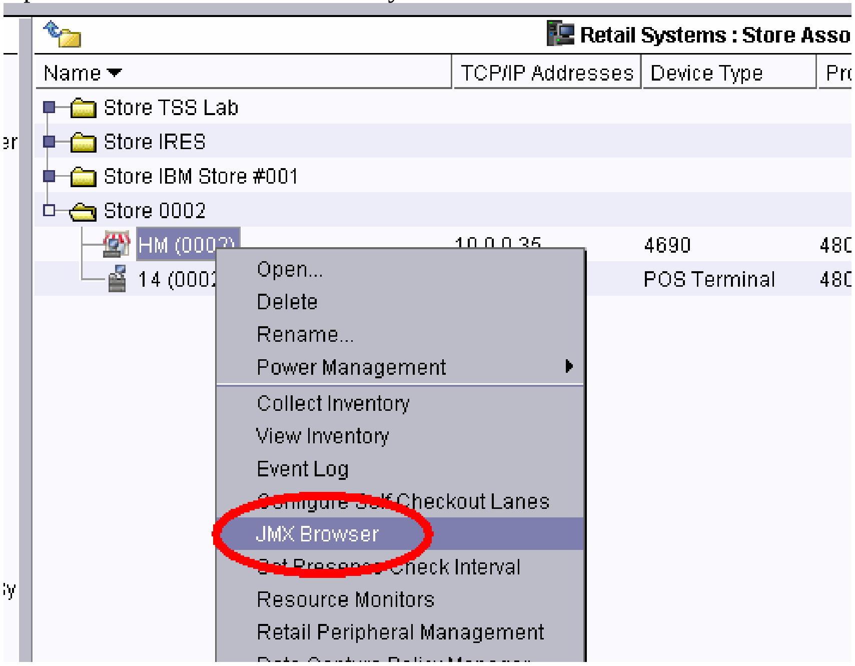
3. Collect inventory, and begin using the retail peripheral management task (see "Collecting and Viewing Inventory for Peripherals" section of this document).

Verifying 4690 Device Mbeans in Director

Even though 4690 does not rely on the IBM UPOS drivers, it does implement its device instrumentation in terms of the UPOS specification. Therefore, the device instrumentation is visible with Director's "JMX Browser" task, with names such as "UPOS_Scanner" (for the scanner).

You can easily use the JMX Browser task within IBM Director to verify that the peripheral devices are appearing correctly within RMA. To do that:

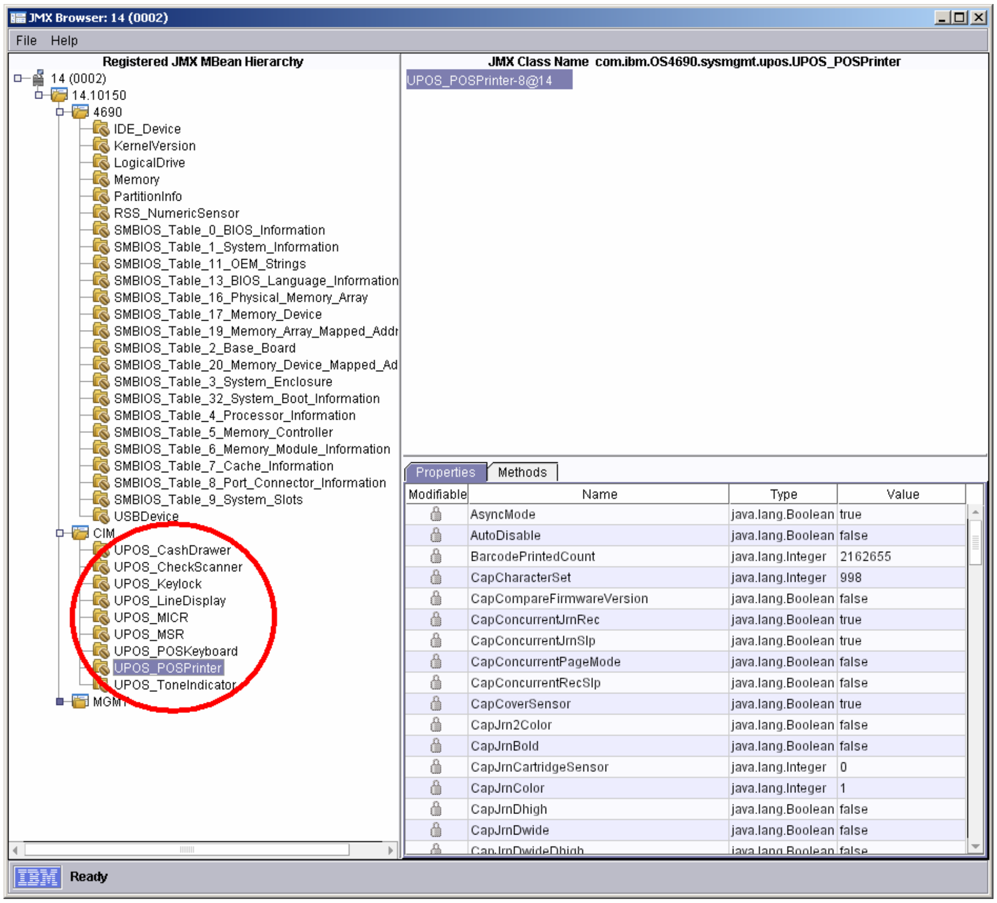
1. Open the JMX Browser for one of your 4690 terminals:



Retail Systems : Store Asso
Open...
Delete
Rename...
Power Management
Collect Inventory
View Inventory
Event Log
Configure Self Checkout Lanes
JMX Browser
Set Presence Check Interval
Resource Monitors
Retail Peripheral Management
Data Capture Policy Manager

Name	TCP/IP Addresses	Device Type	Pro
Store TSS Lab			
Store IRES			
Store IBM Store #001			
Store 0002			
HM (0002)	10.0.0.35	4690	480
14 (0002		POS Terminal	480

2. Expand the tree on the left-hand side of the screen until you see the UPOS Mbeans (for example, "UPOS_POSPrinter").



Registered JMX MBean Hierarchy

```
14 (0002)
  14.10150
    4690
      IDE_Device
      KernelVersion
      LogicalDrive
      Memory
      PartitionInfo
      RSS_NumericSensor
      SMBIOS_Table_0_BIOS_Information
      SMBIOS_Table_1_System_Information
      SMBIOS_Table_11_OEM_Strings
      SMBIOS_Table_13_BIOS_Language_Information
      SMBIOS_Table_16_Physical_Memory_Array
      SMBIOS_Table_17_Memory_Device
      SMBIOS_Table_19_Memory_Array_Mapped_Addr
      SMBIOS_Table_2_Base_Board
      SMBIOS_Table_20_Memory_Device_Mapped_Ad
      SMBIOS_Table_3_System_Enclosure
      SMBIOS_Table_32_System_Boot_Information
      SMBIOS_Table_4_Processor_Information
      SMBIOS_Table_5_Memory_Controller
      SMBIOS_Table_6_Memory_Module_Information
      SMBIOS_Table_7_Cache_Information
      SMBIOS_Table_8_Port_Connector_Information
      SMBIOS_Table_9_System_Slots
      USBDevice
    CIM
      UPOS_CashDrawer
      UPOS_CheckScanner
      UPOS_Keylock
      UPOS_LineDisplay
      UPOS_MICR
      UPOS_MSR
      UPOS_POSKeyboard
      UPOS_POSPrinter
      UPOS_ToneIndicator
    MGMT
```

JMX Class Name com.ibm.OS4690.sysmgmt.upos.UPOS_POSPrinter

UPOS_POSPrinter-8@14

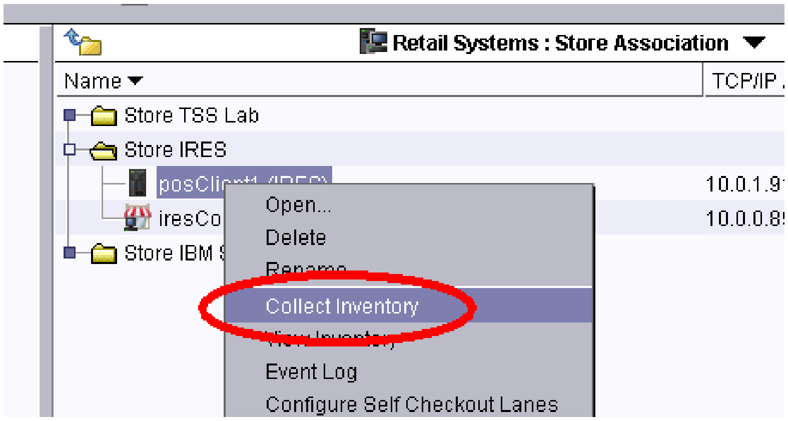
Modifiable	Name	Type	Value
🔒	AsyncMode	java.lang.Boolean	true
🔒	AutoDisable	java.lang.Boolean	false
🔒	BarcodePrintedCount	java.lang.Integer	2162655
🔒	CapCharacterSet	java.lang.Integer	998
🔒	CapCompareFirmwareVersion	java.lang.Boolean	false
🔒	CapConcurrentJrnRec	java.lang.Boolean	true
🔒	CapConcurrentJrnSlp	java.lang.Boolean	true
🔒	CapConcurrentPageMode	java.lang.Boolean	false
🔒	CapConcurrentRecSlp	java.lang.Boolean	false
🔒	CapCoverSensor	java.lang.Boolean	true
🔒	CapJrn2Color	java.lang.Boolean	false
🔒	CapJrnBold	java.lang.Boolean	false
🔒	CapJrnCartridgeSensor	java.lang.Integer	0
🔒	CapJrnColor	java.lang.Integer	1
🔒	CapJrnDhigh	java.lang.Boolean	false
🔒	CapJrnDwide	java.lang.Boolean	false
🔒	CapJrnDwideDhigh	java.lang.Boolean	false

3. Once the UPOS Mbeans are appearing in JMX Browser (as shown above), you can begin working with the devices using the Director user interface. For example, you can collect inventory then use the retail peripheral management task in Director.

Collecting and Viewing Inventory for Peripherals

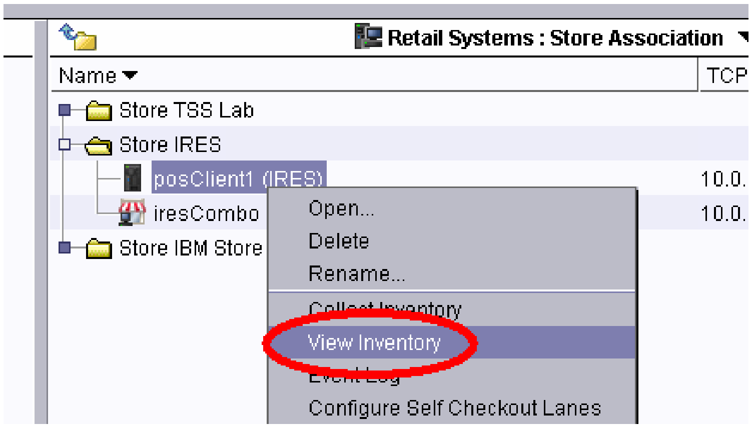
After you have verified that the peripheral MBeans are visible in the JMX Browser (see sections above for steps to verify), you can begin collecting and viewing inventory for the peripheral-attached devices.

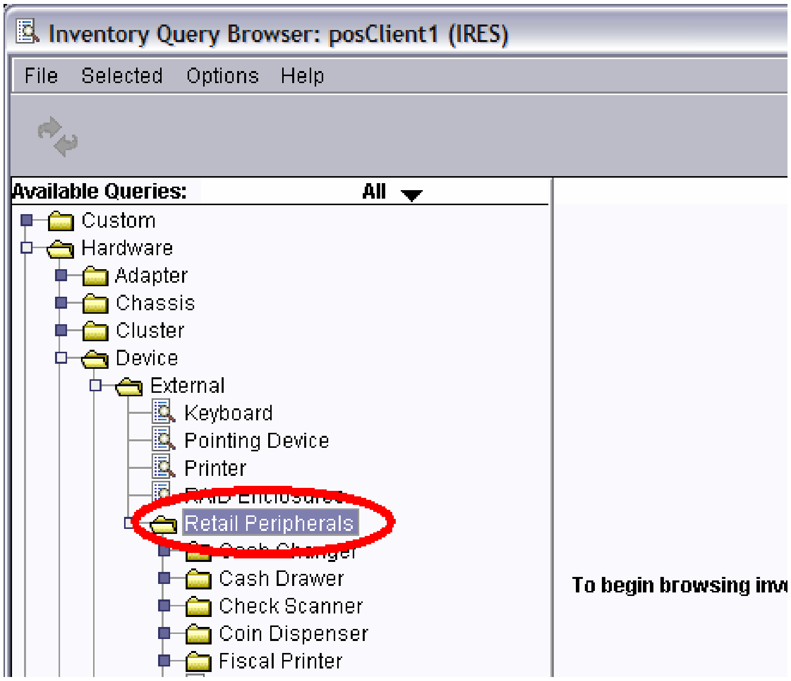
1. Collect inventory for your system(s). If the peripheral MBeans are visible in JMX Browser, then the inventory collection process will gather the inventory information for the peripheral-attached devices.



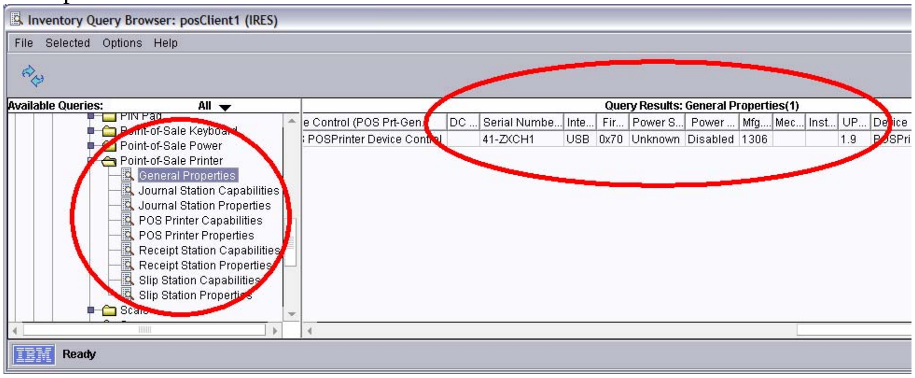
(Keep in mind that there are many ways to collect inventory, schedule the collection, customize the inventory collection settings, etc. (For additional information on collecting and using inventory, see "**Chapter 5 – RMA/Director Basics**".)

2. Once inventory is collected, use the "View Inventory" task, and navigate to "**Hardware / Device / External / Retail Peripherals**" within the inventory query browser.





3. Click on one of the retail peripherals shown in the inventory query browser, and you should be able to examine the attributes collected for that device. The example below shows the POS Printer attributes.



Query Results: General Properties(1)

e Control (POS Prt-Gen.	DC ...	Serial Numbe...	Inte...	Fir...	Power S...	Power ...	Mfg....	Mec...	Inst...	UP...	Device
POSPrinter Device Control		41-ZXCH1	USB	0x70	Unknown	Disabled	1306			1.9	POSPri

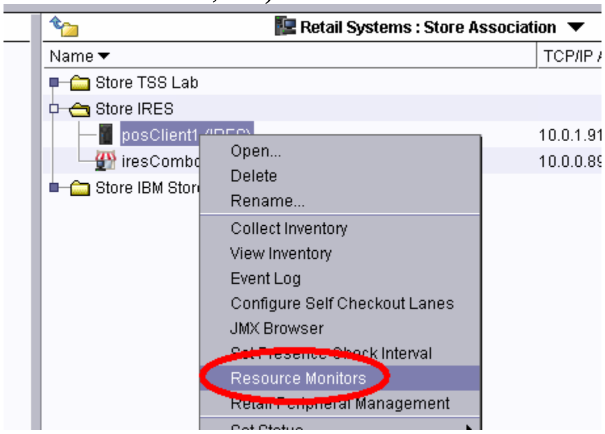
4. Once you've collected inventory, you can begin doing the following:
    - Create dynamic groups based on the inventory information you've collected.
    - Export the inventory to a spreadsheet, XML file, etc.
    - Use the retail peripheral management task to view the inventory and resource monitors for your devices.

Monitoring Peripherals

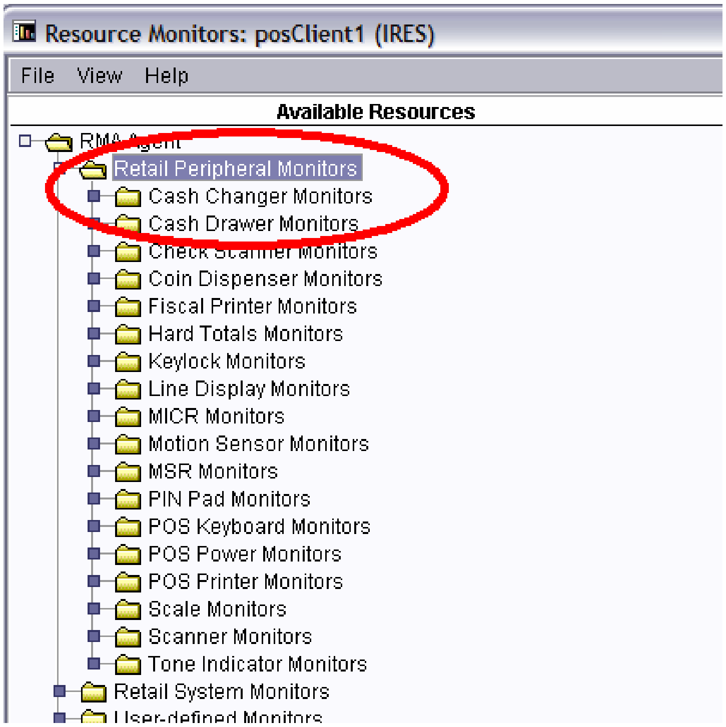
Resource Monitors for Peripherals

Working with the "Resource Monitors" task for peripheral management is no different than for any other attribute within RMA.

1. Drag the task to the device(s) or group(s) you want to monitor (or right-click, use the menus/toolbars, etc.).

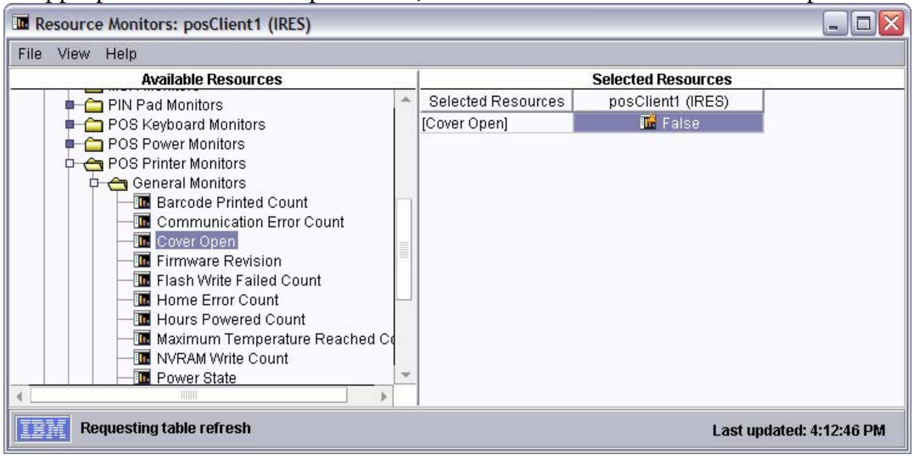


2. After the "Resource Monitors" task is activated, navigate to "**RMA Agent / Retail Peripheral Monitors**".



RMA Agent
Retail Peripheral Monitors
Cash Changer Monitors
Cash Drawer Monitors
Check Scanner Monitors
Coin Dispenser Monitors
Fiscal Printer Monitors
Hard Totals Monitors
Keylock Monitors
Line Display Monitors
MICR Monitors
Motion Sensor Monitors
MSR Monitors
PIN Pad Monitors
POS Keyboard Monitors
POS Power Monitors
POS Printer Monitors
Scale Monitors
Scanner Monitors
Tone Indicator Monitors
Retail System Monitors
User-defined Monitors

3. Choose the peripheral attributes you want to monitor, and create your thresholds as appropriate. In the example below, a threshold is created for the POS printer.



PIN Pad Monitors
POS Keyboard Monitors
POS Power Monitors
POS Printer Monitors
General Monitors
Barcode Printed Count
Communication Error Count
Cover Open
Firmware Revision
Flash Write Failed Count
Home Error Count
Hours Powered Count
Maximum Temperature Reached C
NVRAM Write Count
Power State

Selected Resources	posClient1 (IRES)
[Cover Open]	False

Requesting table refresh

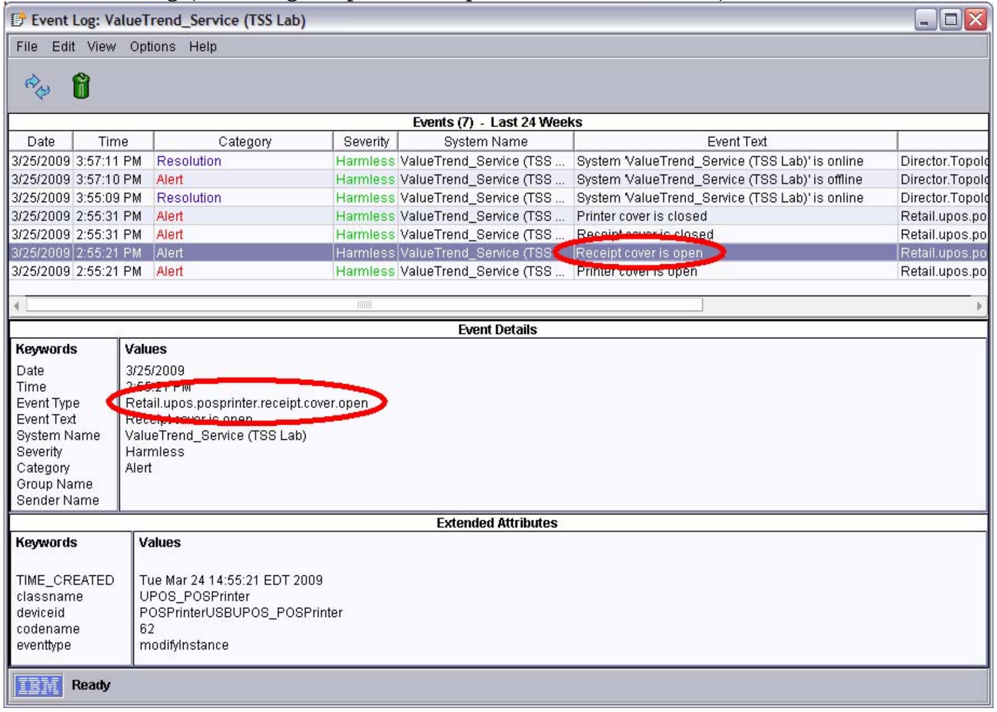
Last updated: 4:12:46 PM

4. Keep in mind that peripheral resource monitors work the same way as other resource monitors – i.e. you can create single or group thresholds; you can organize your threshold into "threshold plans"; you can import/export thresholds; and you can create custom "user-defined" thresholds using any attribute in the JMX Browser. (See "**Chapter 7 – Resource Monitoring**" for more general information on resource monitors.)

Event Management for Peripherals

The UPOS drivers are capable of relaying peripheral events to RMA/Director only on Windows and Linux operating systems. To take advantage of the event forwarding capabilities of the UPOS drivers on Windows and Linux, use the “Event Log” and “Event Action Plans” tasks within IBM Director’s user interface. (See “**Chapter 6 – Event Management**” for more general information on event management.)

For example, when the 4610 printer receipt cover is opened, you will see an event similar to the following (assuming the printer is opened/claimed/enabled):


Event Log: ValueTrend_Service (TSS Lab)
File Edit View Options Help
Ready

Events (7) - Last 24 Weeks

Date	Time	Category	Severity	System Name	Event Text	
3/25/2009	3:57:11 PM	Resolution	Harmless	ValueTrend_Service (TSS ...	System 'ValueTrend_Service (TSS Lab)' is online	Director.Topolo
3/25/2009	3:57:10 PM	Alert	Harmless	ValueTrend_Service (TSS ...	System 'ValueTrend_Service (TSS Lab)' is offline	Director.Topolo
3/25/2009	3:55:09 PM	Resolution	Harmless	ValueTrend_Service (TSS ...	System 'ValueTrend_Service (TSS Lab)' is online	Director.Topolo
3/25/2009	2:55:31 PM	Alert	Harmless	ValueTrend_Service (TSS ...	Printer cover is closed	Retail.upos.po
3/25/2009	2:55:31 PM	Alert	Harmless	ValueTrend_Service (TSS ...	Receipt cover is closed	Retail.upos.po
3/25/2009	2:55:21 PM	Alert	Harmless	ValueTrend_Service (TSS	Receipt cover is open	Retail.upos.po
3/25/2009	2:55:21 PM	Alert	Harmless	ValueTrend_Service (TSS ...	Printer cover is open	Retail.upos.po

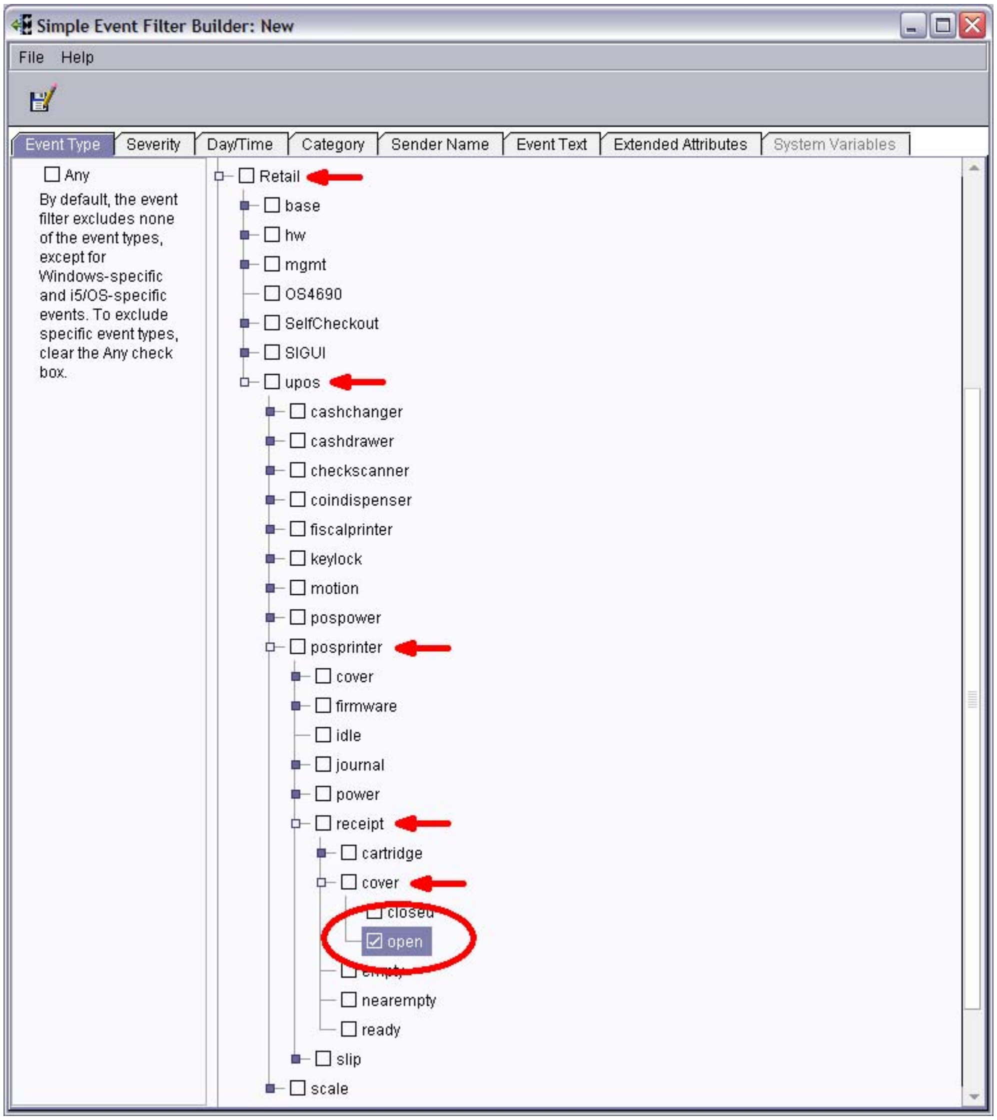
Event Details

Keywords	Values
Date	3/25/2009
Time	2:55:21 PM
Event Type	Retail.upos.posprinter.receipt.cover.open
Event Text	Receipt cover is open
System Name	ValueTrend_Service (TSS Lab)
Severity	Harmless
Category	Alert
Group Name	
Sender Name	

Extended Attributes

Keywords	Values
TIME_CREATED	Tue Mar 24 14:55:21 EDT 2009
classname	UPOS_POSPrinter
deviceid	POSPrinterUSBUPOS_POSPrinter
codename	62
eventtype	modifyInstance

When creating an event filter for these UPOS events, you can use the “Event Type” tab to select the applicable event types for the UPOS-specific events. In the screenshot below, the event type selected is “Retail.upos.posprinter.receipt.cover.open”. (For more information about creating event filters, see “**Chapter 6 – Event Management**”.)



By default, the event filter excludes none of the event types, except for Windows-specific and i5/OS-specific events. To exclude specific event types, clear the Any check box.

A complete list of the UPOS events that are forwarded through RMA and their severities can be found in the UPOSEventQualifiers.properties and UPOSEventSeverities.properties files.

These files are located on the RMA Agent systems in the following directories:
Windows: C:\Program Files\IBM\StoreIntegrator\user\rma\config\cim
Linux: /opt/ibm/StoreIntegrator/user/rma/config/cim

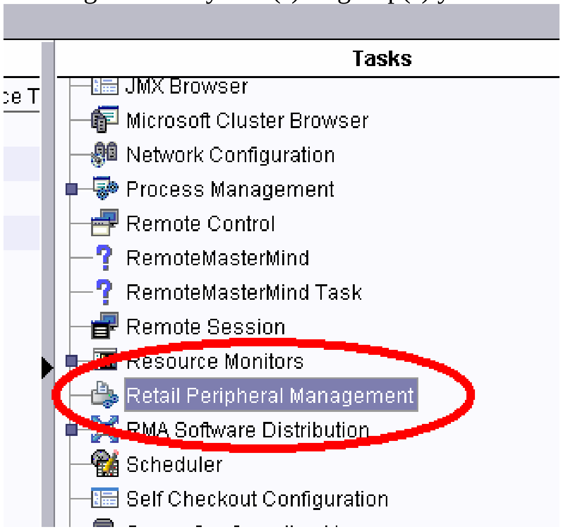
Using the Retail Peripheral Management Task

The retail peripheral management task is a special task in IBM Director that makes it easier for you to work with the peripheral devices in your environment.

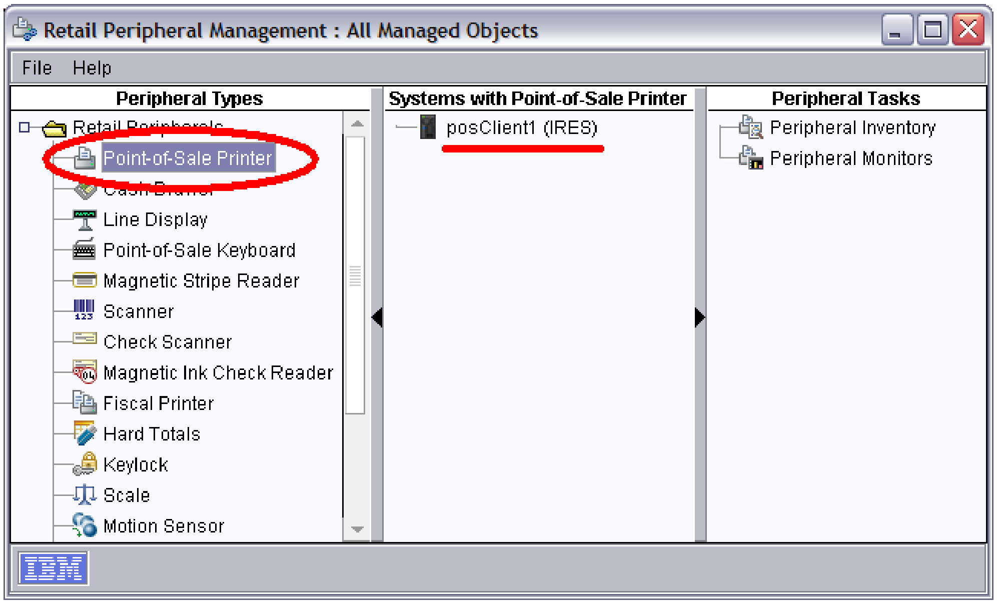
> **Note**: Before you begin using the retail peripheral management task, you MUST have collected valid inventory for the peripherals using the instructions above. Without inventory data for the peripheral devices, the retail peripheral management task will not work!

Use the instructions below to use the retail peripheral management task:

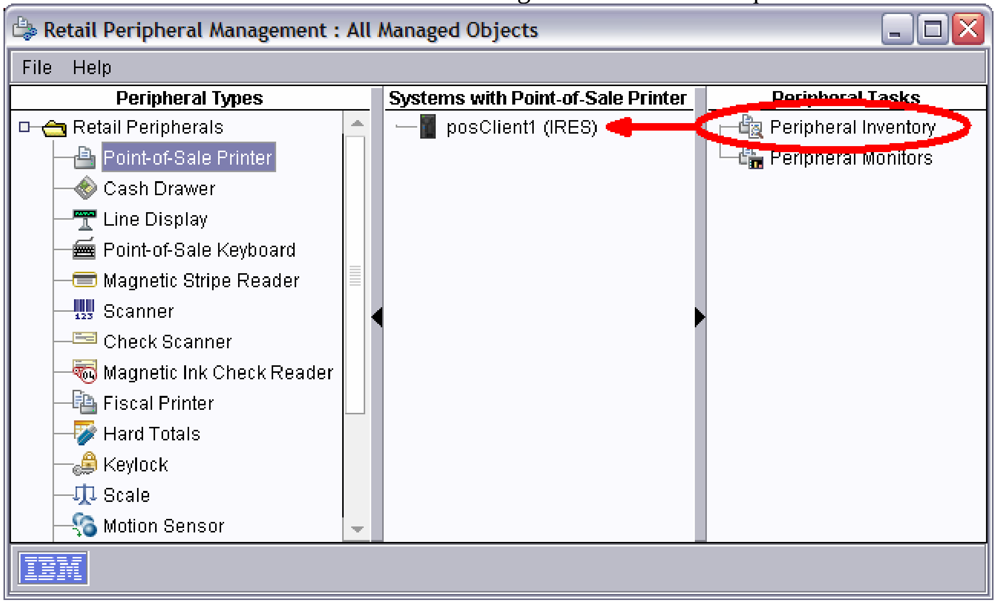
1. Double-click the "Retail Peripheral Management" task in IBM Director. (Or you can drag it to the system(s) or group(s) you want to manage, etc.)



2. On the left, click on the type of peripheral device you are interested in managing, and you will see a list of systems appear in the middle of the screen. Each of the systems listed in the middle of the screen has at least one instance of the device type selected on the left.



3. Finally, drag the "Peripheral Inventory" or "Peripheral Monitors" task to the system(s) you want to apply them to. Then you can work with the inventory information or with the resource monitors using the standard techniques.



4. You will observe that the "Retail Peripheral Management" task is sometimes an easier way to access the desired inventory and/or resource monitors for the peripheral types you are managing. It's really just another way to access the same

information that's available using the standard inventory and resource monitors tasks. Feel free to use whichever approach seems most logical for your needs.

5. It's also a good idea to become familiar with the "Retail Peripheral Management" section of the RMA user's guide, which can be found here: http://www2.clearlake.ibm.com/store/support/html/pubs.html#RMA

Distributing Firmware Updates to Peripherals

Updating Peripheral Device Firmware (JavaPOS / OPOS)

For systems that are running UPOS, there is a batch file called "flash.bat" that runs by default on every reboot of the system. This batch file looks in a particular directory to determine whether there any firmware updates for attached peripheral devices. If updates are found, the batch file automatically flashes those devices.

To update firmware remotely via RMA, you need to copy the updated firmware files into the appropriate directory on the system running UPOS, then reboot the system. Flash.bat will then automatically flash the devices. To verify the flash succeeded you can use inventory (or inventory alerts) to make sure the devices are at the correct firmware level. (See "**Chapter 5 – RMA/Director Basics**" for more information about using inventory and inventory alerts.)

The UPOS user's guide includes details on where to copy your firmware files (page 179 for the 1.13.1 version of the document). If using JavaPOS, look for this information in "POS Printer" chapter, under "Additional JavaPOS Information", "4610 Printer Firmware Update". If using OPOS, look in the "POS Printer" chapter, under "Additional OPOS Information", "4610 Printer Firmware Update".

Example: Updating the 4610 Printer Firmware

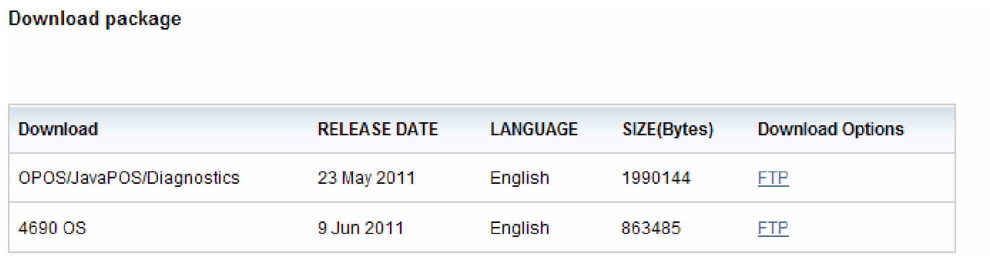
This example explains how to update the firmware for the 4610 printer for remote systems that are running UPOS on Windows.

Instructions:

1. Start by downloading the firmware update files from the RSS support website. Go to the following URL: http://www2.clearlake.ibm.com/store/support/html/4610-1234.html

   Click on "downloads" for the printer you plan to manage, and select the firmware download that is most appropriate for your printer.

   When you download the package from the website, be sure to click on the firmware update files that are intended for "OPOS/JavaPOS/Diagnostics":



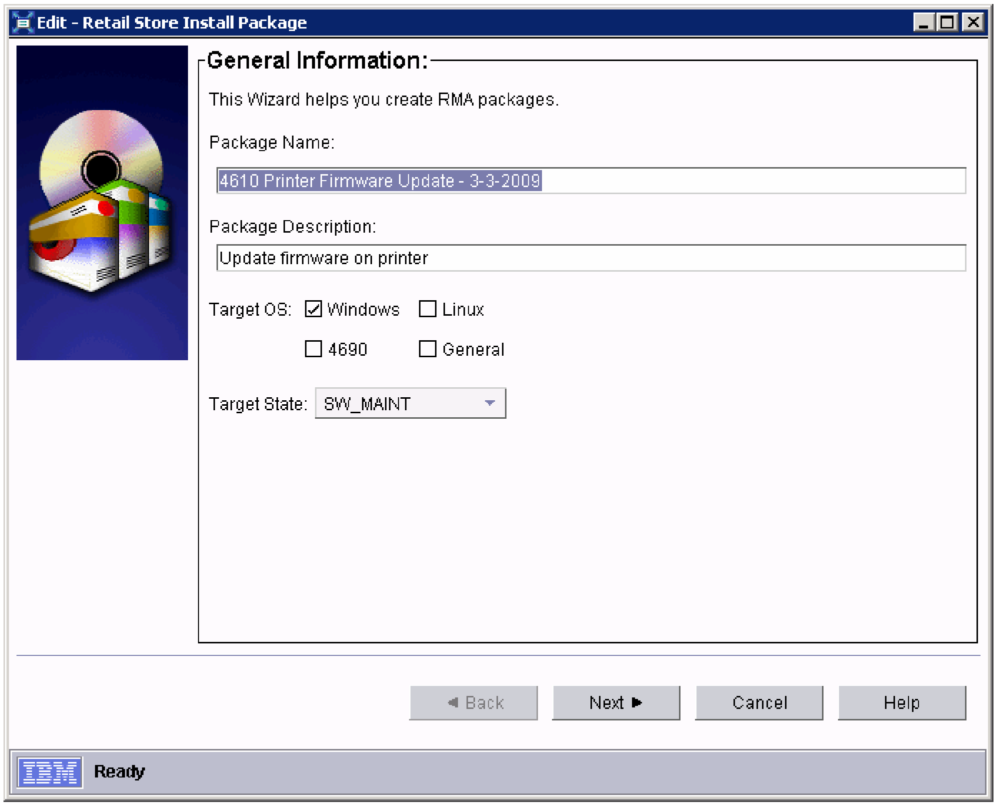
Download package

Download	RELEASE DATE	LANGUAGE	SIZE(Bytes)	Download Options
OPOS/JavaPOS/Diagnostics	23 May 2011	English	1990144	FTP
4690 OS	9 Jun 2011	English	863485	FTP

2. Unzip the file that you downloaded to any location on your Director Server.

3. Create a RMA Software Distribution package to distribute the firmware files to the remote system. (For more information on creating software distribution packages, see "**Chapter 8 – Software Distribution**".)

4. Give your package a name, description, and select "Windows" for the target OS. It's usually a good idea to choose "SW_MAINT" in case this package is ever distributed to a system (such as self-checkout) that uses this flag. (By default, RMA does not use the target states.)



Edit - Retail Store Install Package

General Information:

This Wizard helps you create RMA packages.

Package Name:

4610 Printer Firmware Update - 3-3-2009

Package Description:

Update firmware on printer

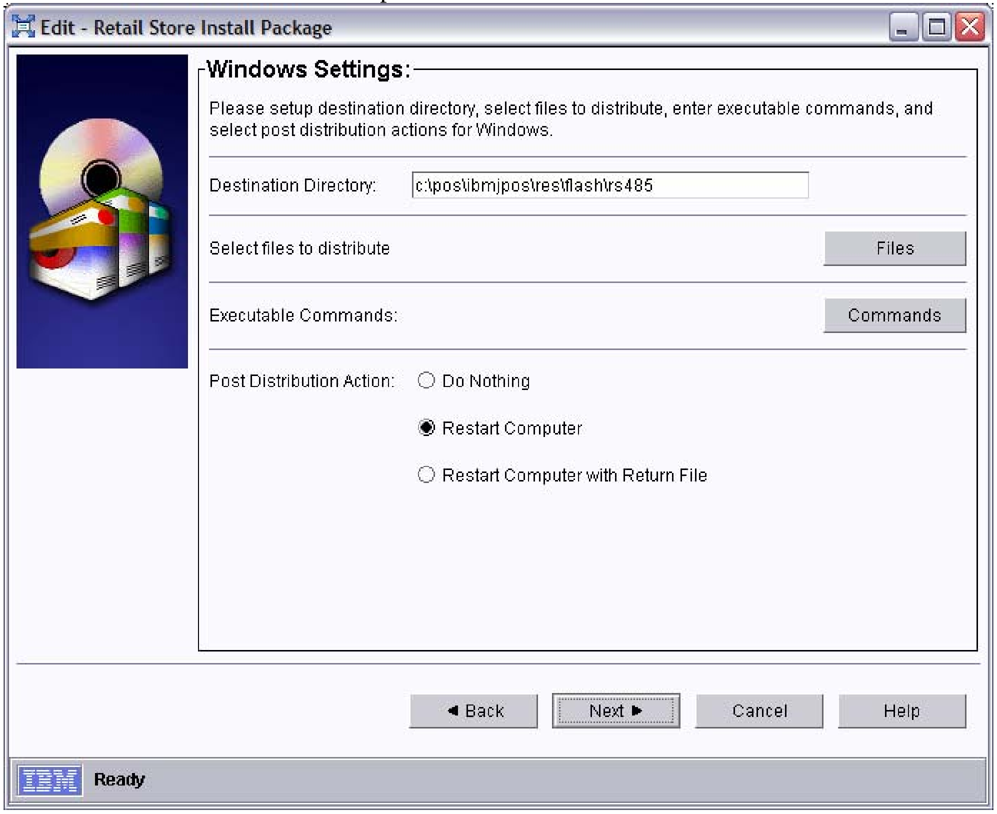
Target OS: ☑ Windows ☐ Linux

☐ 4690 ☐ General

Target State: SW_MAINT

Ready

5. For your destination directory, enter the path found in the UPOS user's guide. (The path illustrated below is for JavaPOS, and will not work on a OPOS system.) Also make sure that "Restart Computer" is selected.



Edit - Retail Store Install Package

Windows Settings:

Please setup destination directory, select files to distribute, enter executable commands, and select post distribution actions for Windows.

Destination Directory: c:\pos\ibmjpos\res\flash\rs485

Select files to distribute

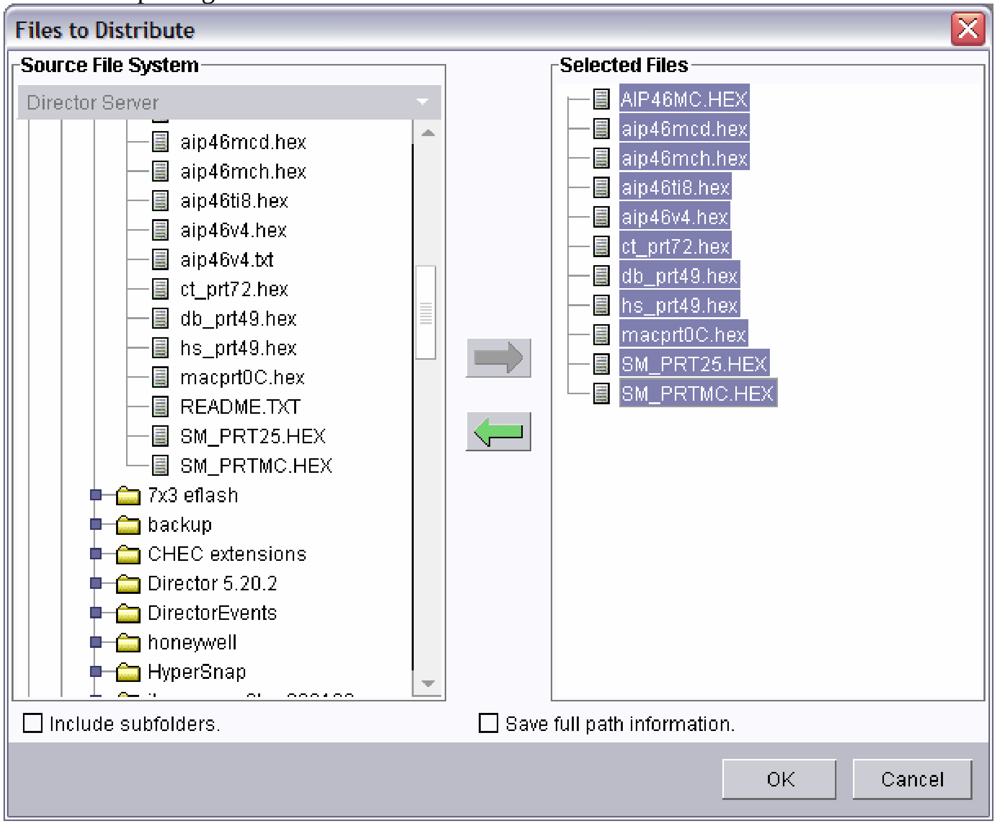
Executable Commands:

Post Distribution Action:
○ Do Nothing
● Restart Computer
○ Restart Computer with Return File

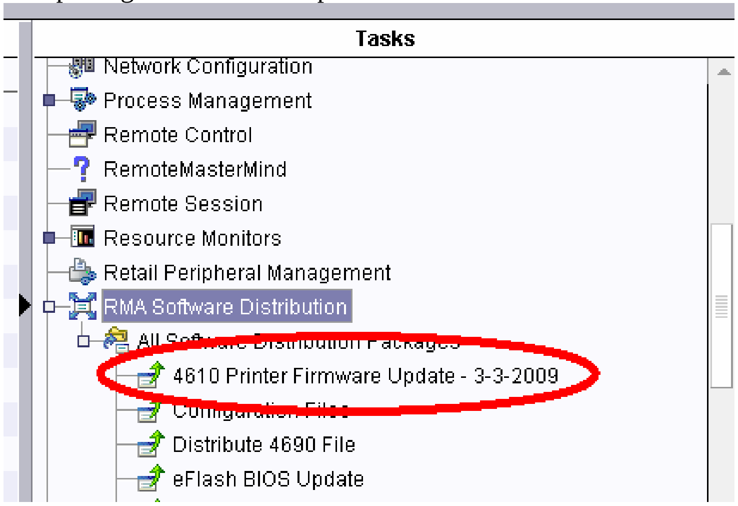
Ready

6. For the files to include in your package, browse to the location where you unzipped the firmware update files, and add all the "hex" files to the software

distribution package.



7. You don’t need any commands, so go ahead and finish creating the software distribution package without commands. When complete, you should see your new package in the “Tasks” pane within the Director console.



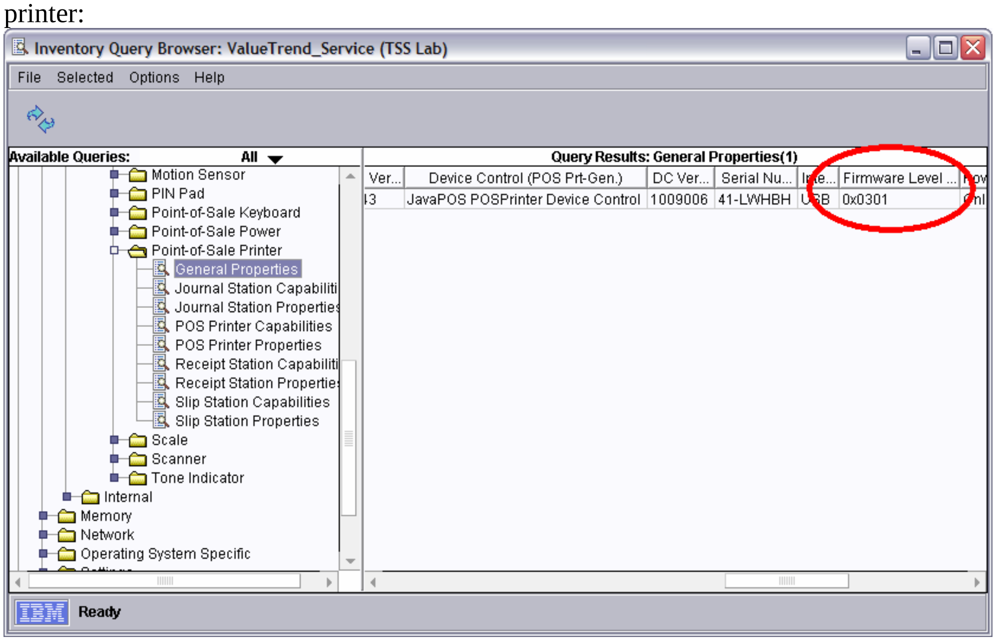
8. You can now distribute the package to your POS systems, or schedule it to distribute at a different time. Refer to “**Chapter 8 – Software Distribution**” for more complete instructions on creating and distributing software packages.

9. After you have distributed the firmware update, and allowed the system to reboot, you can verify that the firmware update succeeded. To do this, you’ll use the inventory features of Director, since the “flash.bat” program (which applies the firmware update to the printer) does not return success/failure information to RMA.

10. Make sure the printer is **opened/claimed/enabled**, then collect inventory on the system. (Or, use a custom inventory collection.)

11. After you’ve collected inventory, you can verify your results using any of the methods listed below. (For more information on these ways to verify the inventory, refer to “**Chapter 5 – RMA/Director Basics**”.)

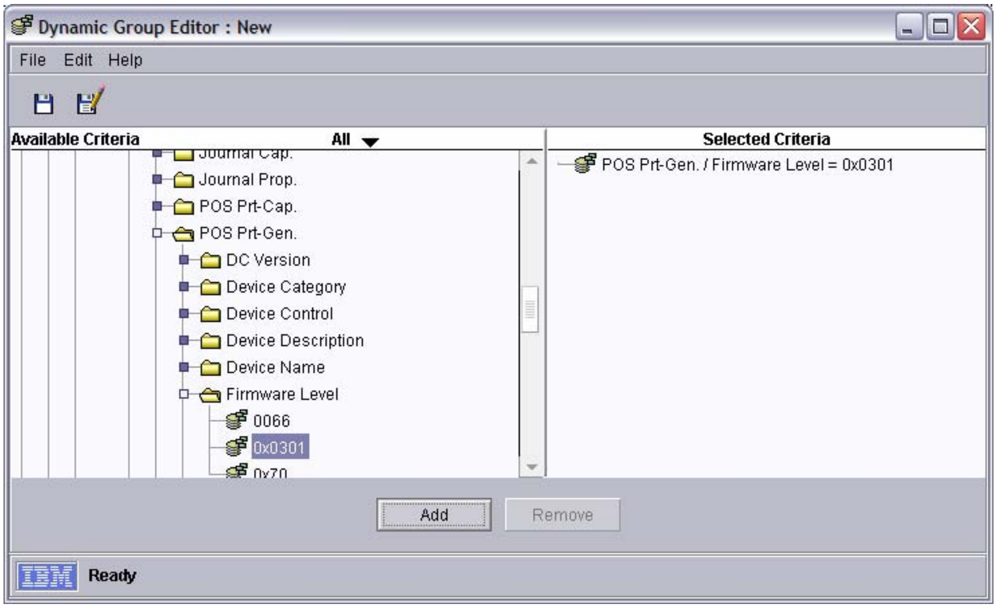
    - Manually view inventory for the system, and check the firmware field for the printer:



Query Results: General Properties(1)

Ver...	Device Control (POS Prt-Gen.)	DC Ver...	Serial Nu...	Inte...	Firmware Level ...	Pow
43	JavaPOS POSPrinter Device Control	1009006	41-LWHBH	USB	0x0301	Onl

    - Or, you could create a “dynamic group” to show ALL printers in your environment that are at the current firmware level:



POS Prt-Gen. / Firmware Level = 0x0301

- Finally, you could use inventory alerts to automatically alert you when the firmware version matches the expected value. (See “**Chapter 5 – RMA/Director Basics**”.)

Example: “Paper Low” Sensor for 4610-2CR / 2NR

This example shows you how to monitor the “paper low” sensor for the 4610-2CR or 2NR printer.

Since this example is a peripheral management example, we’ll assume you already know how to use resource monitors and event management in general. (If not, read “**Chapter 7 – Resource Monitoring**” or “**Chapter 6 – Event Management**” before following this example.)

Instructions (for Windows):

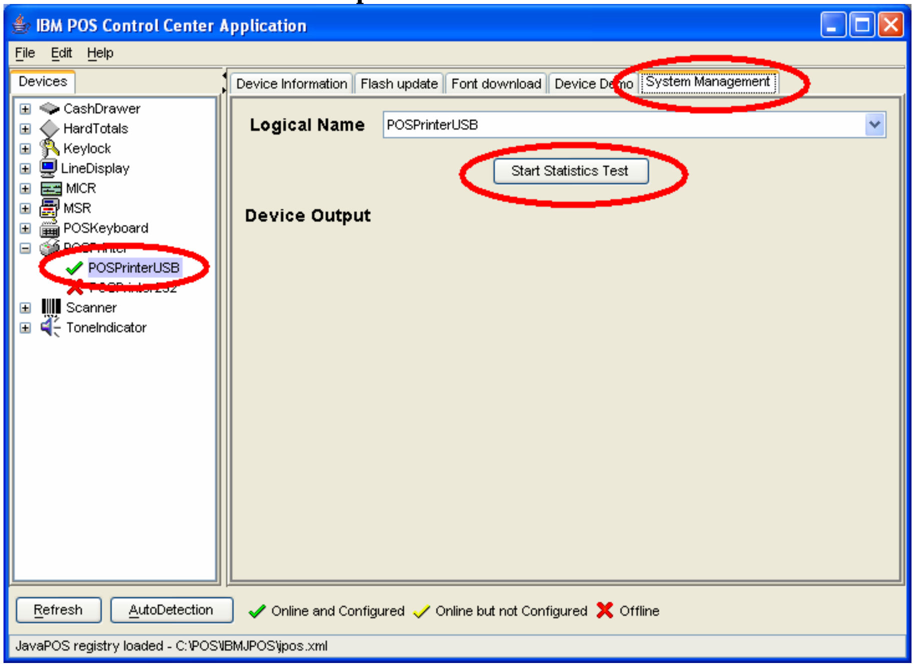
1. Make sure JavaPOS is installed with systems management enabled, at the 1.9.6b version or higher.

2. Configure your jpos.xml to include the POS printer.

3. Open the POS Control Center with the systems management plug-in, and verify that your POS printer appears on the left-hand side of the screen with a green check mark (indicating it is configured correctly and online).

4. Select the printer on the left, then click on the “Systems Management” tab on the right.

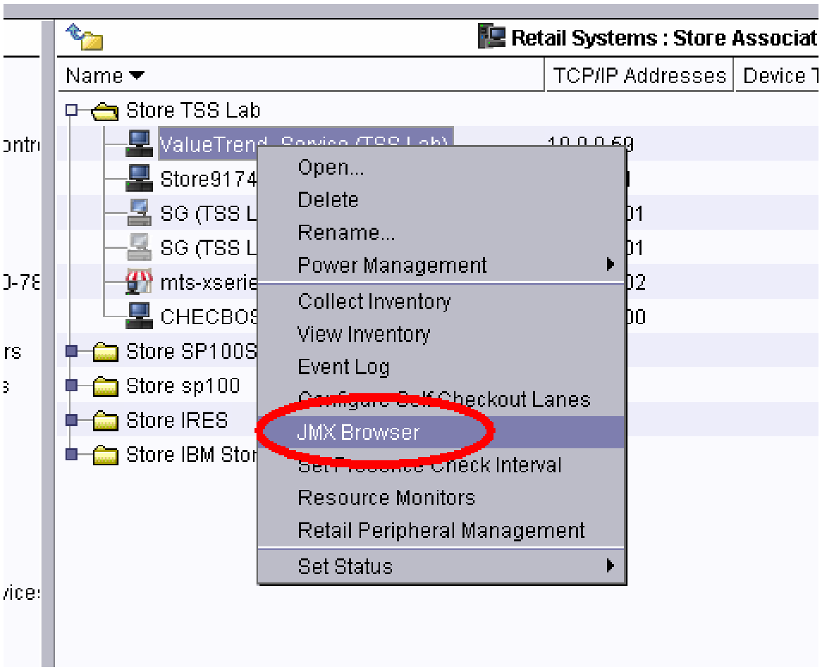
5. Click “Start Statistics Test” to **open/claim/enable** the device.



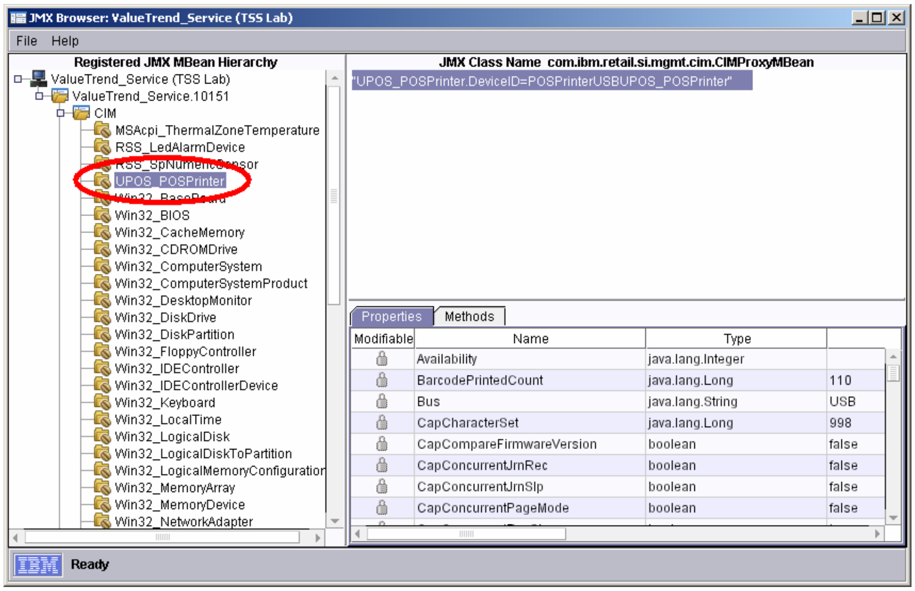
JavaPOS registry loaded - C:\POS\IBMJPOS\jpos.xml

Note: Do not stop the statistics test (i.e. don’t click on “Stop Statistics Test”). Leave the printer opened/claimed/enabled while you proceed with the rest of these steps.

6. Log in to IBM Director, and open the JMX Browser for the system to which the printer is attached.



7. Locate the UPOS_PosPrinter MBean to verify the printer is visible with RMA/Director.

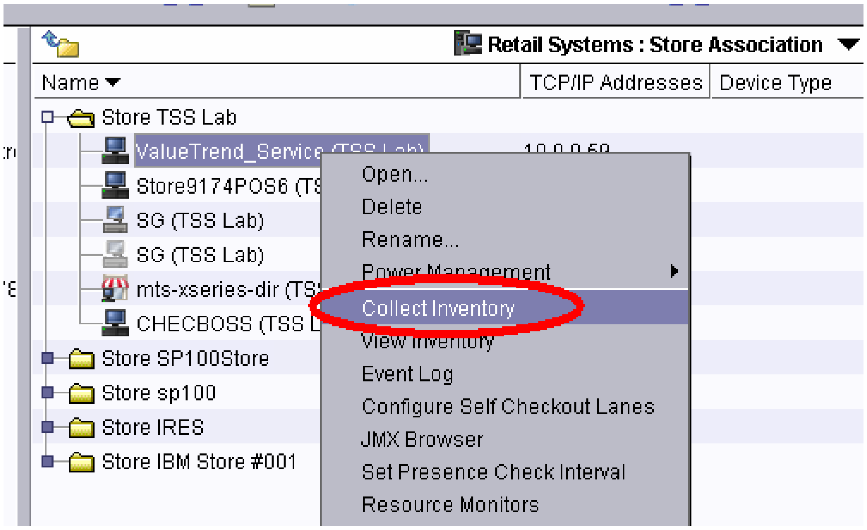


JMX Class Name com.ibm.retail.si.mgmt.cim.CIMProxyMBean

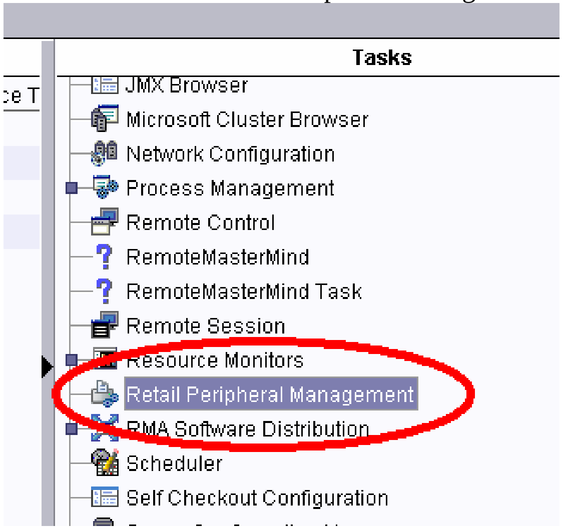
"UPOS_POSPrinter.DeviceID=POSPrinterUSBUPOS_POSPrinter"

Modifiable	Name	Type	
🔒	Availability	java.lang.Integer	
🔒	BarcodePrintedCount	java.lang.Long	110
🔒	Bus	java.lang.String	USB
🔒	CapCharacterSet	java.lang.Long	998
🔒	CapCompareFirmwareVersion	boolean	false
🔒	CapConcurrentJrnRec	boolean	false
🔒	CapConcurrentJrnSlp	boolean	false
🔒	CapConcurrentPageMode	boolean	false

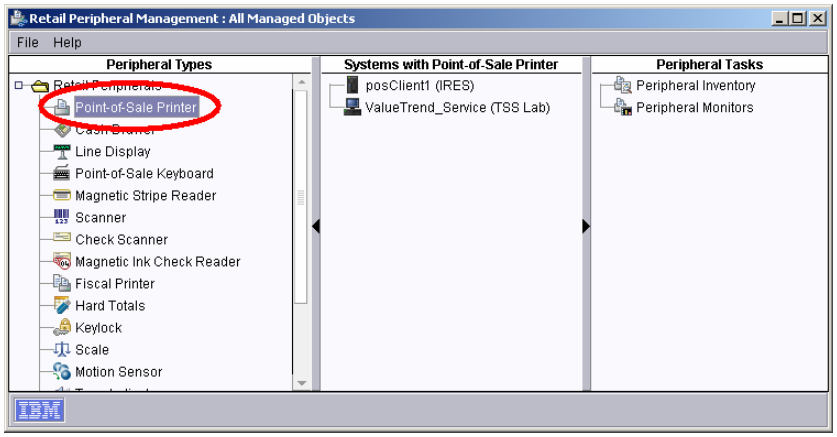
8. Close the JMX Browser, then collect inventory for the system.



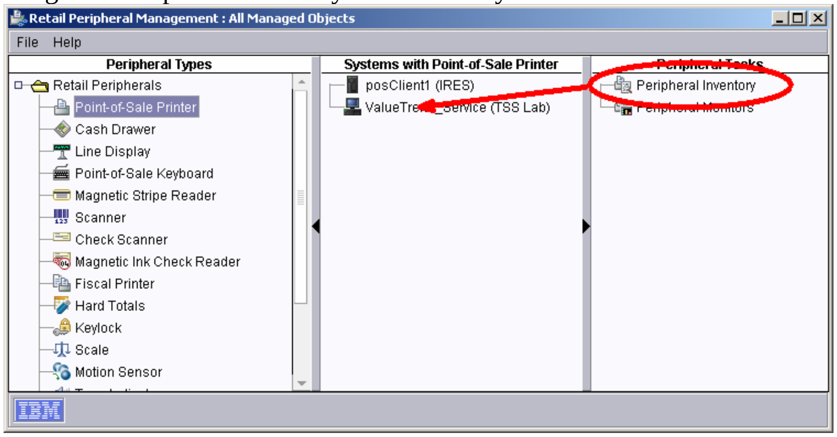
9. Double-click the "Retail Peripheral Management" task in Director.



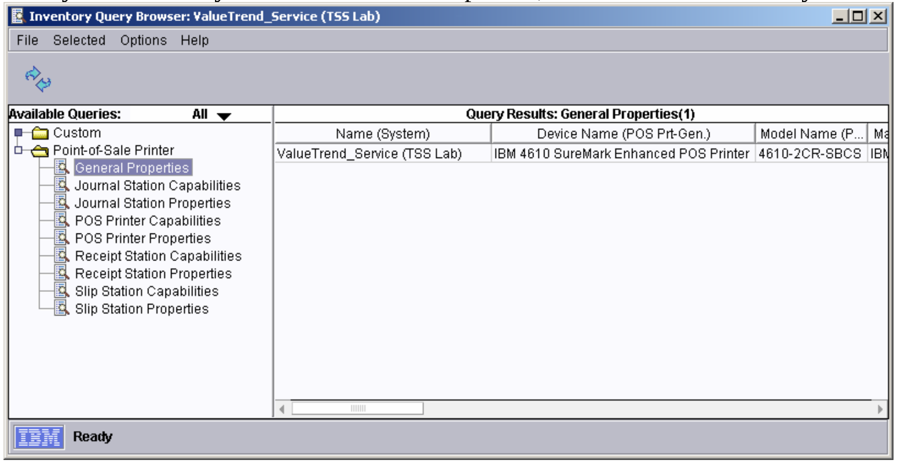
10. Click on "Point-of-Sale Printer" and verify your system appears in the middle section of the screen.



11. Drag the “Peripheral Inventory” task to the system.

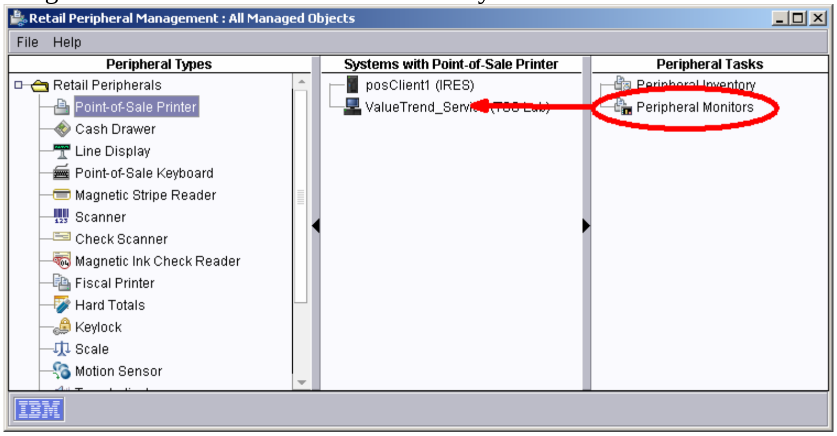


12. Verify the inventory looks correct for the printer, then close the inventory browser.

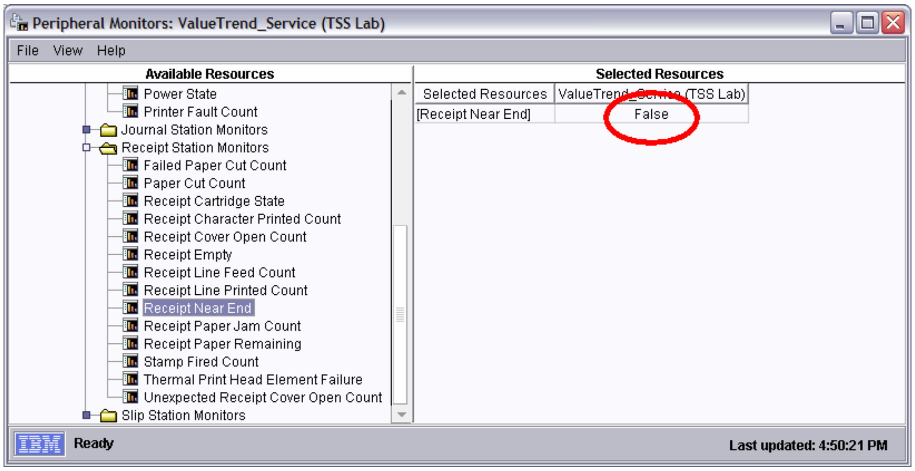

Inventory Query Browser: ValueTrend_Service (TSS Lab)
File
Selected
Options
Help
Available Queries:
All
Custom
Point-of-Sale Printer
General Properties
Journal Station Capabilities
Journal Station Properties
POS Printer Capabilities
POS Printer Properties
Receipt Station Capabilities
Receipt Station Properties
Slip Station Capabilities
Slip Station Properties
Query Results: General Properties(1)
IBM
Ready

Name (System)	Device Name (POS Prt-Gen.)	Model Name (P...	Ma
ValueTrend_Service (TSS Lab)	IBM 4610 SureMark Enhanced POS Printer	4610-2CR-SBCS	IBI

13. Drag the “Resource Monitors” task to the system.

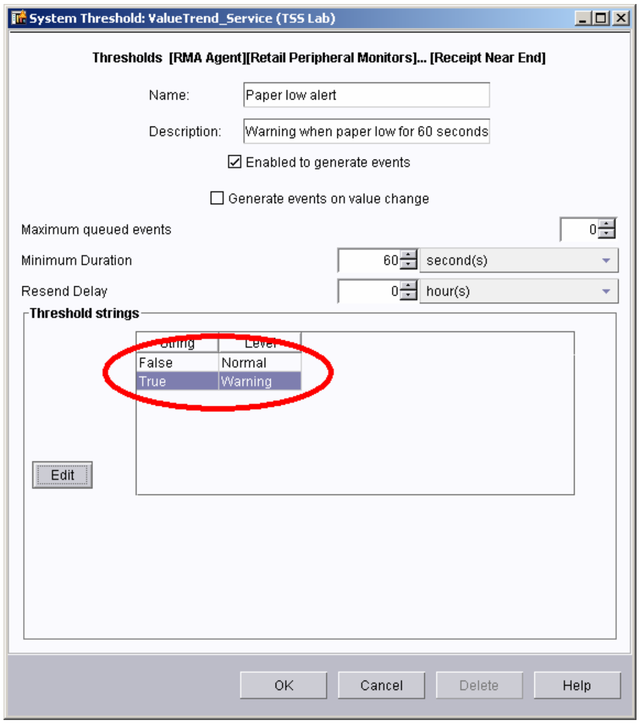


14. Navigate to “Receipt Station Monitors / Receipt Near End” in Resource Monitors. Double-click the value and verify that it reads “false” on the right-hand side of the screen.



Selected Resources	ValueTrend_Service (TSS Lab)
[Receipt Near End]	False

15. Create a threshold to send a “Warning” event when the value changes to “true”.



System Threshold: ValueTrend_Service (TSS Lab)

Thresholds [RMA Agent][Retail Peripheral Monitors]... [Receipt Near End]

Name: Paper low alert

Description: Warning when paper low for 60 seconds

☑ Enabled to generate events

□ Generate events on value change

Maximum queued events: 0

Minimum Duration: 60 second(s)

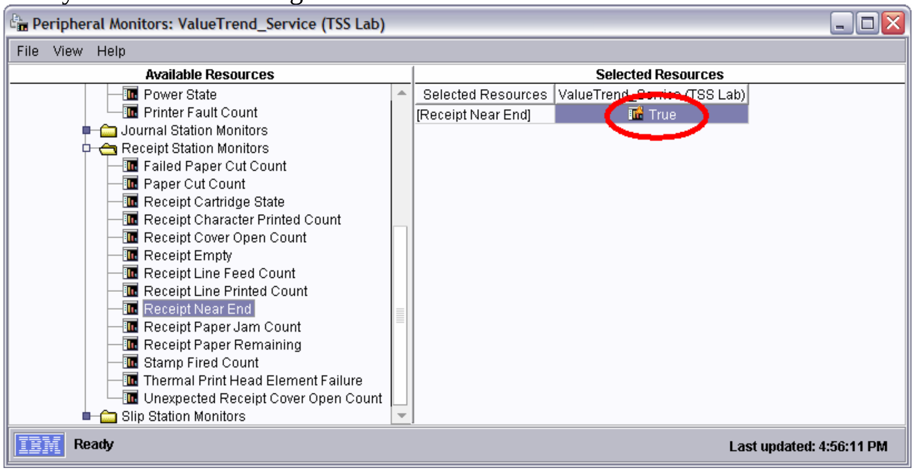
Resend Delay: 0 hour(s)

Threshold strings

String	Level
False	Normal
True	Warning

16. Open the printer cover, and remove the roll of paper (which should be a somewhat new roll of paper with plenty of paper remaining). Then replace the roll of paper with a roll of paper that is almost empty. (i.e. The paper roll should already be showing the red markings that indicate it's almost gone.) This triggers the "paper low" scenario.

17. Verify that the value changed to "True" in the resource monitors UI.



Peripheral Monitors: ValueTrend_Service (TSS Lab)

Available Resources

- Power State
- Printer Fault Count
- Journal Station Monitors
- Receipt Station Monitors
  - Failed Paper Cut Count
  - Paper Cut Count
  - Receipt Cartridge State
  - Receipt Character Printed Count
  - Receipt Cover Open Count
  - Receipt Empty
  - Receipt Line Feed Count
  - Receipt Line Printed Count
  - Receipt Near End
  - Receipt Paper Jam Count
  - Receipt Paper Remaining
  - Stamp Fired Count
  - Thermal Print Head Element Failure
  - Unexpected Receipt Cover Open Count
- Slip Station Monitors

Selected Resources

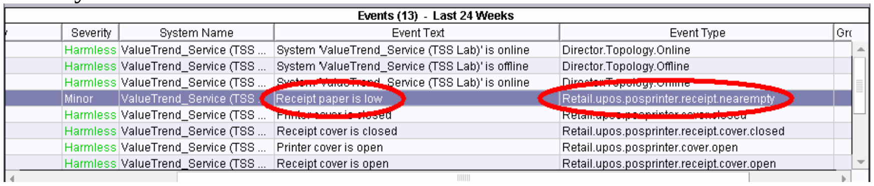
Selected Resources	ValueTrend_Service (TSS Lab)
[Receipt Near End]	True

Ready

Last updated: 4:56:11 PM

18. Go back to the main Director console (i.e. close the peripheral management and resource monitor windows), and view the event log for the device. You should see 2 different events:

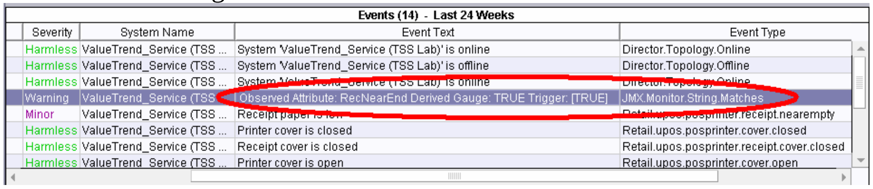
    - The “Retail.upos.posprinter.receipt.nearempty” event that was forwarded directly from the UPOS drivers:



Events (13) - Last 24 Weeks

Severity	System Name	Event Text	Event Type	Grc
Harmless	ValueTrend_Service (TSS ...	System 'ValueTrend_Service (TSS Lab)' is online	Director.Topology.Online	
Harmless	ValueTrend_Service (TSS ...	System 'ValueTrend_Service (TSS Lab)' is offline	Director.Topology.Offline	
Harmless	ValueTrend_Service (TSS ...	System 'ValueTrend_Service (TSS Lab)' is online	Director.Topology.Online	
Minor	ValueTrend_Service (TSS ...	Receipt paper is low	Retail.upos.posprinter.receipt.nearempty	
Harmless	ValueTrend_Service (TSS ...	Printer cover is closed	Retail.upos.posprinter.cover.closed	
Harmless	ValueTrend_Service (TSS ...	Receipt cover is closed	Retail.upos.posprinter.receipt.cover.closed	
Harmless	ValueTrend_Service (TSS ...	Printer cover is open	Retail.upos.posprinter.cover.open	
Harmless	ValueTrend_Service (TSS ...	Receipt cover is open	Retail.upos.posprinter.receipt.cover.open	

    - The “JMX.Monitor.String.Matches” event that was generated by your resource monitoring threshold:



Events (14) - Last 24 Weeks

Severity	System Name	Event Text	Event Type
Harmless	ValueTrend_Service (TSS ...	System 'ValueTrend_Service (TSS Lab)' is online	Director.Topology.Online
Harmless	ValueTrend_Service (TSS ...	System 'ValueTrend_Service (TSS Lab)' is offline	Director.Topology.Offline
Harmless	ValueTrend_Service (TSS ...	System 'ValueTrend_Service (TSS Lab)' is online	Director.Topology.Online
Warning	ValueTrend_Service (TSS ...	Observed Attribute: RecNearEnd Derived Gauge: TRUE Trigger: [TRUE]	JMX.Monitor.String.Matches
Minor	ValueTrend_Service (TSS ...	Receipt paper is low	Retail.upos.posprinter.receipt.nearempty
Harmless	ValueTrend_Service (TSS ...	Printer cover is closed	Retail.upos.posprinter.cover.closed
Harmless	ValueTrend_Service (TSS ...	Receipt cover is closed	Retail.upos.posprinter.receipt.cover.closed
Harmless	ValueTrend_Service (TSS ...	Printer cover is open	Retail.upos.posprinter.cover.open

19. You can now create a filter for either one of these two events, then test your filter, and/or create an event action plan to handle the event according to your needs. (See “**Chapter 6 – Event Management**” for more details on this step.)

Chapter 10 – Power Management

Retailers are becoming more and more energy conscious and one of the areas they have defined as an opportunity to reduce energy consumption and lower costs is through Power Management of Point of Sale (POS). The IBM Director console provides a unique Power Management interface to remotely manage the power management schemes for RMA agents. Through the Director Console you have the ability to schedule an enterprise Power Off, Restart, Power On (Wake On LAN), and Suspend of your systems.

This chapter explains what platforms and agents are supported and how to manage Power Management using IBM Director and RMA. It teaches you how to invoke a Power Off, Power On, Suspend, and Restart of a single system. It will also teach you how to use the IBM Director Scheduler to define a "Store Close" and "Store Open" for your systems.

Introduction to Power Management

There are several different ways to manage power of POS devices using RMA and IBM Director.

1. Shutdown and Power Off ("S5"). Off. The hardware is completely off, the operating system has shut down; nothing has been saved. Requires a complete reboot to return to the working state. The typical power consumption when a system is power off is 2W.

2. Restart. This reboots the operating system on the target system.

3. Suspend ("Deep Sleep"). The System Appears off, the CPU has no power, RAM is in slow refresh and the power supply is in a reduced power mode. In "Deep Sleep" mode the typical power consumption is 3W.

4. Power On ("Wake On LAN / WOL"). Wake on LAN (WOL) is a technology that allows a network professional to remotely power on a computer or to wake it up from "Deep Sleep" mode. By remotely triggering the computer to wake up and perform scheduled maintenance tasks, the technician does not have to physically visit each computer on the network.

The following table summarizes the power management capabilities of RMA on the various platforms:

Agent	Shutdown and Power Off [1]	Restart[1]	Power On[2 3] WOL	Suspend
Linux GA, Linux Kiosk GA	Yes	Yes	Yes	No
Windows GA,	Yes	Yes	Yes	Yes[4]

Windows Kiosk GA, SCS Lane				
Windows MA, Linux MA, 4690 Controller MA	No[5]	Yes[5]	No[5]	No[5]
4690 Controller GA	Yes	Yes	No	No
4690 Terminal	Yes[6]	Yes[6]	Yes[6,7]	Yes[6,8]

Notes:

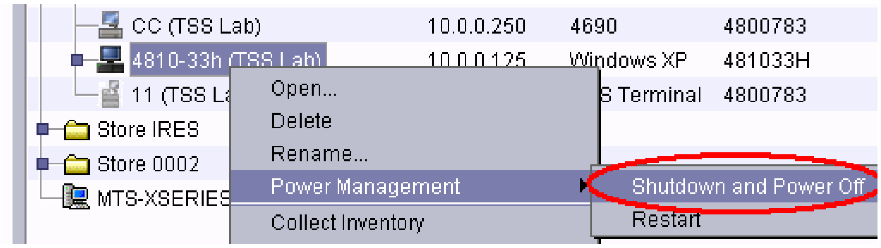
- 1 – Shutdown and Power Off and Restart are available when the managed object is online.
- 2 – Power On (Wake on LAN) is available when the managed object is offline.
- 3 – Power On (Wake on LAN) functionality requires that system BIOS and network settings are configured properly to support Wake On LAN.
- 4 – The hardware model has to support "Deep Sleep", the BIOS has to be enabled for S3, and the NIC needs to configured to wake a system out of suspend mode.
- 5 – If the in-store Master Agent is powered off, all communication is lost with the other agents in the store.
- 6 – Refer to the 4690 publications for the situations in which power management is supported on a terminal.
- 7 – Power On is only available for 4690 Enhanced Terminals running version V6R2 or later
- 8 – Suspend is only available for terminals running version V6R2 or later

> **Note**: This document assumes that the UPOS drivers (if used) are at the 1.9.6b version or higher – older UPOS driver versions do not have power management support for Retail Peripherals.

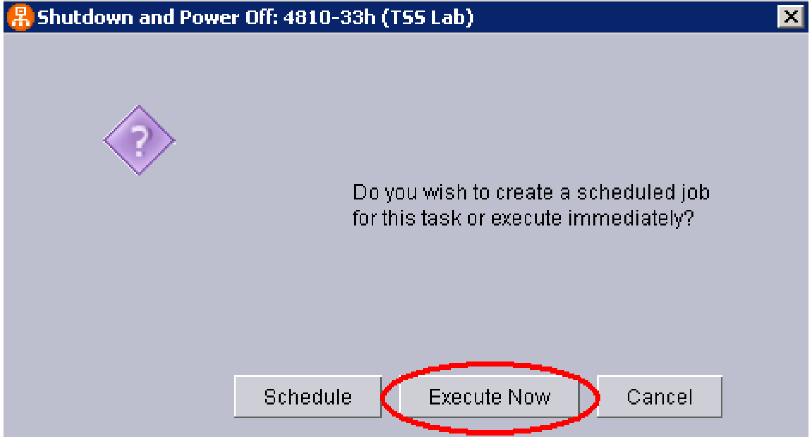
The instructions below will help you plan, install, configure, and effectively use the power management capabilities of the RMA and IBM Director solution.

Example: Shutdown and Power Off a Single System

1. Right-click on a system, select "Power Management", and select "Shutdown and Power Off".

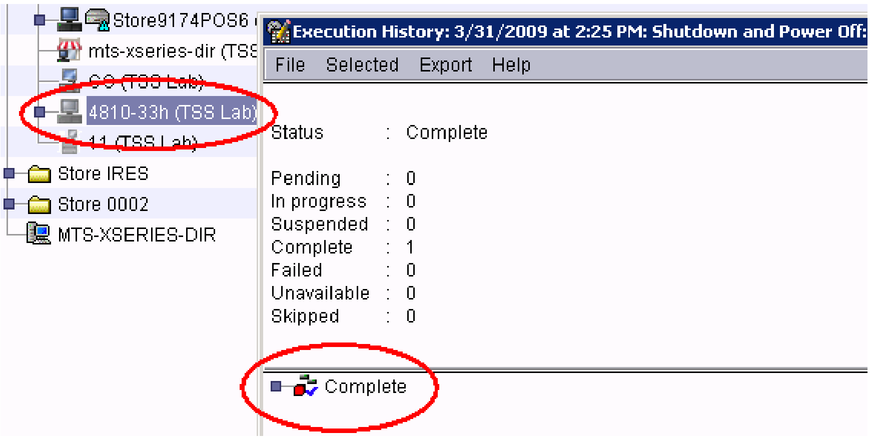


2. Select “Execute Now”, the Execution History will show Completed, and the device will go offline.



Shutdown and Power Off: 4810-33h (TSS Lab)

Do you wish to create a scheduled job for this task or execute immediately?



Execution History: 3/31/2009 at 2:25 PM: Shutdown and Power Off:

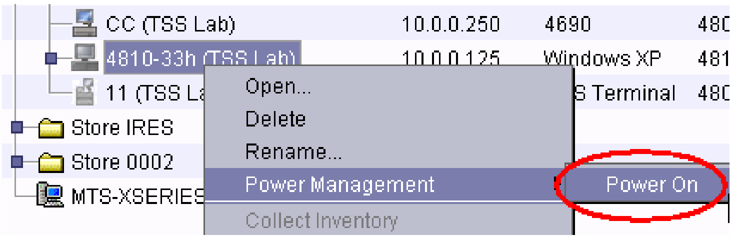
```
Status       :  Complete

Pending      :  0
In progress  :  0
Suspended    :  0
Complete     :  1
Failed       :  0
Unavailable  :  0
Skipped      :  0
```

Complete

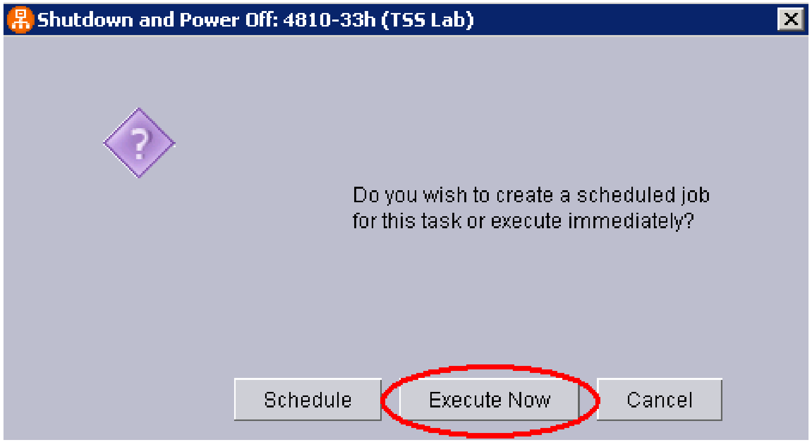
Example: Power On “Wake On LAN” a Single System

Note: In order for RMA to have the ability to Power On a system, the systems BIOS has be enabled for “Wake On LAN”. Refer to hardware user guide for instructions on how to enable ‘Wake On LAN” for each hardware platform.

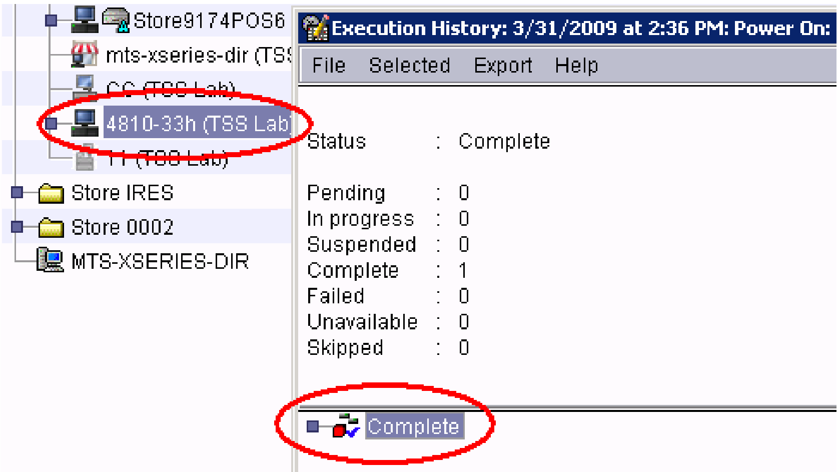
1. Right-click on a powered off system select “Power Management”, and select “Power On”.


CC (TSS Lab) 10.0.0.250 4690 480
4810-33h (TSS Lab) 10.0.0.125 Windows XP 481
11 (TSS La… S Terminal 480
Store IRES
Store 0002
MTS-XSERIES
Open...
Delete
Rename...
Power Management
Collect Inventory
Power On

2. Select “Execute Now”, the Execution History will show Completed, and the device will come online.



Do you wish to create a scheduled job for this task or execute immediately?



Status : Complete

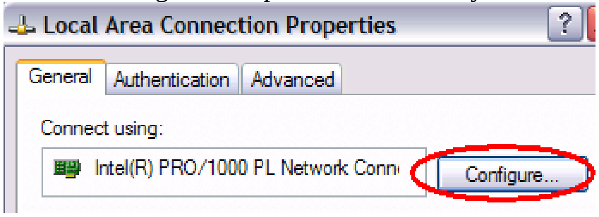
Pending : 0
In progress : 0
Suspended : 0
Complete : 1
Failed : 0
Unavailable : 0
Skipped : 0

Example: Suspend “Deep Sleep” a Single System

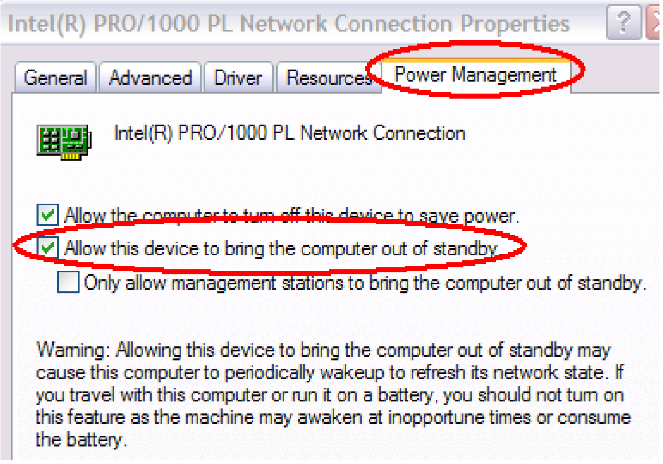
Note: This example is only possible using RMA 2.5 or higher! On 2.4 and lower, it’s not possible to suspend a remote system.

Note: In order for RMA to have the ability to suspend a system, the hardware platform has be support "Deep Sleep", the systems BIOS has be enabled for "S3", and the NIC has to be enabled to bring the system out of suspend mode. Refer to hardware user guide for instructions on how to enable 'S3" for each hardware platform.

1. Verify the NIC card is enabled to bring the system out of suspend, by opening Network Connections, go to the Properties of the NIC, click the "Configure" button, select the "Power Management" tab, and verify the check box "Allow the device to bring the computer out of standby" is checked.



Connect using:
Intel(R) PRO/1000 PL Network Conn

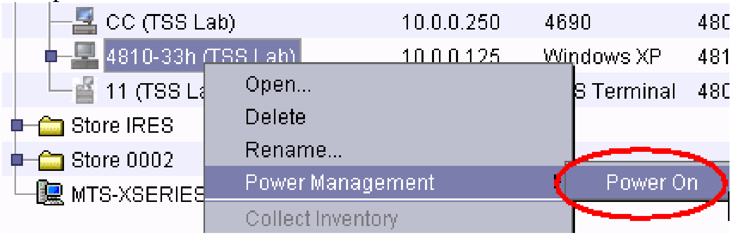


Intel(R) PRO/1000 PL Network Connection

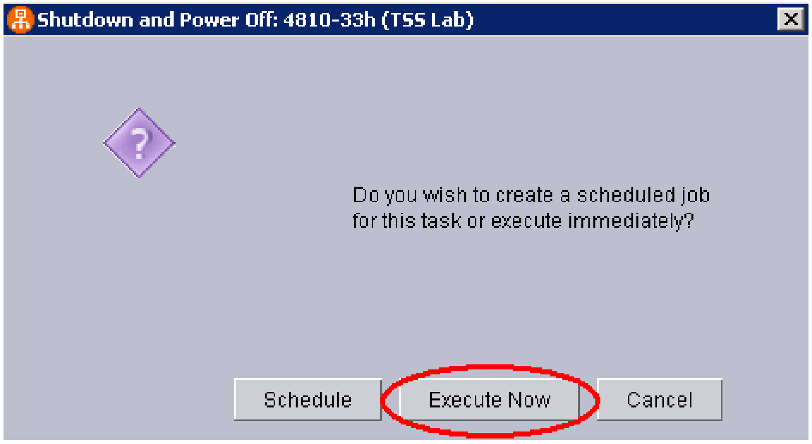
☑ Allow the computer to turn off this device to save power.
☑ Allow this device to bring the computer out of standby.
□ Only allow management stations to bring the computer out of standby.

Warning: Allowing this device to bring the computer out of standby may cause this computer to periodically wakeup to refresh its network state. If you travel with this computer or run it on a battery, you should not turn on this feature as the machine may awaken at inopportune times or consume the battery.

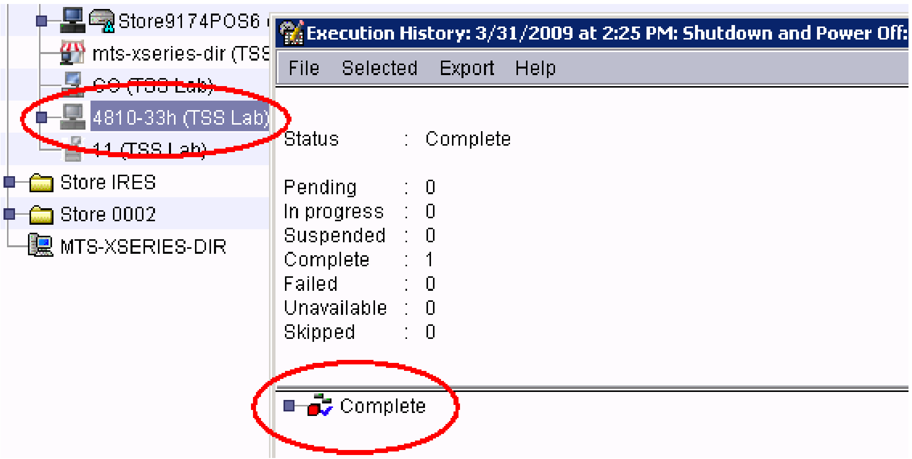
2. Right-click on a powered off system select "Power Management", and select "Suspend".



3. Select “Execute Now”, the Execution History will show Completed, and the device will come online.



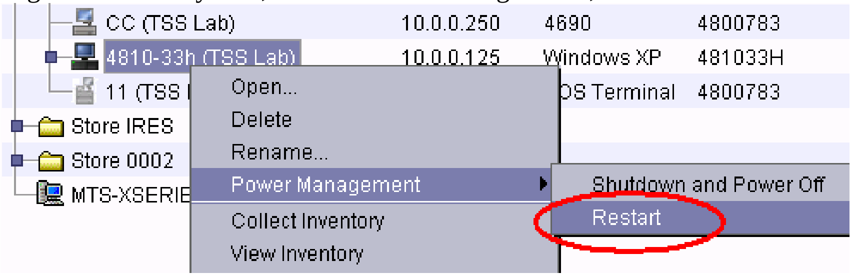
Do you wish to create a scheduled job for this task or execute immediately?



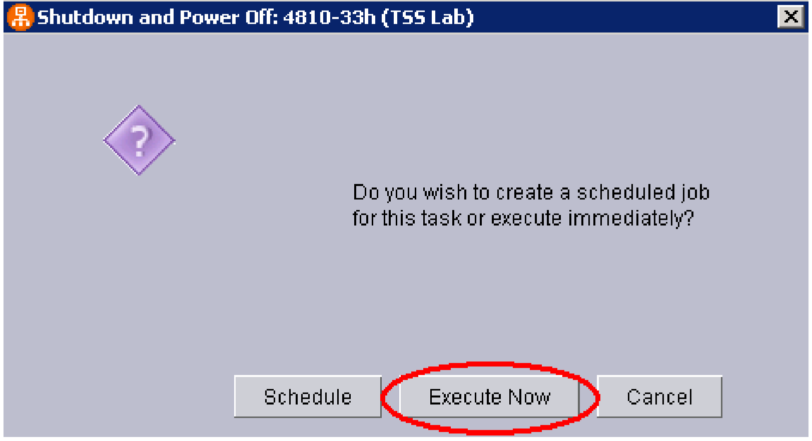
```
Status       :  Complete

Pending      :  0
In progress  :  0
Suspended    :  0
Complete     :  1
Failed       :  0
Unavailable  :  0
Skipped      :  0
```

Example: Restart a Single System

1. Right-click on a system, select “Power Management”, and select “Restart”.

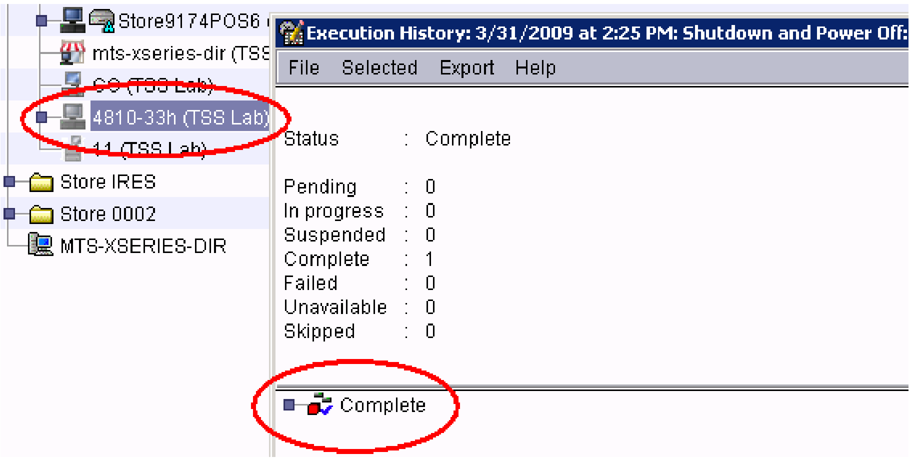


2. Select “Execute Now”, the Execution History will show Completed, and the device will go offline.



Shutdown and Power Off: 4810-33h (TSS Lab)

Do you wish to create a scheduled job for this task or execute immediately?



Execution History: 3/31/2009 at 2:25 PM: Shutdown and Power Off:

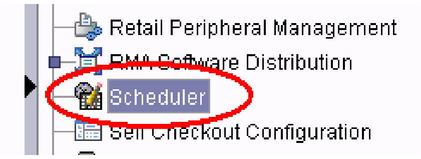
```
Status       :  Complete

Pending      :  0
In progress  :  0
Suspended    :  0
Complete     :  1
Failed       :  0
Unavailable  :  0
Skipped      :  0
```

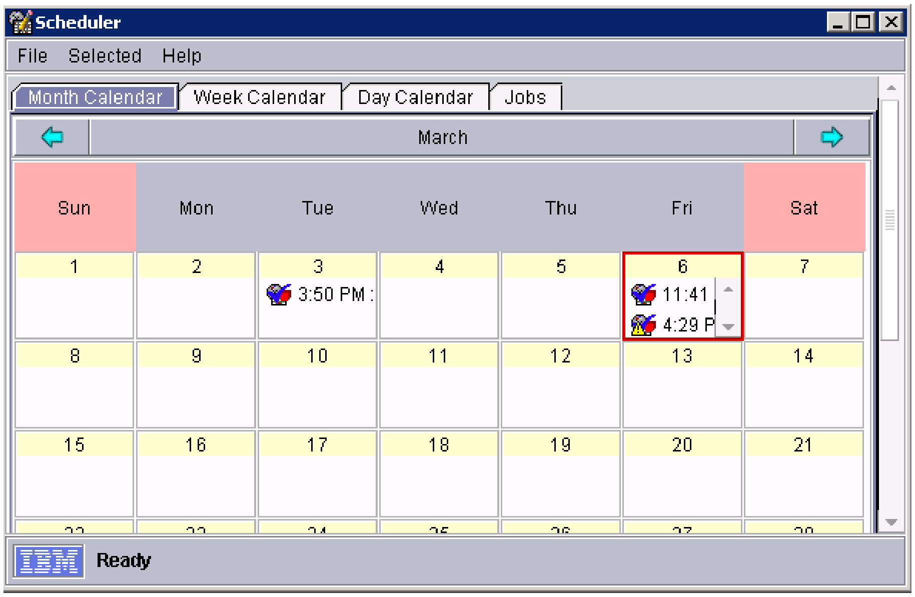
Example: Schedule a “Store Close” and “Store Open” Power Policy

Most customers are interested in scheduling an enterprise wide shutdown and power on of systems for the closing and opening of a store day. Using the IBM Director Scheduler you can schedule a Power Off and Power On systems for a specific time. This example is provides the steps for configuring a scheduled “Store Close” and “Store Open” Power Policy.

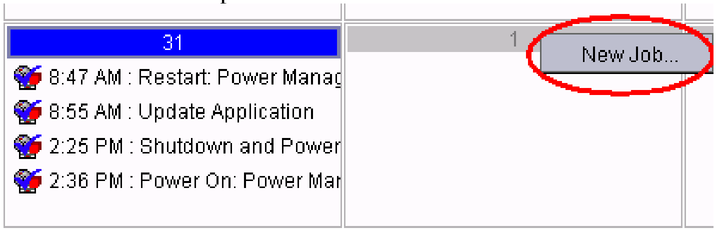
Store Close “Power Off” Example:

1. Double-click on the Scheduler from the Task Pane, the Scheduler will open.

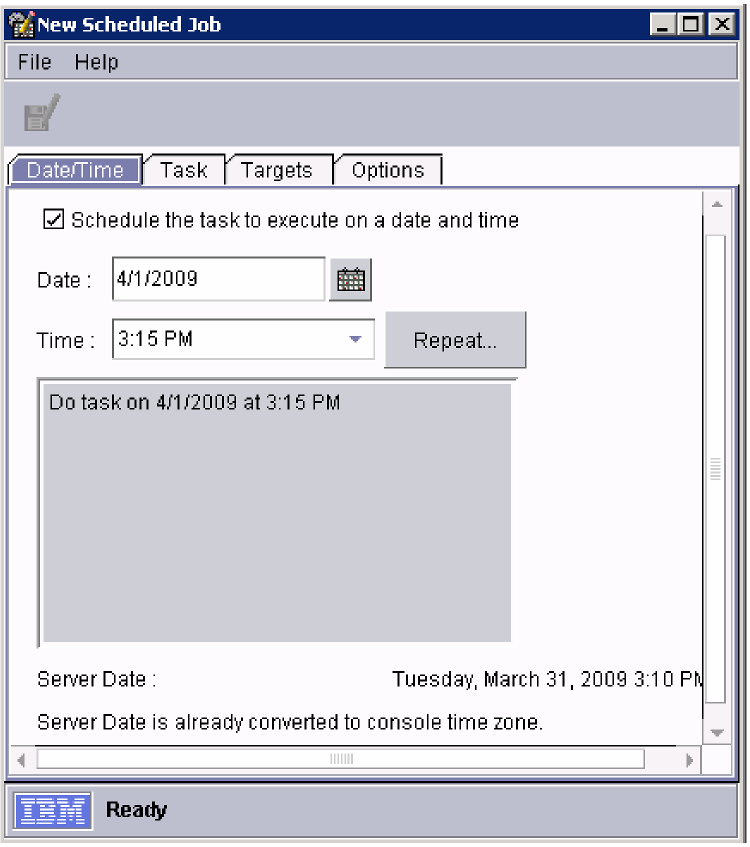

Retail Peripheral Management
RMA Software Distribution
Scheduler
Self Checkout Configuration



2. Right-click on a date in the Scheduler and select "New Job" and "New Scheduled Job" window will open.



8:47 AM : Restart: Power Manag
8:55 AM : Update Application
2:25 PM : Shutdown and Power
2:36 PM : Power On: Power Mar



☑ Schedule the task to execute on a date and time

Date : 4/1/2009

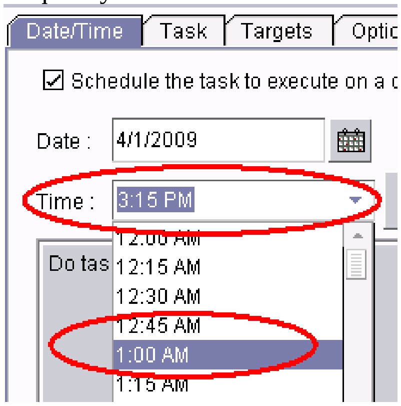
Time : 3:15 PM

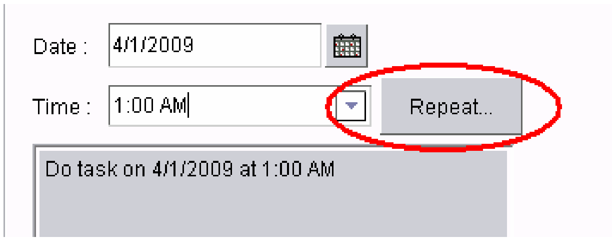
Do task on 4/1/2009 at 3:15 PM

Server Date : Tuesday, March 31, 2009 3:10 PM

Server Date is already converted to console time zone.

3. Select the "Time" drop down box to select the time you want to schedule a Power Off of your store systems, and the select the "Repeat" button to define the frequency of the Power Off.



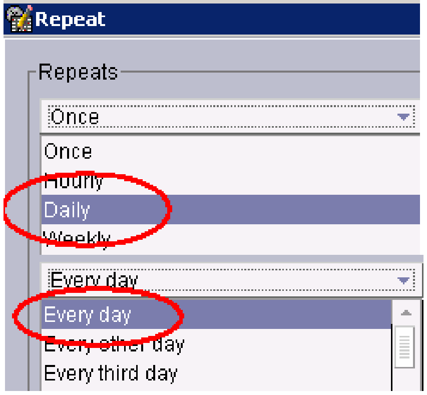


Date : 4/1/2009

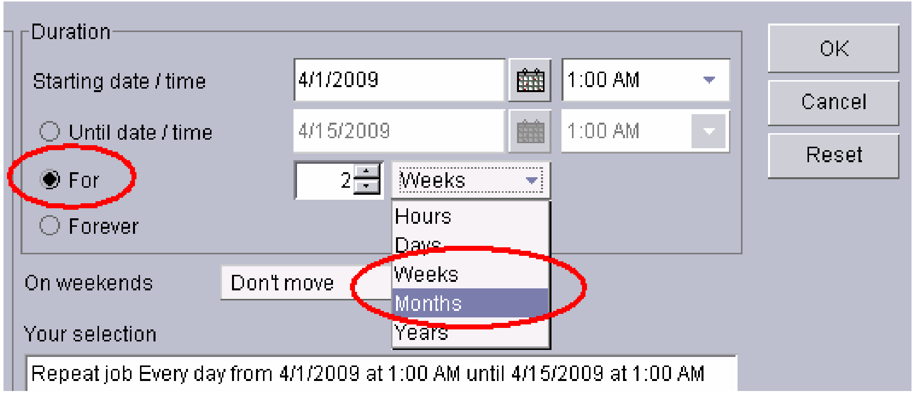
Time : 1:00 AM

Do task on 4/1/2009 at 1:00 AM

4. Select the “Repeats” drop down box, select “Daily”, select the second “Repeats” drop down box and select “Every day”.



5. Configure the Duration fields by selecting the “For” radio button, selecting “Months” from the drop down list, and selecting “Don’t move” for the “On Weekends” field, then select OK.



Duration

Starting date / time 4/1/2009 1:00 AM

○ Until date / time 4/15/2009 1:00 AM

● For 2 Weeks

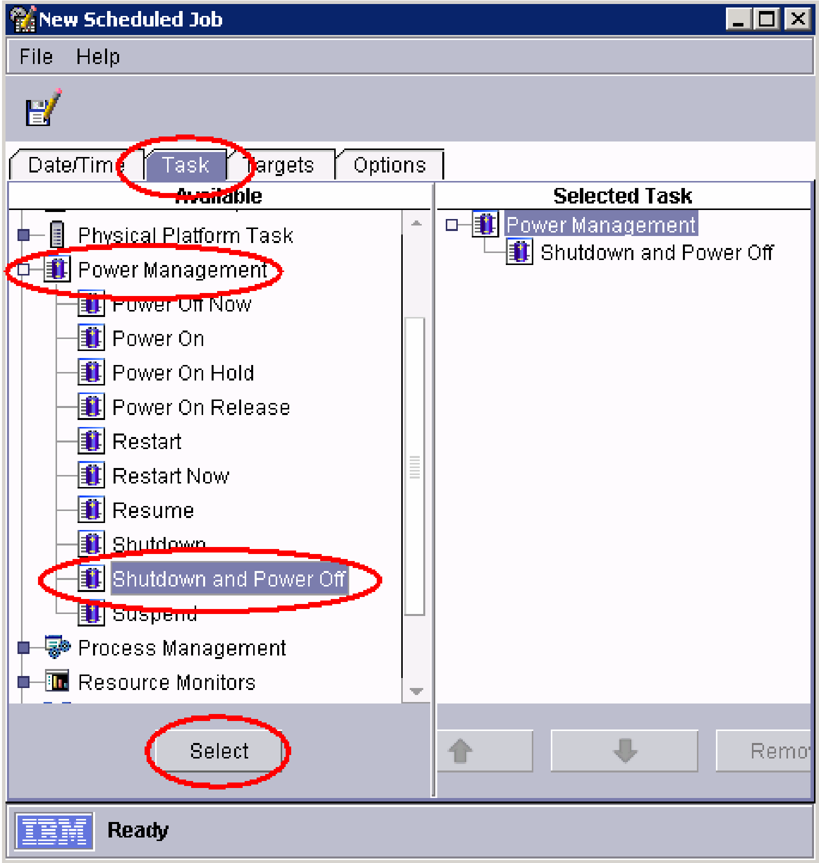
○ Forever

On weekends Don't move

Your selection

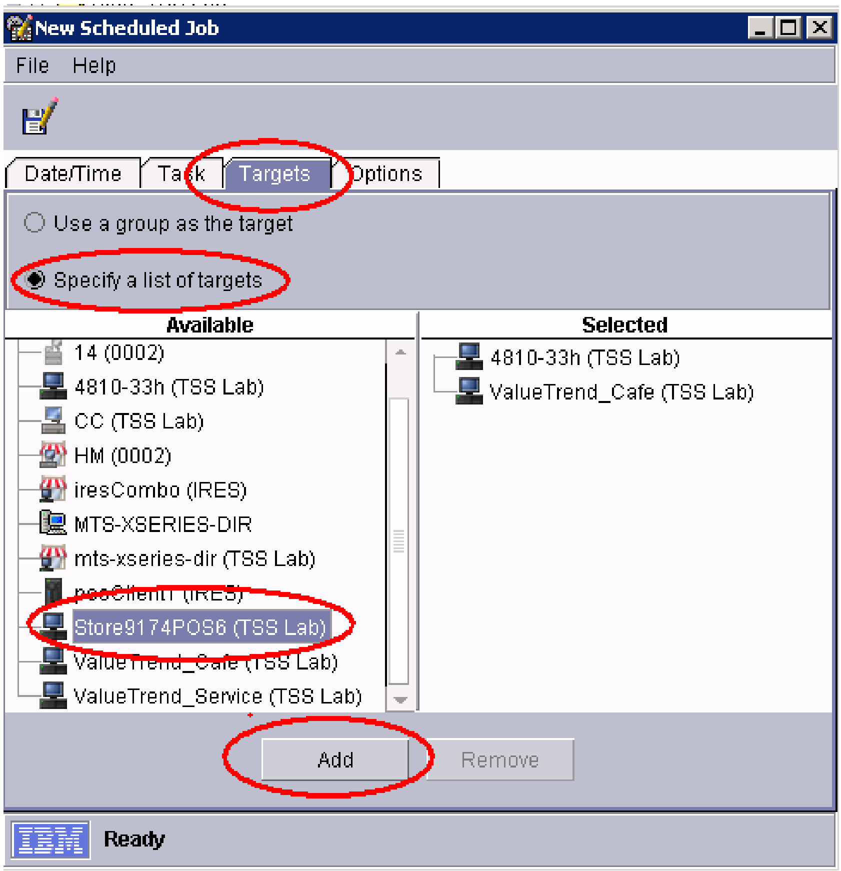
Repeat job Every day from 4/1/2009 at 1:00 AM until 4/15/2009 at 1:00 AM

6. On the New Schedule window select the “Task” tab, expand the “Power Management” tree, select “Shutdown and Power Off”, click on “Select” button.



7. On the New Schedule window select the “Target” tab, select the “Specify a list of targets” radio button, select the system(s), select the “Add” button.

> **Note:** You can select the “Use a group as the target” radio button to select a group of systems, but remember not all operating systems support a “Power On”, so be sure the group you select does not have systems that can not be woken up.



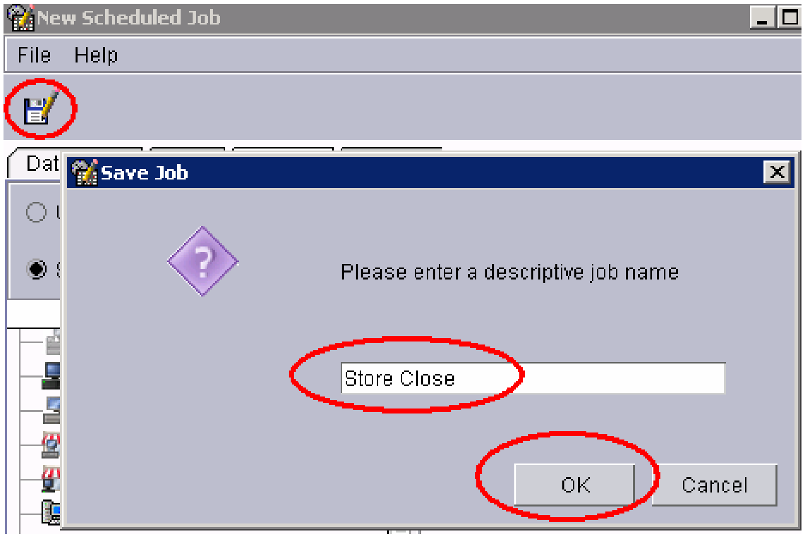
○ Use a group as the target

● Specify a list of targets

Available	Selected
14 (0002)	4810-33h (TSS Lab)
4810-33h (TSS Lab)	ValueTrend_Cafe (TSS Lab)
CC (TSS Lab)	
HM (0002)	
iresCombo (IRES)	
MTS-XSERIES-DIR	
mts-xseries-dir (TSS Lab)	
posClient1 (IRES)	
Store9174POS6 (TSS Lab)	
ValueTrend_Cafe (TSS Lab)	
ValueTrend_Service (TSS Lab)	

Note: In order for RMA to have the ability to Power On a system, the systems BIOS has be enabled for “Wake On LAN”. Refer to hardware user guide for instructions on how to enable ‘Wake On LAN” for each hardware platform.

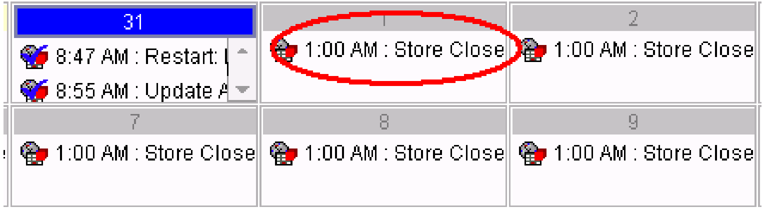
8. Click the “Save As” button, enter a saved job name as “Store Close”, click OK, click OK on the Job Saved message, and then close the New Schedule Job window.



Please enter a descriptive job name

Store Close

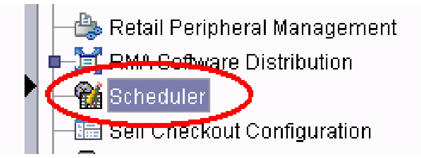
9. The New Schedule Job will appear on the Scheduler.

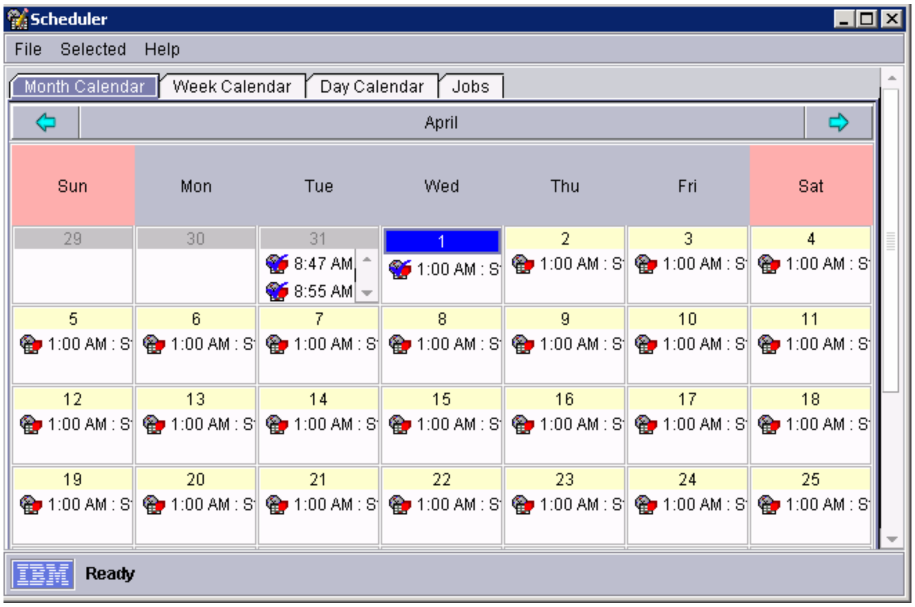


31	1	2
8:47 AM : Restart: I 8:55 AM : Update A	1:00 AM : Store Close	1:00 AM : Store Close
7	8	9
1:00 AM : Store Close	1:00 AM : Store Close	1:00 AM : Store Close

Store Open “Power On” Example:

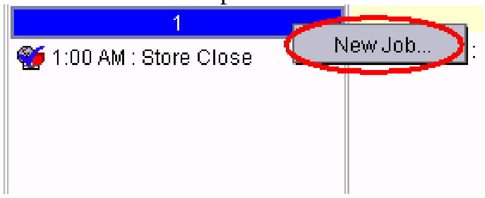
1. Double-click on the Scheduler from the Task Pane, the Scheduler will open.


Retail Peripheral Management
RMA Software Distribution
Scheduler
Self Checkout Configuration

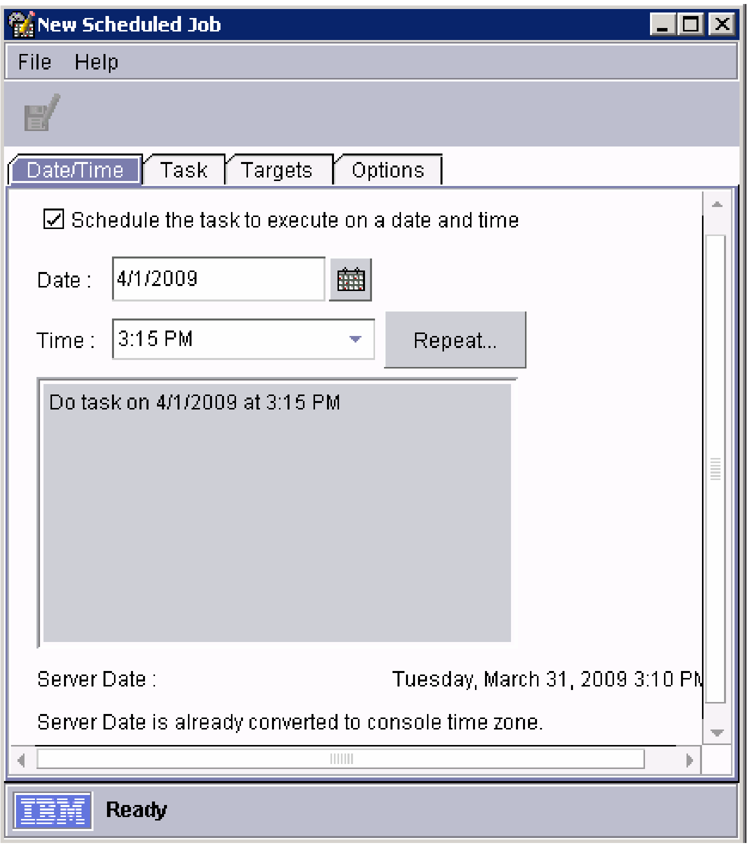


Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31 8:47 AM 8:55 AM	1 1:00 AM : S	2 1:00 AM : S	3 1:00 AM : S	4 1:00 AM : S
5 1:00 AM : S	6 1:00 AM : S	7 1:00 AM : S	8 1:00 AM : S	9 1:00 AM : S	10 1:00 AM : S	11 1:00 AM : S
12 1:00 AM : S	13 1:00 AM : S	14 1:00 AM : S	15 1:00 AM : S	16 1:00 AM : S	17 1:00 AM : S	18 1:00 AM : S
19 1:00 AM : S	20 1:00 AM : S	21 1:00 AM : S	22 1:00 AM : S	23 1:00 AM : S	24 1:00 AM : S	25 1:00 AM : S

2. Right-click on a date in the Scheduler and select “New Job” and “New Scheduled Job” window will open.



1:00 AM : Store Close



New Scheduled Job

☑ Schedule the task to execute on a date and time

Date : 4/1/2009

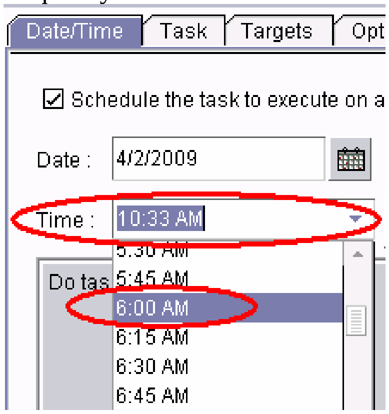
Time : 3:15 PM

Do task on 4/1/2009 at 3:15 PM

Server Date : Tuesday, March 31, 2009 3:10 PM

Server Date is already converted to console time zone.

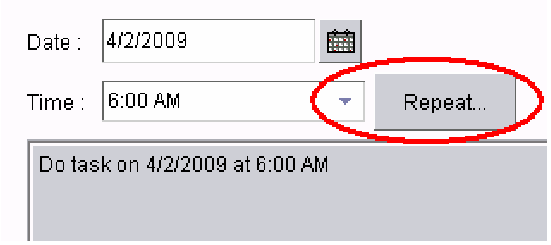
3. Select the “Time” drop down box to select the time you want to schedule a Power Off of your store systems, and the select the “Repeat” button to define the frequency of the Power On.



☑ Schedule the task to execute on a

Date : 4/2/2009

Time : 10:33 AM

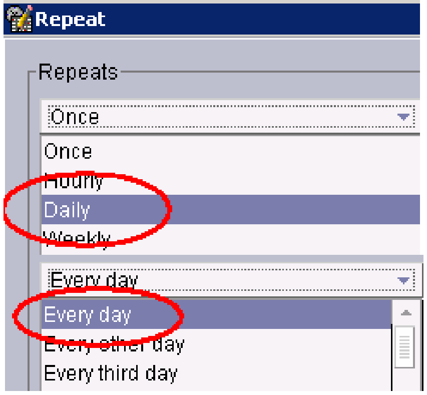


Date : 4/2/2009

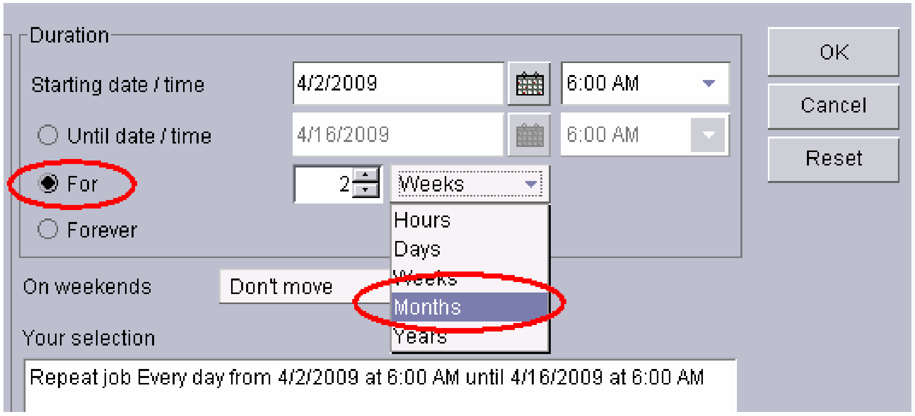
Time : 6:00 AM

Do task on 4/2/2009 at 6:00 AM

4. Select the “Repeats” drop down box, select “Daily”, select the second “Repeats” drop down box and select “Every day”.



5. Configure the Duration fields by selecting the “For” radio button, selecting “Months” from the drop down list, and selecting “Don’t move” for the “On Weekends” field, then select OK.



Duration

Starting date / time 4/2/2009 6:00 AM

○ Until date / time 4/16/2009 6:00 AM

● For 2 Weeks

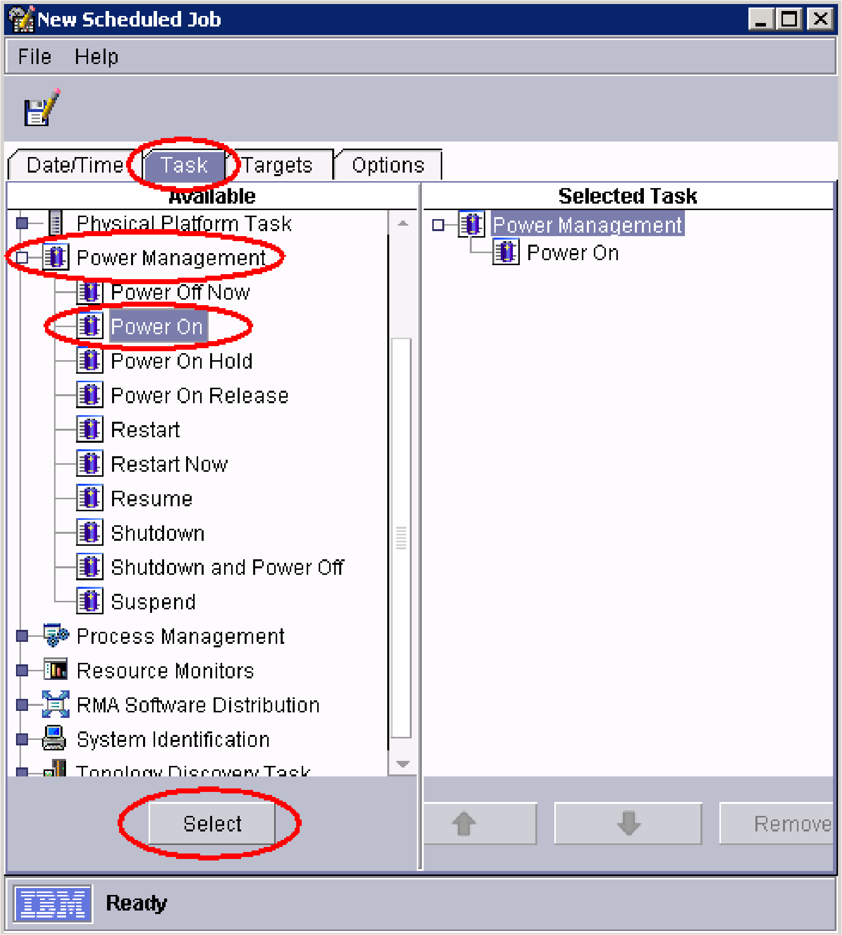
○ Forever

On weekends Don't move

Your selection

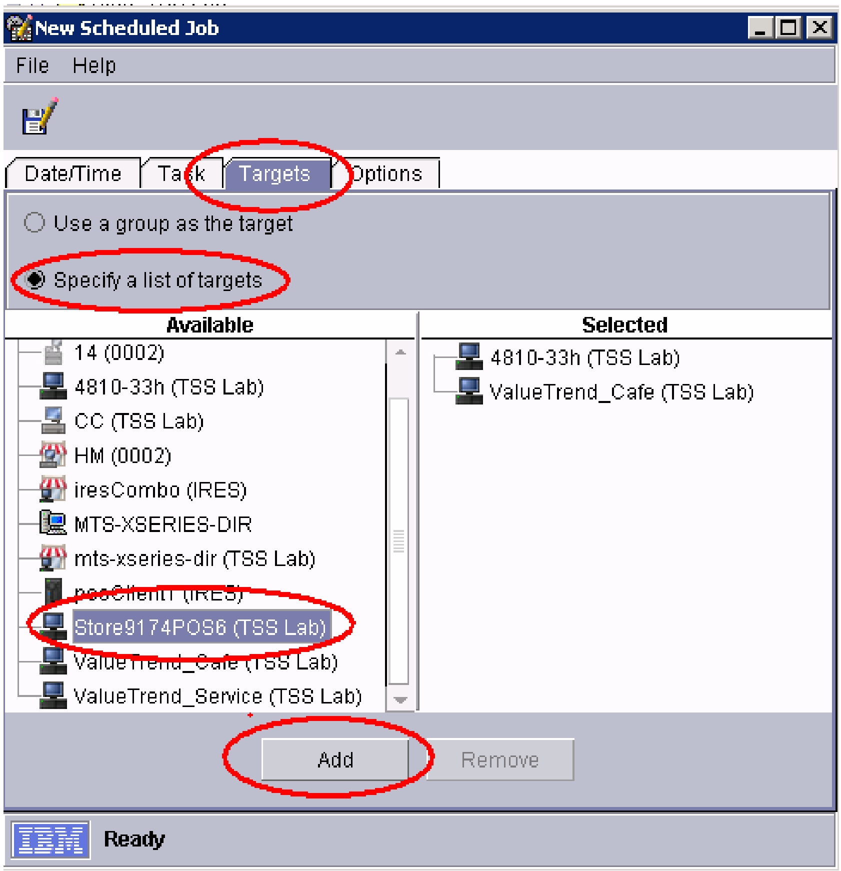
Repeat job Every day from 4/2/2009 at 6:00 AM until 4/16/2009 at 6:00 AM

6. On the New Schedule window select the “Task” tab, expand the “Power Management” tree, select “Power On”, click on “Select” button.



7. On the New Schedule window select the “Target” tab, select the “Specify a list of targets” radio button, select the system(s), select the “Add” button.

Note: You can select the “Use a group as the target” radio button to select a group of systems, but remember not all operating systems support a “Power On”, so be sure the group you select does not have systems that can not be woken up.



○ Use a group as the target

● Specify a list of targets

Available

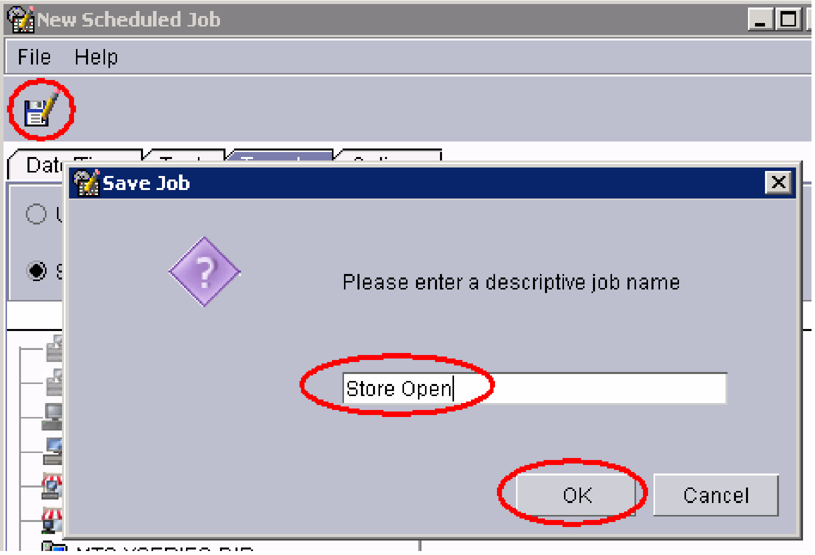
- 14 (0002)
- 4810-33h (TSS Lab)
- CC (TSS Lab)
- HM (0002)
- iresCombo (IRES)
- MTS-XSERIES-DIR
- mts-xseries-dir (TSS Lab)
- posClient1 (IRES)
- Store9174POS6 (TSS Lab)
- ValueTrend_Cafe (TSS Lab)
- ValueTrend_Service (TSS Lab)

Selected

- 4810-33h (TSS Lab)
- ValueTrend_Cafe (TSS Lab)

> **Note:** In order for RMA to have the ability to Power On a system, the systems BIOS has be enabled for “Wake On LAN”. Refer to hardware user guide for instructions on how to enable ‘Wake On LAN” for each hardware platform.

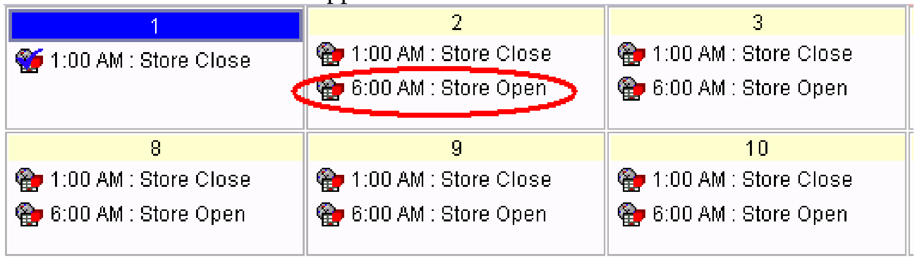
8. Click the “Save As” button, enter a saved job name as “Store Open”, click OK, click OK on the Job Saved message, and then close the New Schedule Job window.



Please enter a descriptive job name

Store Open

9. The New Schedule Job will appear on the Scheduler.



1	2	3
1:00 AM : Store Close	1:00 AM : Store Close 6:00 AM : Store Open	1:00 AM : Store Close 6:00 AM : Store Open
8	**9**	**10**
1:00 AM : Store Close 6:00 AM : Store Open	1:00 AM : Store Close 6:00 AM : Store Open	1:00 AM : Store Close 6:00 AM : Store Open

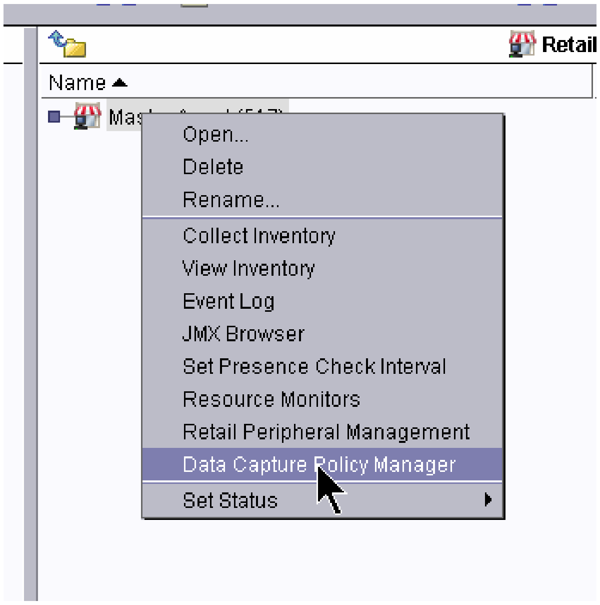
Chapter 11 – Data Capture

Comment:
Need to add in the future:
Introduction to RMA Data Capture
TBD …
- Using the data capture policy manager
- Soliciting data capture
- Viewing capture history
- Invocation on single agent
- Data capture events

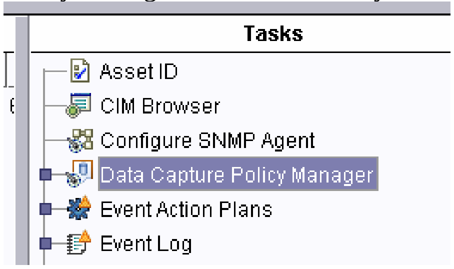
Example: Generic file capture using RMA data capture

This example shows you how to collect a file from a remote POS system using RMA data capture. Although this example describes how to collect a file from a 4690 file system, the same exact procedure can be used to collect files from Windows or Linux as well.

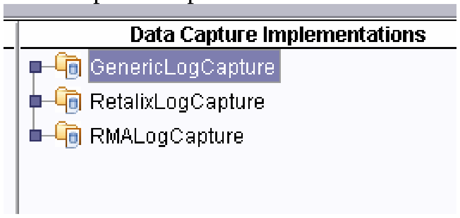
1. From the IBM Director Console, initiate the Data Capture Policy Manager. If this is the first Data Capture Implementation done on this Director Server, this must be done by right clicking a Master Agent and selecting "Data Capture Policy Manager". This will populate the manager with the available policies on that agent.



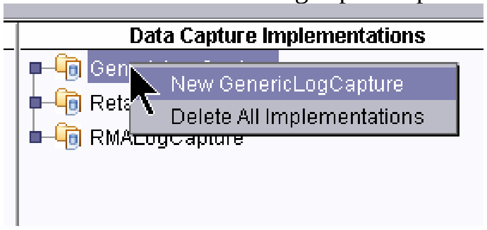
2. After the first Data Capture Implementation for a Master Agent, the Data Capture Policy Manager can be initiated by double clicking it in the task list.



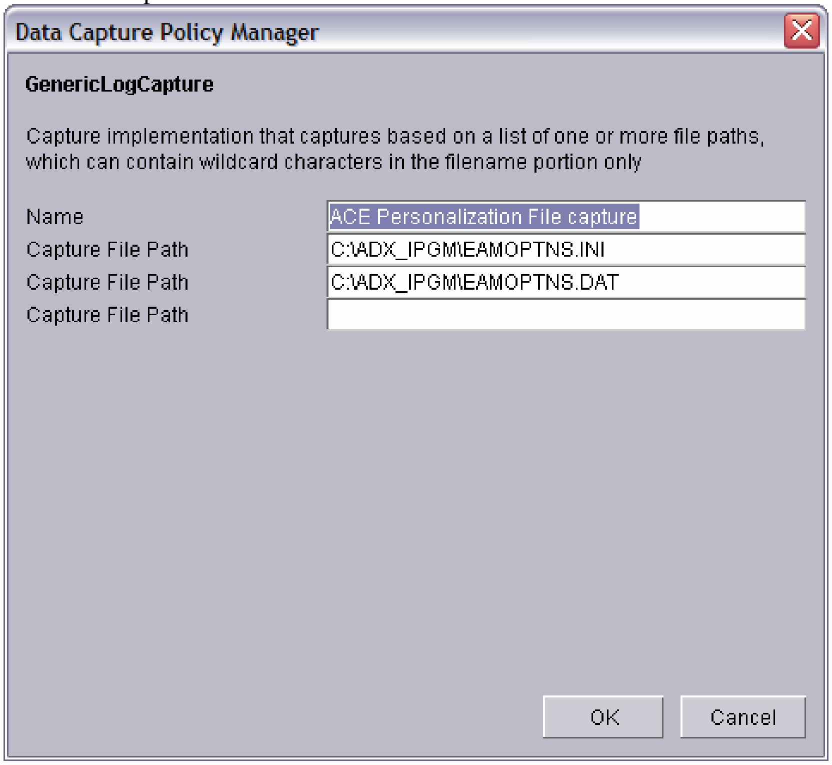
3. Inside the Data Capture Policy Manager, right click GenericLogCapture under the Data Capture Implementations column:



4. Select the New GenericLogCapture option.



5. Enter a meaning full name for the capture implementation and the name(s) of the files to be captured.



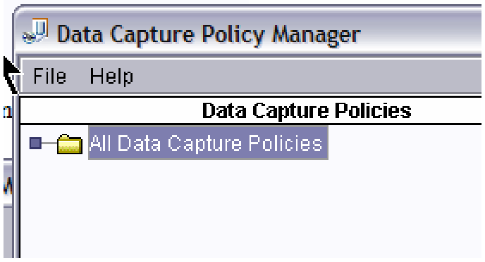
GenericLogCapture

Capture implementation that captures based on a list of one or more file paths, which can contain wildcard characters in the filename portion only

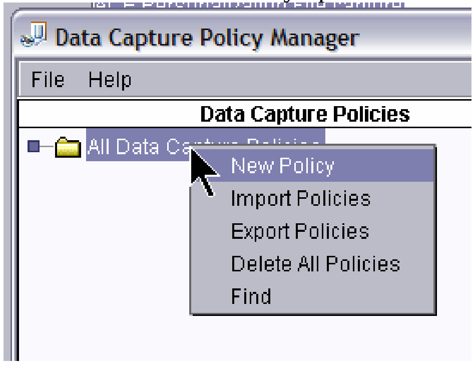
Name	ACE Personalization File capture
Capture File Path	C:\ADX_IPGM\EAMOPTNS.INI
Capture File Path	C:\ADX_IPGM\EAMOPTNS.DAT
Capture File Path	

Note: Wildcards can be used for file names only in the Capture File Path

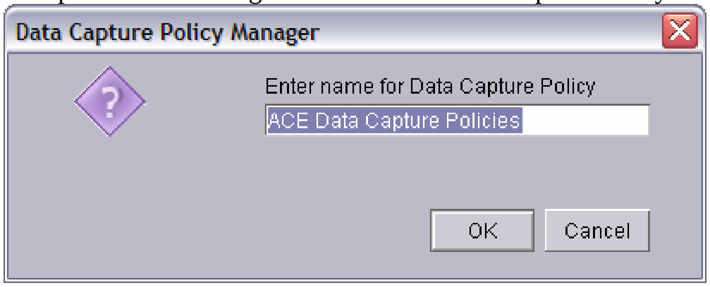
6. To create a policy for this implementation, right click “All Data Capture Policies” in the Data Capture Policies list.



7. And select the New Policy option.

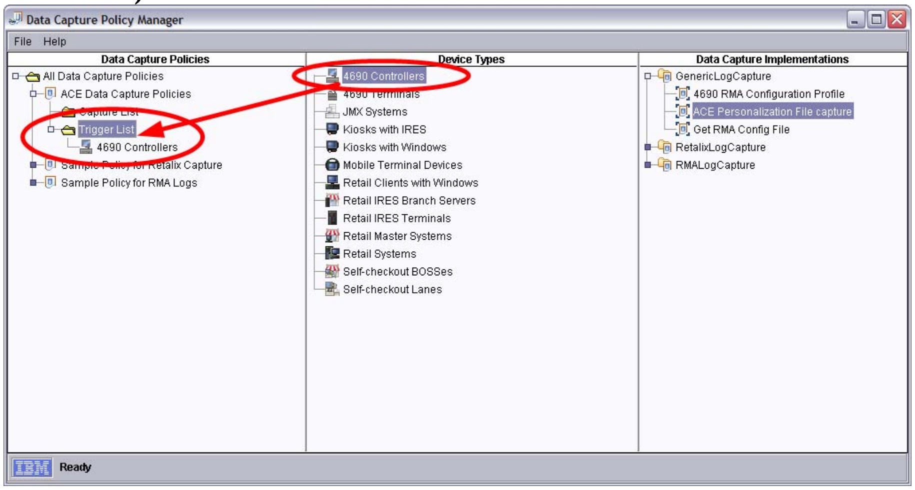


8. And provide a meaningful name for the Data Capture Policy.

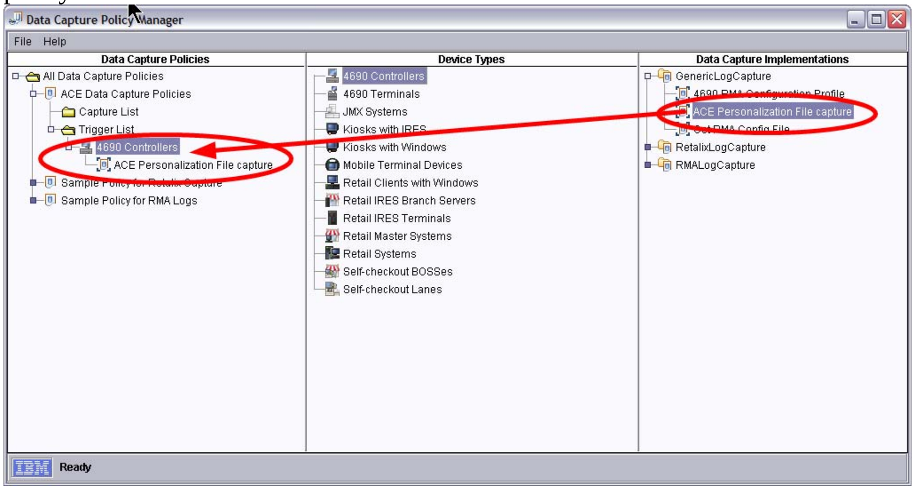


Enter name for Data Capture Policy: ACE Data Capture Policies

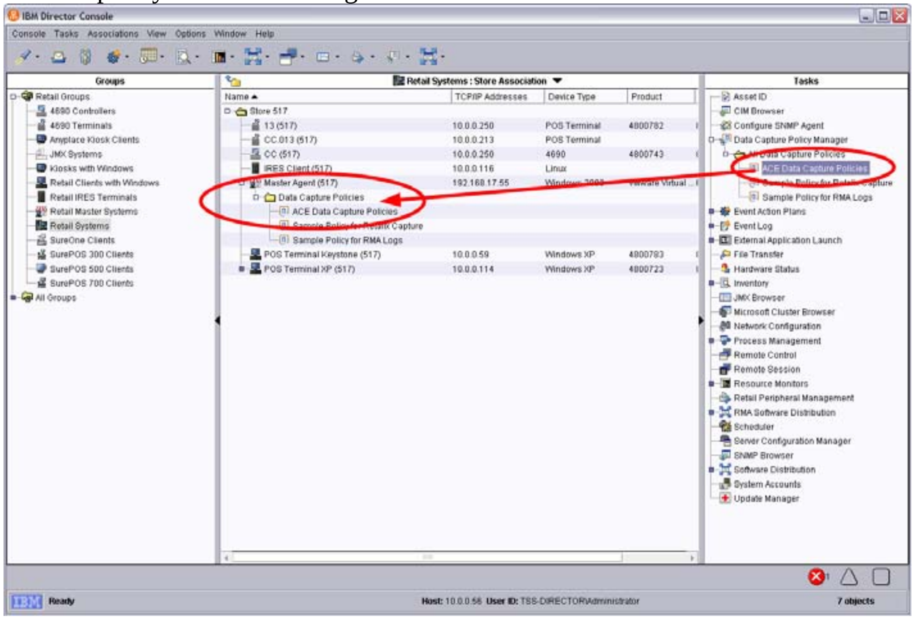
9. Expand the tree for the new policy and drag the “4690 Controller” device type to its Trigger List. **(If using Windows instead, drag “Retail Clients with Windows”.)**



10. Drag the new implementation to the device type in the trigger list for the new policy.

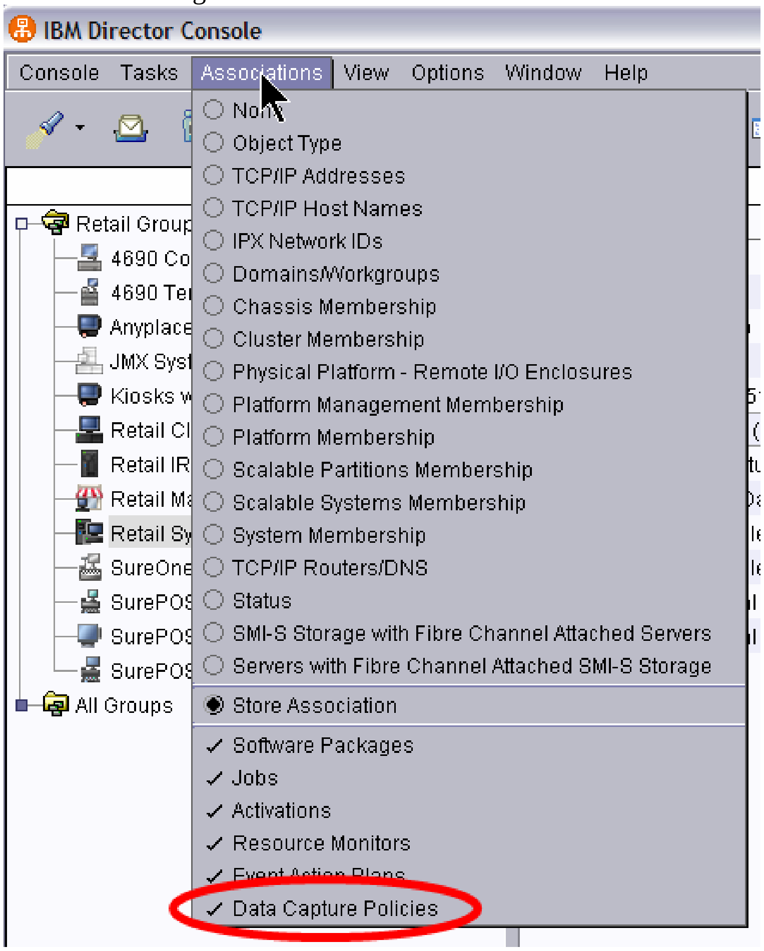


11. Close the data capture policy manager window, and return to the main Director Console view. Expand Data Capture Policy Manager under the Tasks list and drag the new policy to the Master Agent.

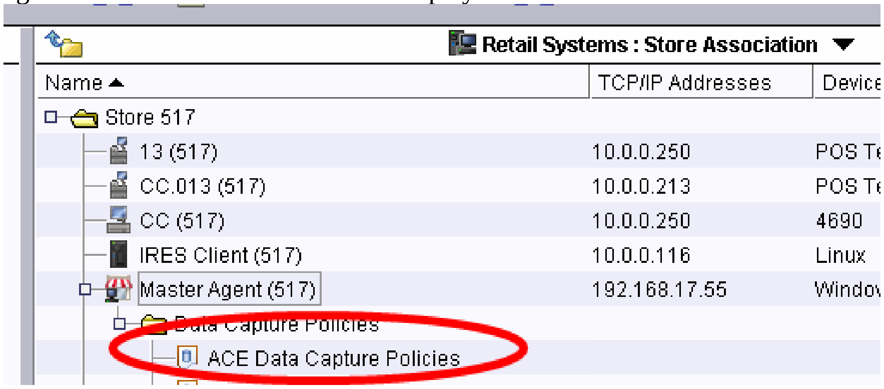


Name	TCP/IP Addresses	Device Type	Product
Store 517			
13 (517)	10.0.0.250	POS Terminal	4800782
CC.013 (517)	10.0.0.213	POS Terminal	
CC (517)	10.0.0.250	4690	4800743
IRES Client (517)	10.0.0.116	Linux	
Master Agent (517)	192.168.17.55	Windows 2003	VMware Virtual ...
Data Capture Policies			
ACE Data Capture Policies			
Sample Policy for Retail Capture			
Sample Policy for RMA Logs			
POS Terminal Keystone (517)	10.0.0.59	Windows XP	4800783
POS Terminal XP (517)	10.0.0.114	Windows XP	4800723

12. Use the “Associations” menu to make sure that “Data Capture Policies” is checked. This allows you to view all the data capture policies that are associated with the master agent.

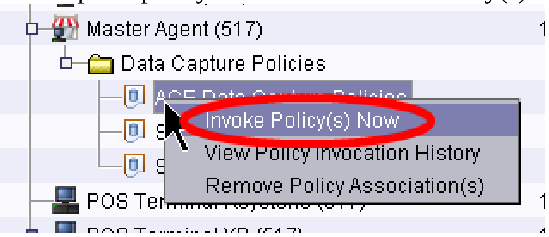


13. You should now be able to see your data capture policy associated with the master agent in the main Director Console display.



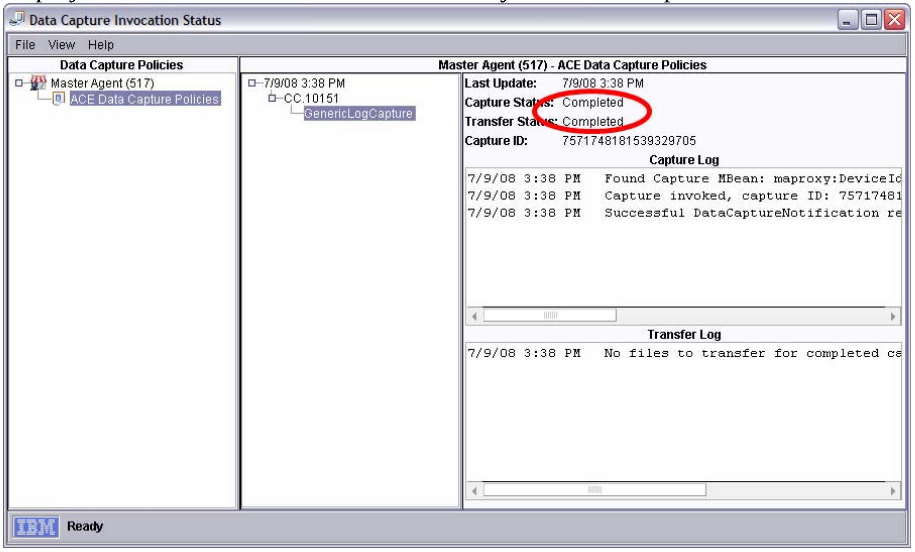
Name	TCP/IP Addresses	Device
Store 517		
13 (517)	10.0.0.250	POS Te
CC.013 (517)	10.0.0.213	POS Te
CC (517)	10.0.0.250	4690
IRES Client (517)	10.0.0.116	Linux
Master Agent (517)	192.168.17.55	Windov
Data Capture Policies		
ACE Data Capture Policies		

14. To invoke the policy (i.e. to trigger the policy to collect ACE files), right-click the data capture policy and select “Invoke Policy(s) Now”.



Master Agent (517)
Data Capture Policies
ACE Data Capture Policies
Invoke Policy(s) Now
View Policy Invocation History
Remove Policy Association(s)
POS Terminal Kyotoms (517)

15. You will now see the “Data Capture Invocation Status” screen, which allows you to see the history of data captures that were taken for this data capture policy. Expand the Data Capture Policies tree and select the policy invoked to show the invocations for this policy. Expand the tree for the invocation of interest to display it’s status. You should see that each system is “Completed”.

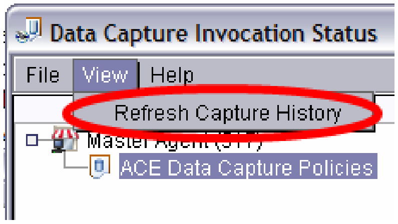


Last Update: 7/9/08 3:38 PM
Capture Status: Completed
Transfer Status: Completed
Capture ID: 7571748181539329705

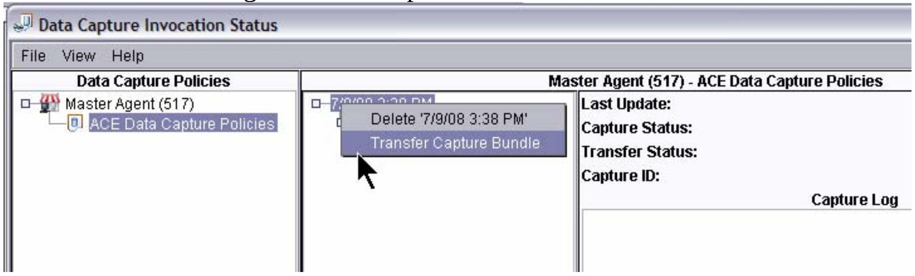
```
7/9/08 3:38 PM   Found Capture MBean: maproxy:DeviceId
7/9/08 3:38 PM   Capture invoked, capture ID: 75717481
7/9/08 3:38 PM   Successful DataCaptureNotification re
```

```
7/9/08 3:38 PM   No files to transfer for completed ca
```

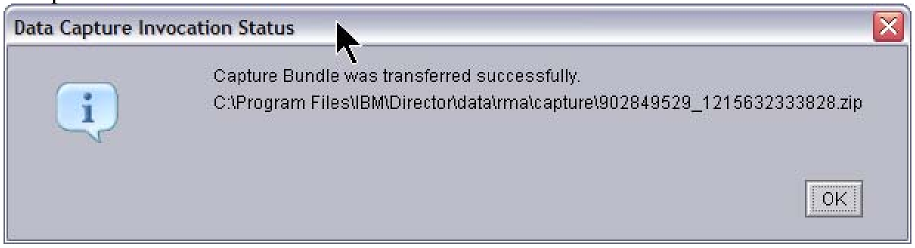
16. NOTE: You may need to “refresh” this view a few times before you can see that it has completed. To refresh, use the “View” menu.



17. After the data capture policy invocation reaches the status of “Completed”, you can transfer the capture bundle to the Director Server by right-clicking the date/time and selecting “Transfer Capture Bundle”.



18. You'll see the location of the ZIP file on the following screen. You can now unzip that file access the files transfered.


Data Capture Invocation Status

Capture Bundle was transferred successfully.
C:\Program Files\IBM\Director\data\rma\capture\902849529_1215632333828.zip

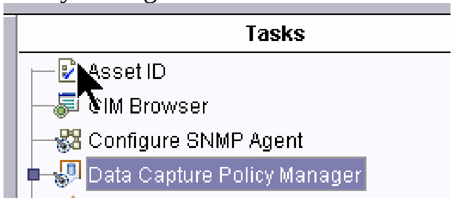
19. To access the files captured, open the capture bundle's ZIP file on the Director Server. Enter the folders exposed at each level until the folder contains a ZIP file. The captured files should be in the ZIP file.

> **Note:** You can return to the data capture invocation history at any time by right-clicking the data capture policy (in the main Director Console view) and selecting "View Policy Invocation History"

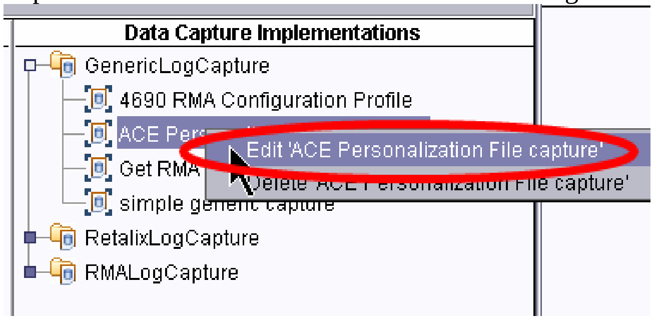
Example: Modifying an Existing Generic Capture Policy

1. The following procedure can be used to modify an existing data capture implementation to change the files specified.

2. Enter the Data Capture Policy Manager by double clicking the Data Capture Policy Manager task on the Director Console.

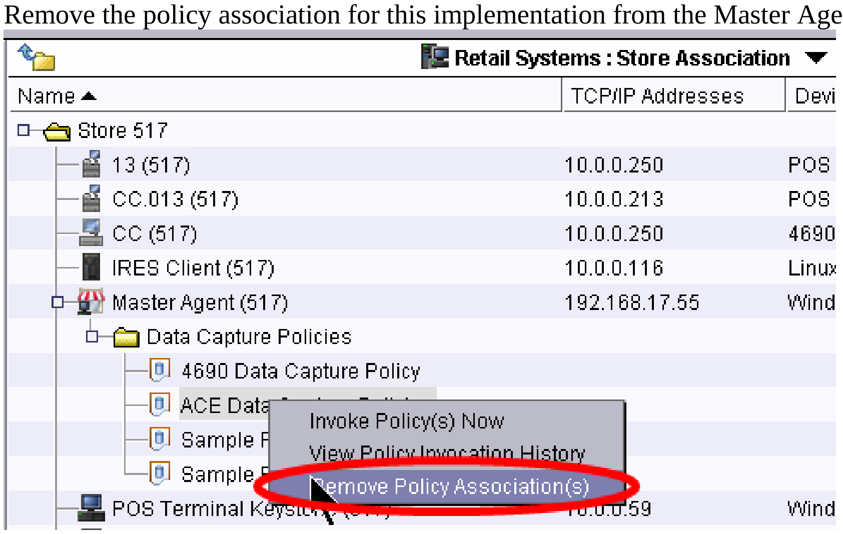


3. Expand the GenericLogCapture Implementation and right click the implementation to be modified. Select Edit to change the implementation.


Data Capture Implementations
GenericLogCapture
4690 RMA Configuration Profile
ACE Pers
Get RMA
simple generic capture
RetalixLogCapture
RMALogCapture
Edit 'ACE Personalization File capture'
Delete 'ACE Personalization File capture'

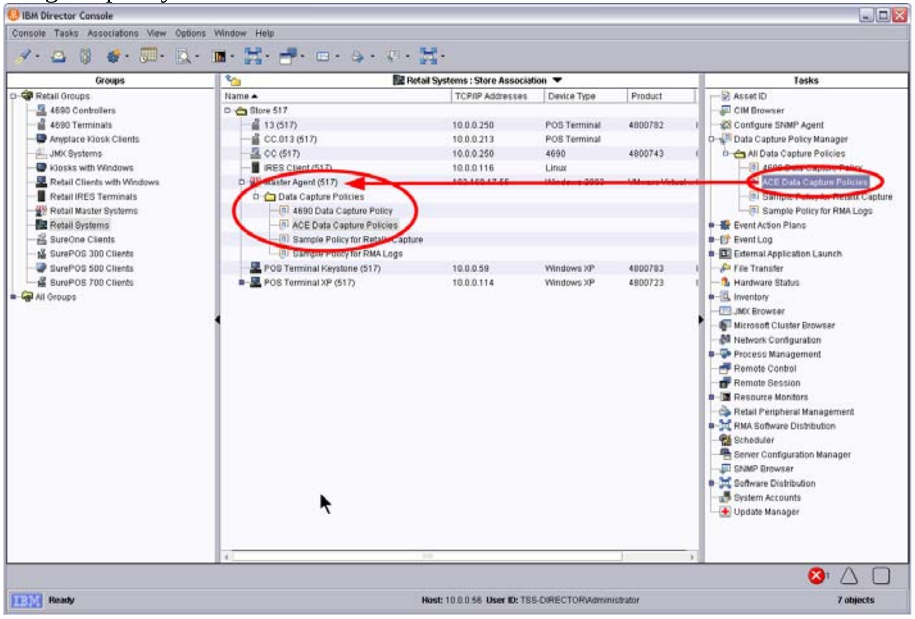
4. Edit the list of files in the Data Capture Implementation and accept by clicking OK.

5. Remove the policy association for this implementation from the Master Agent.


Retail Systems : Store Association
Invoke Policy(s) Now
View Policy Invocation History
Remove Policy Association(s)

Name	TCP/IP Addresses	Devi
Store 517		
13 (517)	10.0.0.250	POS
CC.013 (517)	10.0.0.213	POS
CC (517)	10.0.0.250	4690
IRES Client (517)	10.0.0.116	Linux
Master Agent (517)	192.168.17.55	Wind
Data Capture Policies		
4690 Data Capture Policy		
ACE Data		
Sample F		
Sample		
POS Terminal Keyst (517)	10.0.0.59	Wind

6. Drag the policy to the MA to re-associate it.



Name ▲	TCP/IP Addresses	Device Type	Product
Store 517			
13 (517)	10.0.0.250	POS Terminal	4800782
CC.013 (517)	10.0.0.213	POS Terminal	
CC (517)	10.0.0.250	4690	4800743
IRES Client (517)	10.0.0.116	Linux	
Master Agent (517)	192.168.47.55	Windows 2003	VMware Virtual...
Data Capture Policies			
4690 Data Capture Policy			
ACE Data Capture Policies			
Sample Policy for Retail Capture			
Sample Policy for RMA Logs			
POS Terminal Keystone (517)	10.0.0.59	Windows XP	4800783
POS Terminal XP (517)	10.0.0.114	Windows XP	4800723

Host: 10.0.0.56 User ID: TSS-DIRECTOR\Administrator

7 objects

Example: How to Collect RMA Log Files using RMA Data Capture

To collect RMA log files remotely, you can create a “data capture policy” and associate it to the master agent. After you’ve created a data capture policy, you can collect RMA log files in one of two ways:

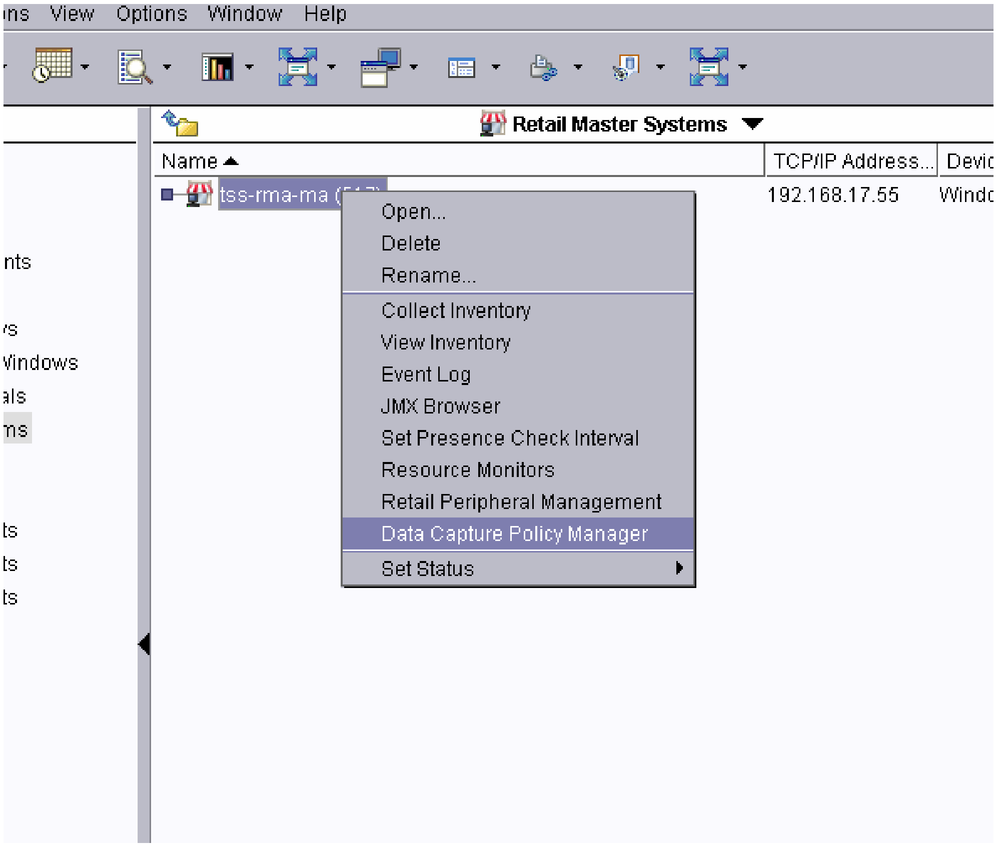
1. To manually “solicit” the collection of RMA log files using your data capture policy, you can right-click the policy, and select “Invoke policy(s) Now”. This will immediately trigger the MA (and all attached GA’s) to collect log files in a data capture bundle. You can then use the data capture policy invocation history to transfer the capture bundle to the Director Server and view the files.

2. If RMA encounters an error, it will sometimes automatically trigger an “unsolicited” data capture. An event will be sent to Director, and you can use the data capture policy invocation history to obtain the data capture files for the error.

Use the instructions below to set up your data capture policy, associate it to the master agent, then invoke the policy to obtain the RMA log files.

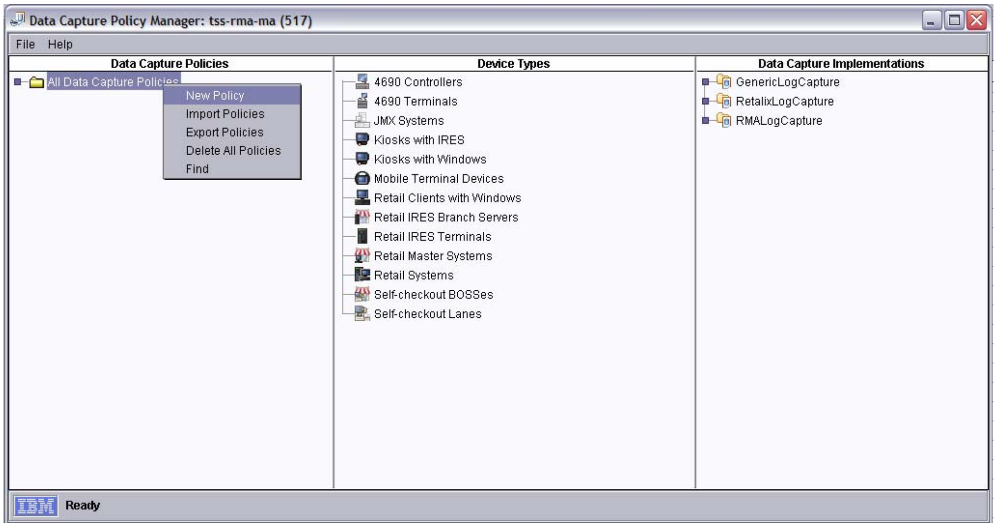
Steps:

1. Right-click the master agent in the Director console, and select “Data Capture Policy Manager”.

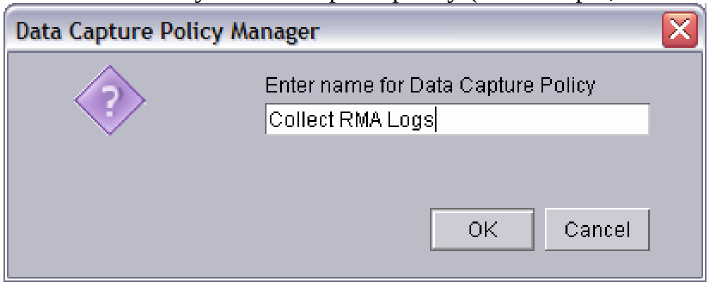


Warning: Do not invoke the data capture policy manager from the "Tasks" pane by double-clicking it. It must be invoked on the master agent using the method described above, or else some of the steps below will not be possible.

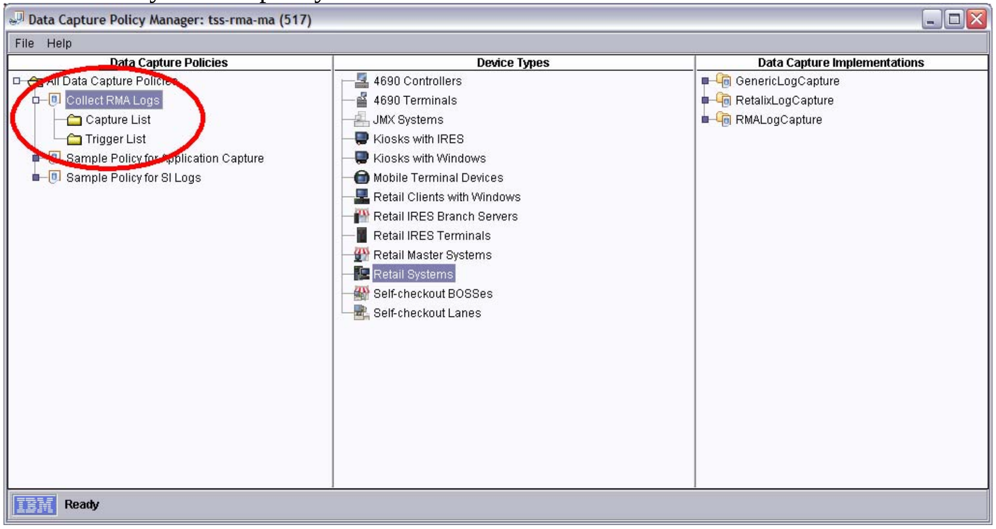
2. The "Data Capture Policy Manager" will appear. Right-click "All Data Capture Policies" and select "New Policy".



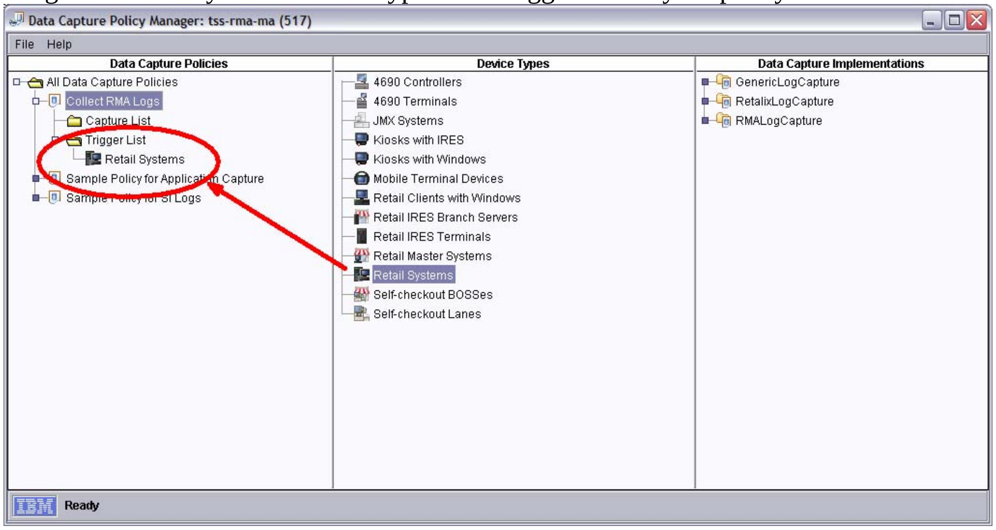
3. Enter a name for your data capture policy (for example, “Collect RMA Logs”).


Data Capture Policy Manager
Enter name for Data Capture Policy
Collect RMA Logs
OK
Cancel

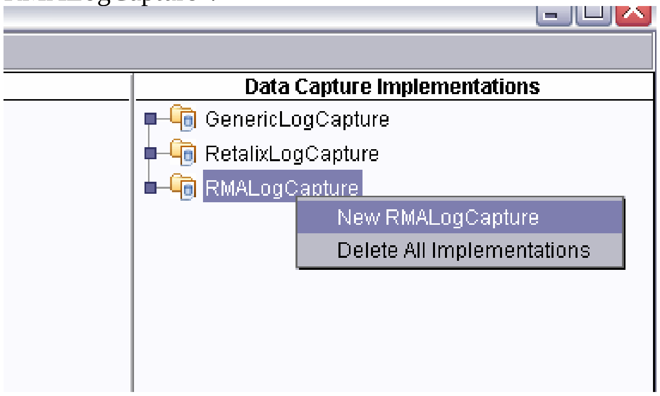
4. You will see your new policy in the tree on the left-hand side of the screen.



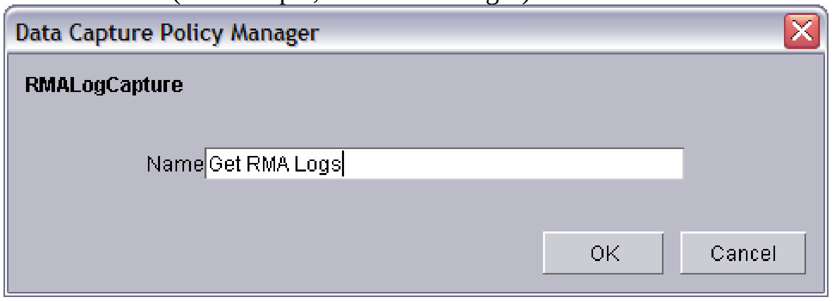
5. Drag the “Retail Systems” device type to the trigger list for your policy.



6. Right-click the “RMALogCapture” implementation, and choose “New RMALogCapture”.

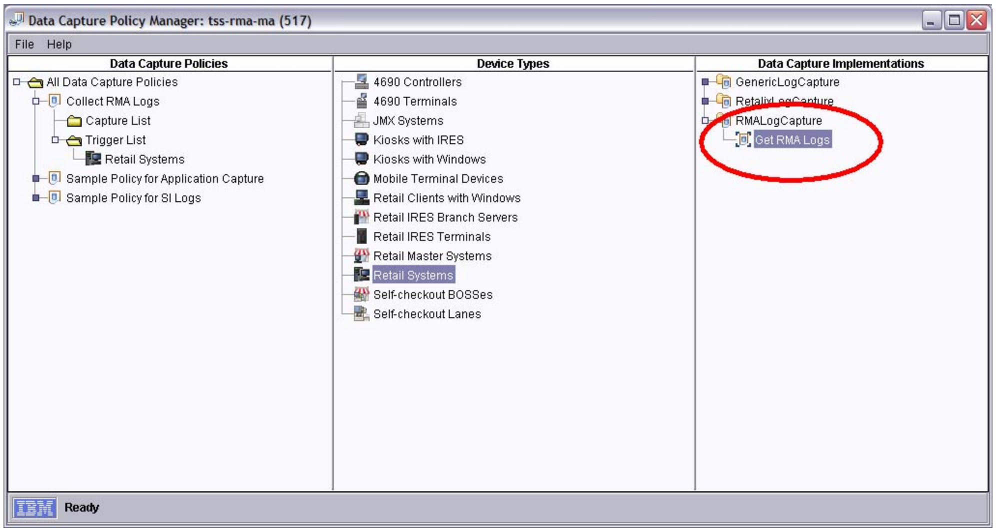


7. Give it a name (for example, “Get RMA Logs”).



Name Get RMA Logs

8. After you click OK, you’ll see your new implementation in the tree on the right-hand side of the screen.



Data Capture Policy Manager: tss-rma-ma (517)

File Help

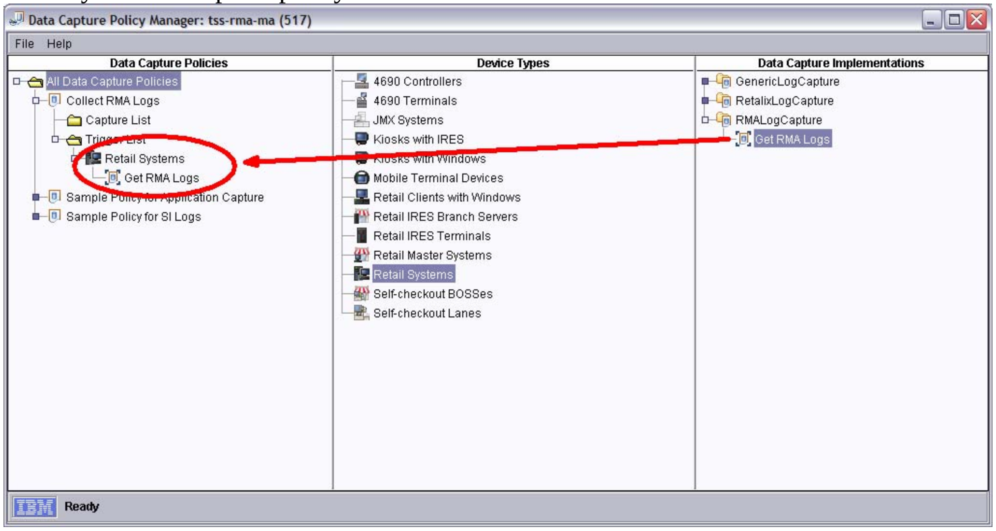
Data Capture Policies
- All Data Capture Policies
  - Collect RMA Logs
    - Capture List
    - Trigger List
      - Retail Systems
  - Sample Policy for Application Capture
  - Sample Policy for SI Logs

Device Types
- 4690 Controllers
- 4690 Terminals
- JMX Systems
- Kiosks with IRES
- Kiosks with Windows
- Mobile Terminal Devices
- Retail Clients with Windows
- Retail IRES Branch Servers
- Retail IRES Terminals
- Retail Master Systems
- Retail Systems
- Self-checkout BOSSes
- Self-checkout Lanes

Data Capture Implementations
- GenericLogCapture
- RetalixLogCapture
- RMALogCapture
  - Get RMA Logs

Ready

9. Drag your new implementation so that it appears underneath "Retail Systems" within your data capture policy.



Data Capture Policy Manager: tss-rma-ma (517)

File Help

Data Capture Policies
- All Data Capture Policies
  - Collect RMA Logs
    - Capture List
    - Trigger List
      - Retail Systems
        - Get RMA Logs
  - Sample Policy for Application Capture
  - Sample Policy for SI Logs

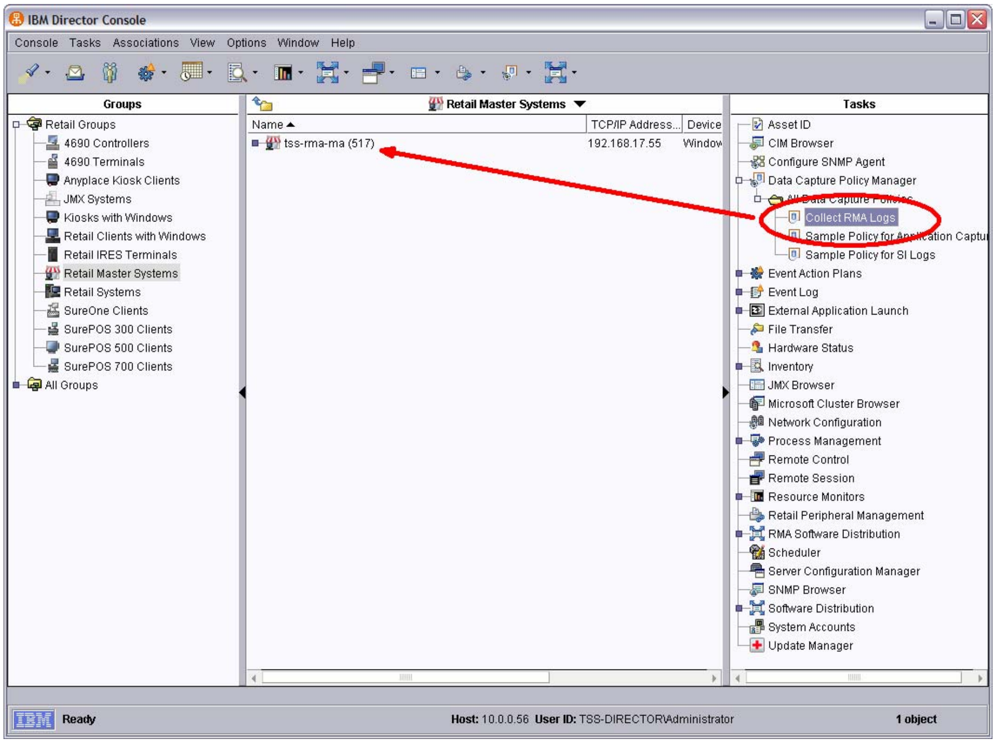
Device Types
- 4690 Controllers
- 4690 Terminals
- JMX Systems
- Kiosks with IRES
- Kiosks with Windows
- Mobile Terminal Devices
- Retail Clients with Windows
- Retail IRES Branch Servers
- Retail IRES Terminals
- Retail Master Systems
- Retail Systems
- Self-checkout BOSSes
- Self-checkout Lanes

Data Capture Implementations
- GenericLogCapture
- RetalixLogCapture
- RMALogCapture
  - Get RMA Logs

Ready

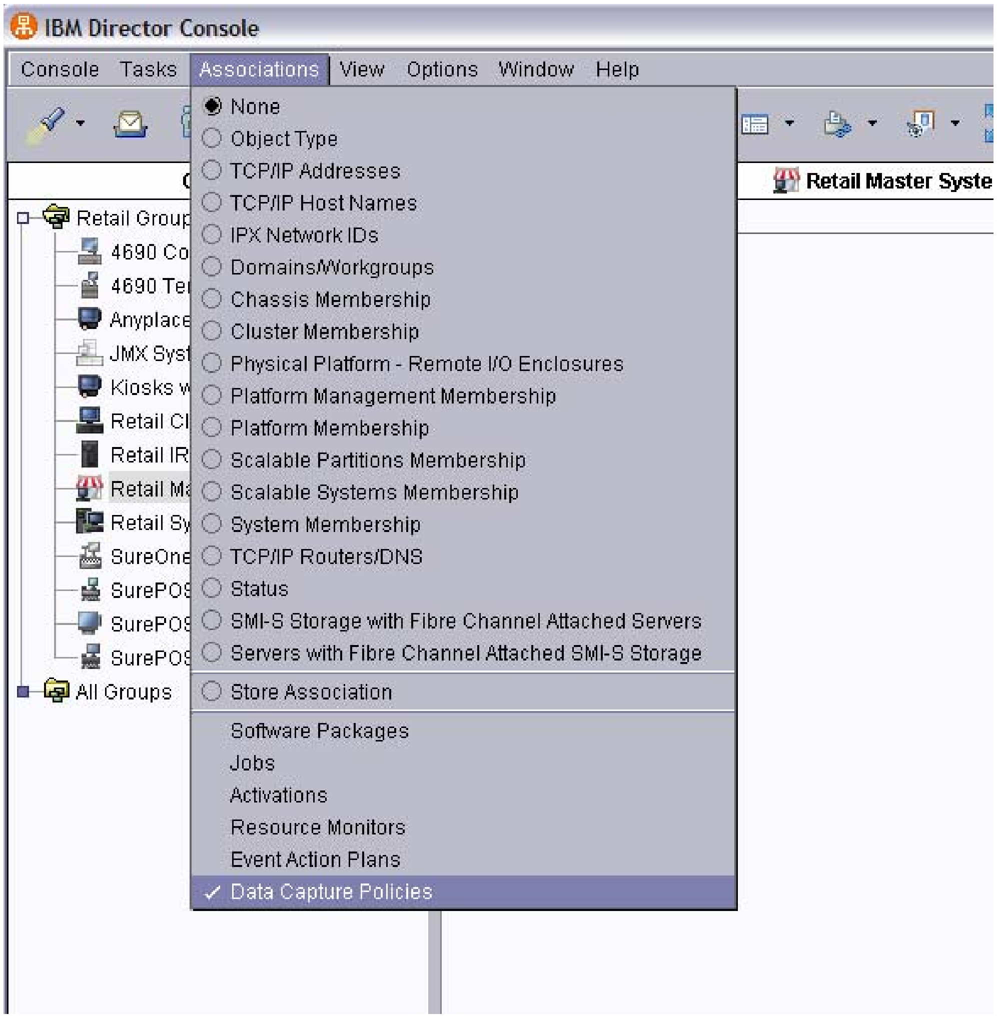
10. Close the data capture policy manager window, and return to the main Director Console view.

11. You will now see your new data capture policy in the "Tasks" pan underneath "Data Capture Policy Manager / All Data Capture Policies". Drag your new data capture policy to the master agent.

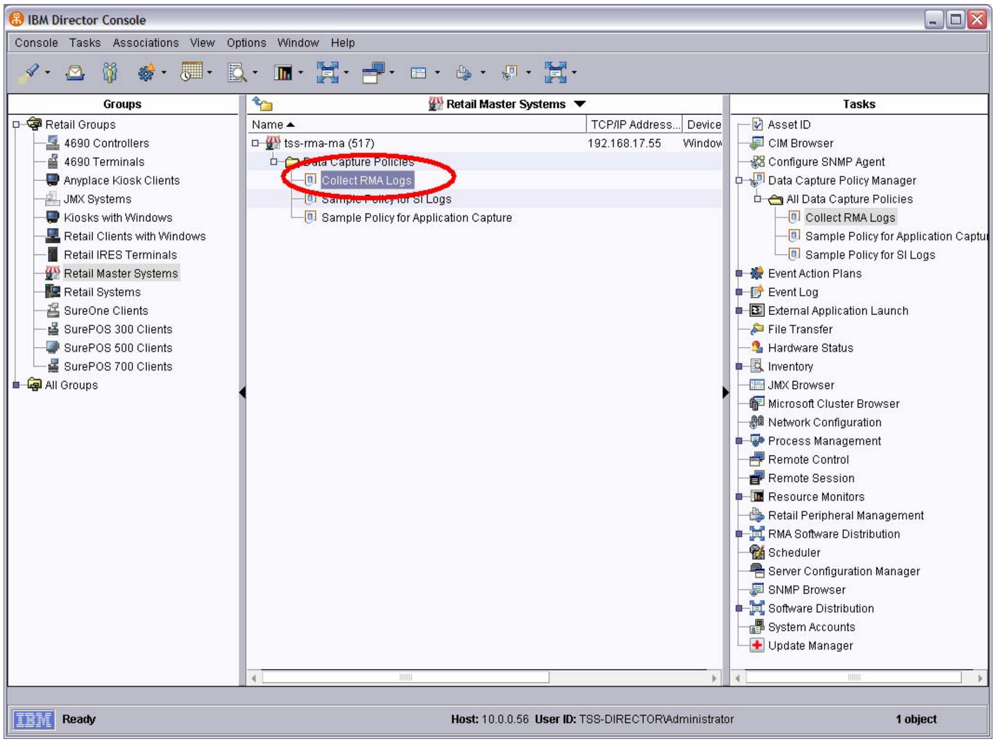


Name ▲	TCP/IP Address...	Device
tss-rma-ma (517)	192.168.17.55	Window

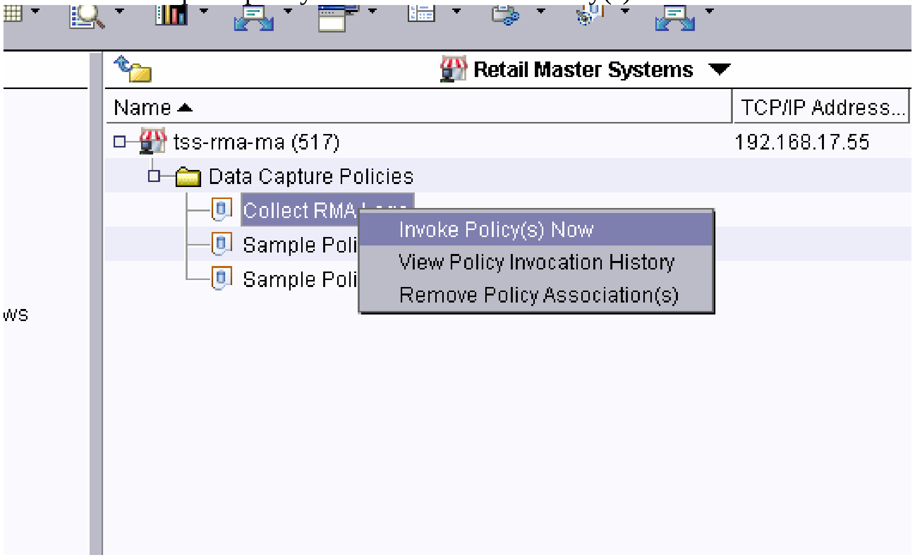
12. Use the “Associations” menu to be sure that “Data Capture Policies” is checked. This allows you to view all the data capture policies that are associated with the master agent.



13. You should now be able to see your data capture policy associated to the master agent in the main Director Console display.

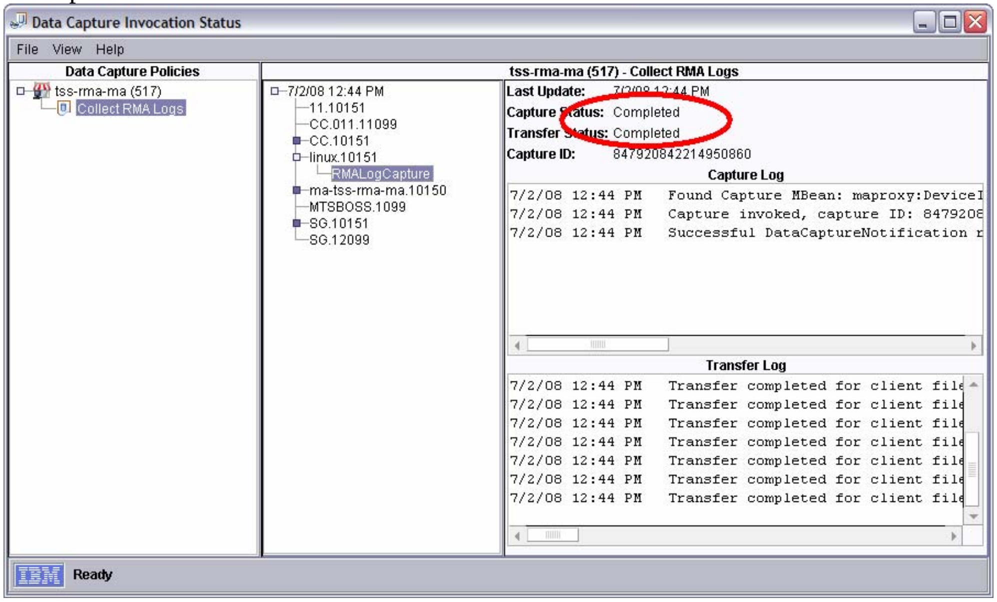


14. To invoke the policy (i.e. to trigger the policy to collect RMA log files), right-click the data capture policy and select “Invoke Policy(s) Now”.



15. You will now see the “Data Capture Invocation Status” screen, which allows you to see the history of data captures that were taken for this data capture policy.

You can expand the tree(s) to display the status for the data capture on each GA attached to the MA (as well as for the MA). You should see that each system is “Completed”.



tss-rma-ma (517) - Collect RMA Logs

Last Update: 7/2/08 12:44 PM
Capture Status: Completed
Transfer Status: Completed
Capture ID: 847920842214950860

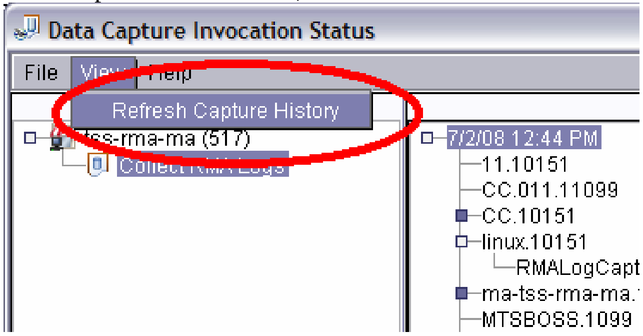
Capture Log

```
7/2/08 12:44 PM   Found Capture MBean: maproxy:DeviceI
7/2/08 12:44 PM   Capture invoked, capture ID: 8479208
7/2/08 12:44 PM   Successful DataCaptureNotification r
```

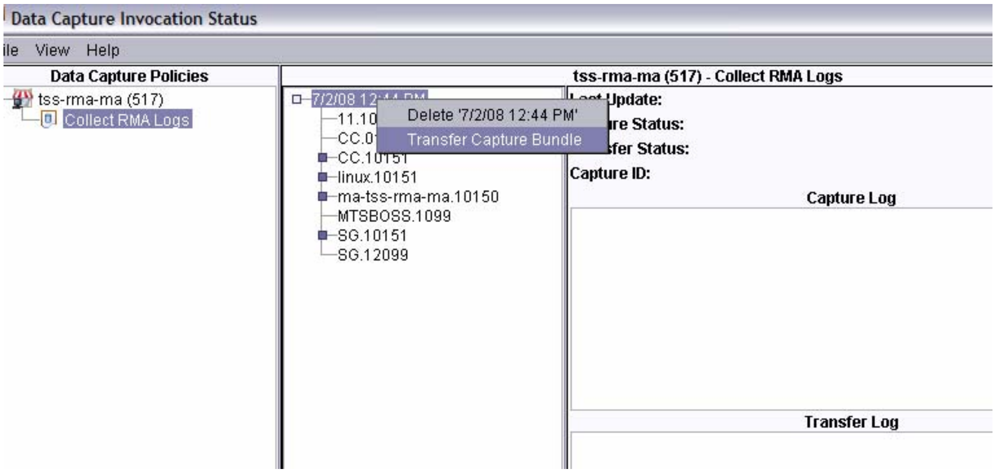
Transfer Log

```
7/2/08 12:44 PM   Transfer completed for client file
7/2/08 12:44 PM   Transfer completed for client file
7/2/08 12:44 PM   Transfer completed for client file
7/2/08 12:44 PM   Transfer completed for client file
7/2/08 12:44 PM   Transfer completed for client file
7/2/08 12:44 PM   Transfer completed for client file
7/2/08 12:44 PM   Transfer completed for client file
```

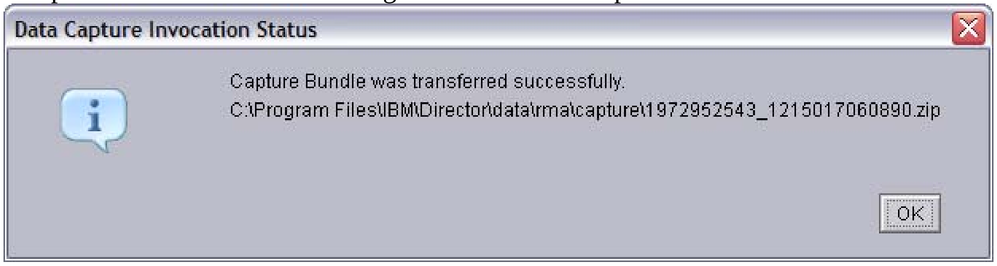
NOTE: You may need to “refresh” this view a few times before you can see that it has completed. To refresh, use the “View” menu.



16. After the data capture policy invocation reaches the status of “Completed”, you can transfer the capture bundle to the Director Server by right-clicking the date/time and selecting “Transfer Capture Bundle”.

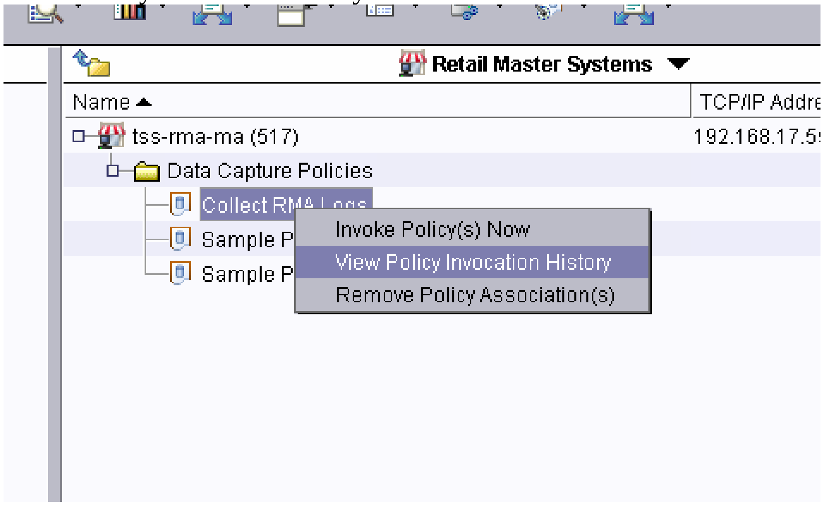


17. You'll see the location of the ZIP file on the following screen. You can now unzip that file to view the RMA log files for the data capture.

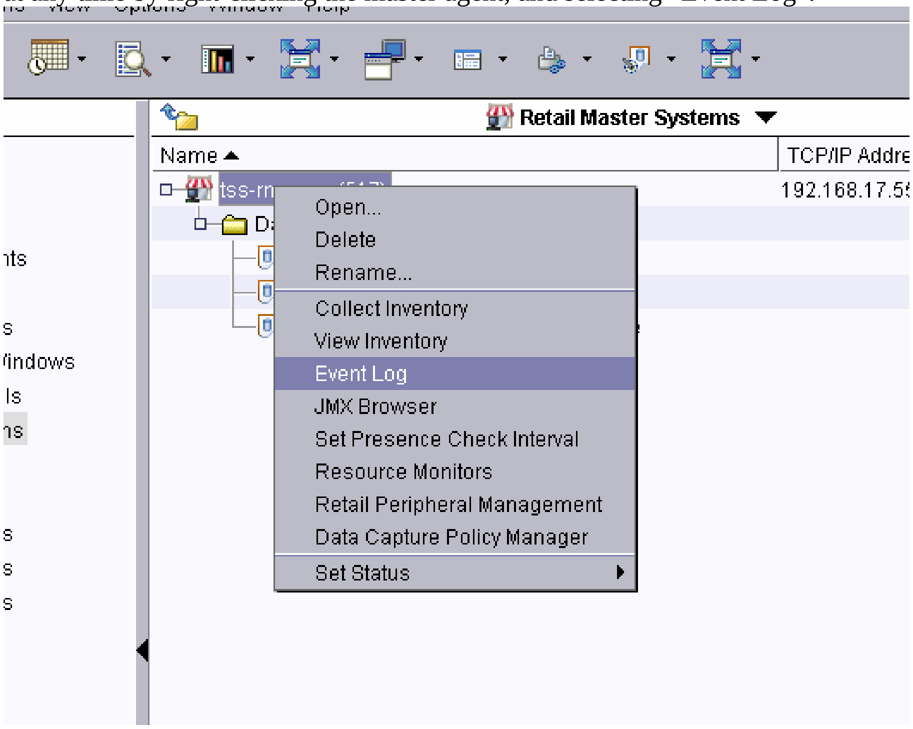


```
Capture Bundle was transferred successfully.
C:\Program Files\IBM\Director\data\rma\capture\1972952543_1215017060890.zip
```

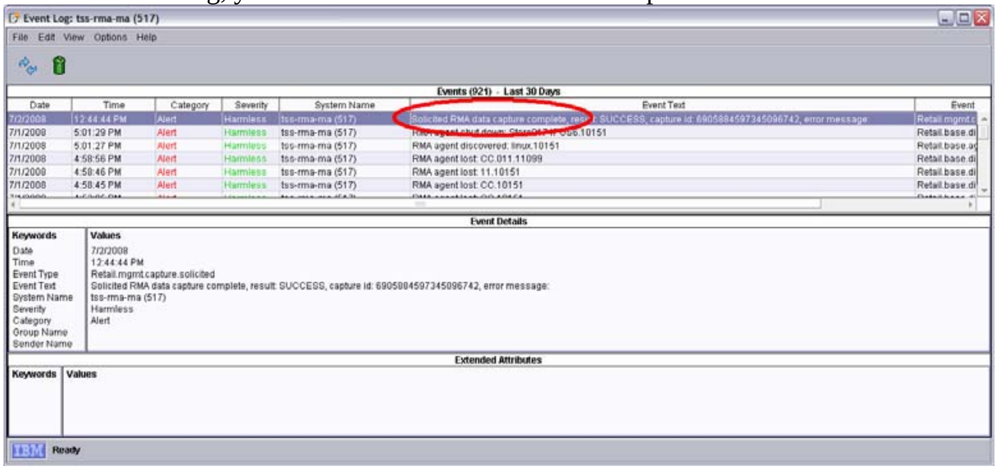
Note: You can return to the data capture invocation history at any time by right-clicking the data capture policy (in the main Director Console view) and selecting "View Policy Invocation History".



Note: Any time a data capture completes (solicited or unsolicited), Director will receive an event in the event log for the master agent. You can go to the event log at any time by right-clicking the master agent, and selecting “Event Log”.



Inside the event log, you will see an event for each data capture invocation.



Events (921) - Last 30 Days

Date	Time	Category	Severity	System Name	Event Text	Event
7/2/2008	12:44:44 PM	Alert	Harmless	tss-rma-ma (517)	Solicited RMA data capture complete, res[illegible] SUCCESS, capture id: 6905884597345096742, error message:	Retail.mgmt.c
7/1/2008	5:01:29 PM	Alert	Harmless	tss-rma-ma (517)	RMA agent shut down: Store[illegible]006.10151	Retail.base.di
7/1/2008	5:01:27 PM	Alert	Harmless	tss-rma-ma (517)	RMA agent discovered: linux.10151	Retail.base.a
7/1/2008	4:58:56 PM	Alert	Harmless	tss-rma-ma (517)	RMA agent lost: CC.011.11099	Retail.base.di
7/1/2008	4:58:46 PM	Alert	Harmless	tss-rma-ma (517)	RMA agent lost: 11.10151	Retail.base.di
7/1/2008	4:58:45 PM	Alert	Harmless	tss-rma-ma (517)	RMA agent lost: CC.10151	Retail.base.di

Event Details

Keywords	Values
Date	7/2/2008
Time	12:44:44 PM
Event Type	Retail.mgmt.capture.solicited
Event Text	Solicited RMA data capture complete, result: SUCCESS, capture id: 6905884597345096742, error message:
System Name	tss-rma-ma (517)
Severity	Harmless
Category	Alert
Group Name	
Sender Name	

Extended Attributes

Keywords	Values

You can create event action plans based on these events, which will allow you to react to the data capture events in a more advanced way (for example, by sending an email, or displaying a message on the Console, or by flagging the system status for review). This allows you to proactively detect when a data capture occurs. (The data capture events are especially useful when RMA encounters a serious error and takes an automatic/unsolicited data capture – this allows you to detect that the problem occurred so you will know to check the invocation history to obtain the capture bundle.)

Chapter 12 – Using the RMA File Transfer Task

This chapter explains how to use the "RMA File Transfer" task in the IBM Director Console for RMA agents. From this task you have the ability to:

- Browse details of the file system of a remote MA or GA
- Create, delete, or rename directories
- View, edit, rename, or delete files
- Drag-and-drop to transfer files or directories between Director and RMA MA/GA

While this task allows you to quickly and easily transfer files to and from a single target system, it is not intended to replace RMA Software Distribution which can be used to deploy packages to many systems as once. Instead, the RMA File Transfer task is helpful in debugging problems and applying patches to small numbers of systems.

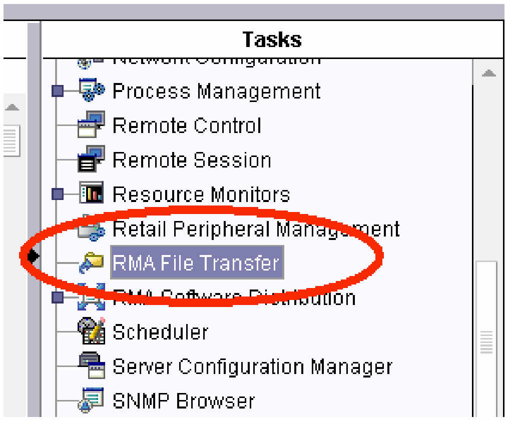
Introduction to the RMA File Transfer Task

RMA File Transfer task

The "RMA File Transfer" task was introduced in RMA V2R6. It can be launched on Windows and Linux agents running RMA V2R4 or later, and 4690 agents running 4690 V6R2 or later.

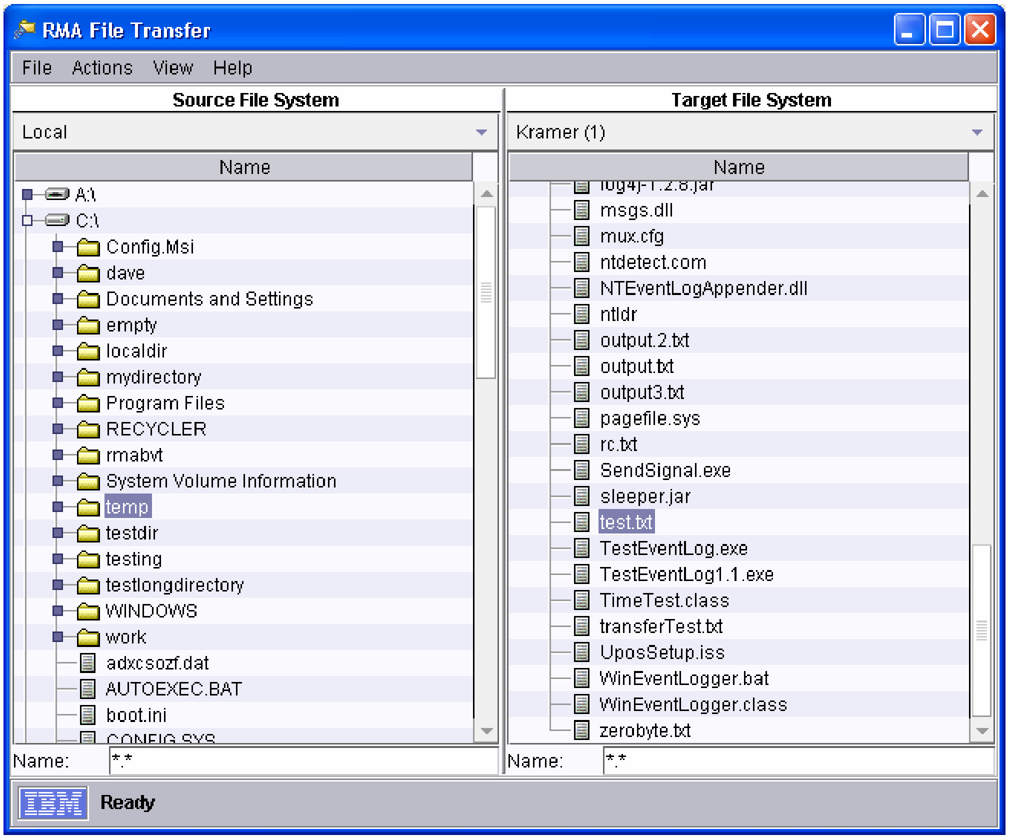
The "RMA File Transfer" task appears in the tasks pane in the Director Console, and can be launched like any other task, with the caveat that it can only be used on a single system at a time:

- Drag-and-drop to a single managed object
- Right-click a single managed object and use the context menu to select "RMA File Transfer"
- Use the console toolbar or "tasks" menu

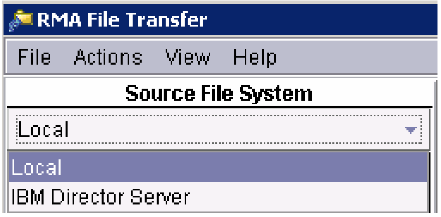


Using the RMA File Transfer Task

Once you launch the RMA File Transfer task, you will see the "RMA File Transfer" window appear, as shown below.

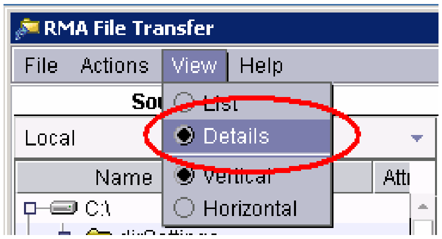


The "Source File System" on the left can be set to show the file tree from either the local system where you are running the IBM Director Console, or the IBM Director Server system itself. To change between those systems, simply click on the drop box at the top of the panel:

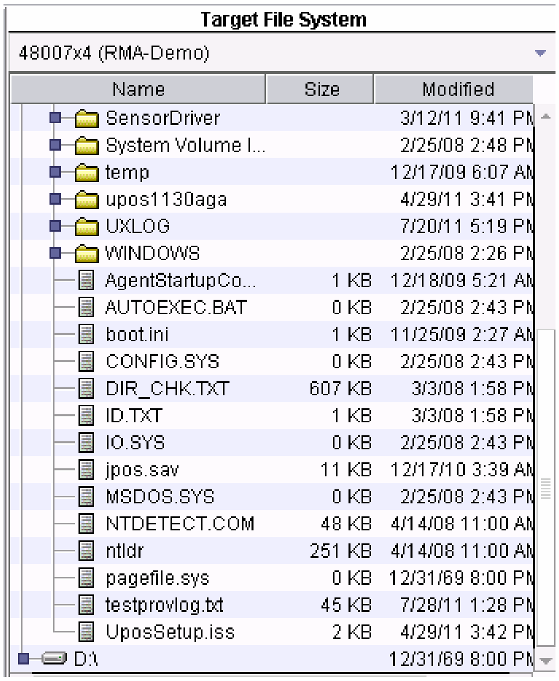


The "Target File System" will only show the file tree from the RMA Agent system.

If you would like to view file attributes on either the source or target systems, select “Details” from the “View” menu:



This may slow down the performance of the RMA File Transfer task, but will show more detailed information such as file sizes and last modified dates:



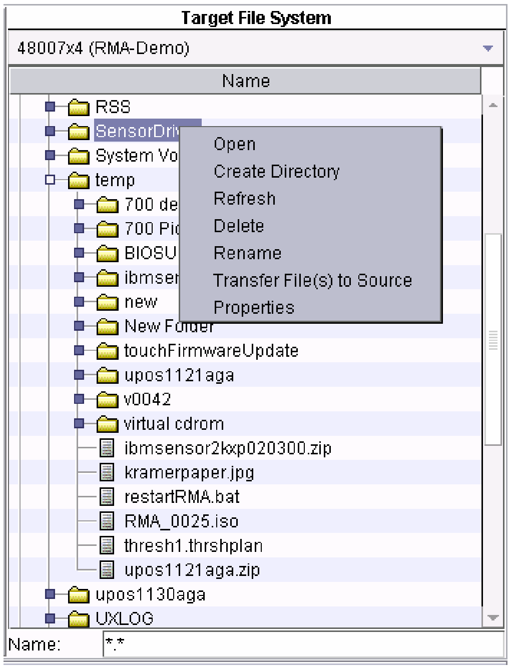
Target File System

48007x4 (RMA-Demo)

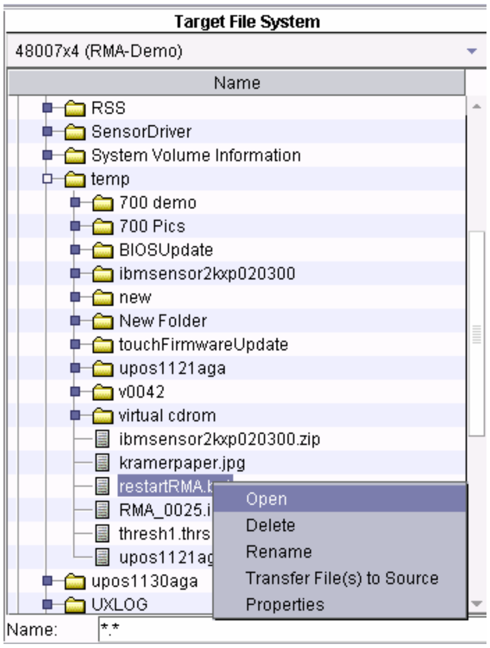
Name	Size	Modified
SensorDriver		3/12/11 9:41 PM
System Volume I...		2/25/08 2:48 PM
temp		12/17/09 6:07 AM
upos1130aga		4/29/11 3:41 PM
UXLOG		7/20/11 5:19 PM
WINDOWS		2/25/08 2:26 PM
AgentStartupCo...	1 KB	12/18/09 5:21 AM
AUTOEXEC.BAT	0 KB	2/25/08 2:43 PM
boot.ini	1 KB	11/25/09 2:27 AM
CONFIG.SYS	0 KB	2/25/08 2:43 PM
DIR_CHK.TXT	607 KB	3/3/08 1:58 PM
ID.TXT	1 KB	3/3/08 1:58 PM
IO.SYS	0 KB	2/25/08 2:43 PM
jpos.sav	11 KB	12/17/10 3:39 AM
MSDOS.SYS	0 KB	2/25/08 2:43 PM
NTDETECT.COM	48 KB	4/14/08 11:00 AM
ntldr	251 KB	4/14/08 11:00 AM
pagefile.sys	0 KB	12/31/69 8:00 PM
testprovlog.txt	45 KB	7/28/11 1:28 PM
UposSetup.iss	2 KB	4/29/11 3:42 PM
D:\		12/31/69 8:00 PM

Modifying Files and Folders

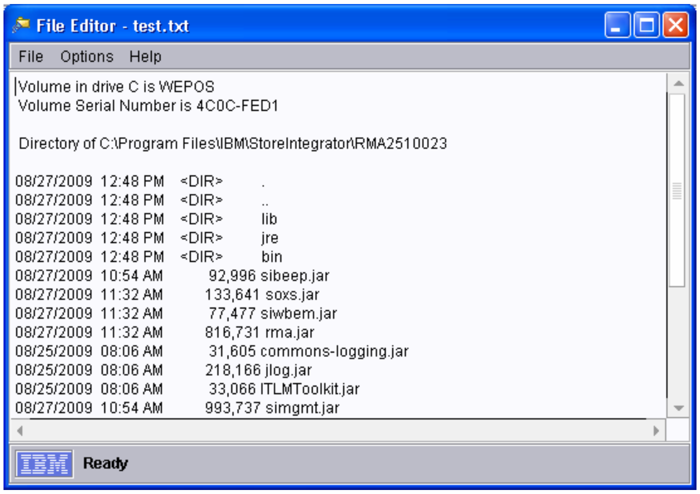
To create, delete, or rename a directory on the target file system, simply right-click and select the proper option:



Similarly, to edit, delete, or rename a file, right-click on the file and select the proper option:



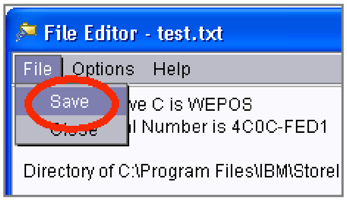
If you choose to “Open” the file, the “RMA File Transfer” task will launch a text editor on the file:



```
|Volume in drive C is WEPOS
 Volume Serial Number is 4C0C-FED1

 Directory of C:\Program Files\IBM\StoreIntegrator\RMA2510023

08/27/2009  12:48 PM    <DIR>          .
08/27/2009  12:48 PM    <DIR>          ..
08/27/2009  12:48 PM    <DIR>          lib
08/27/2009  12:48 PM    <DIR>          jre
08/27/2009  12:48 PM    <DIR>          bin
08/27/2009  10:54 AM            92,996 sibeep.jar
08/27/2009  11:32 AM           133,641 soxs.jar
08/27/2009  11:32 AM            77,477 siwbem.jar
08/27/2009  11:32 AM           816,731 rma.jar
08/25/2009  08:06 AM            31,605 commons-logging.jar
08/25/2009  08:06 AM           218,166 jlog.jar
08/25/2009  08:06 AM            33,066 ITLMToolkit.jar
08/27/2009  10:54 AM           993,737 simgmt.jar
```

Note: You should only “Open” files that are readable in a text editor.

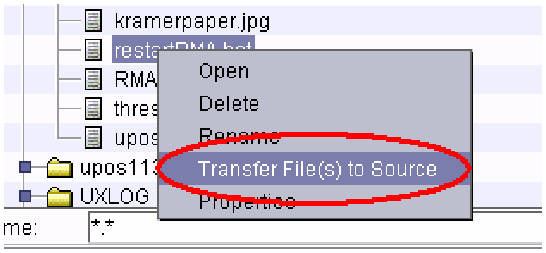
From there, you can make any changes that you choose and then select “File / Save” to save the file back to the remote system’s hard drive:

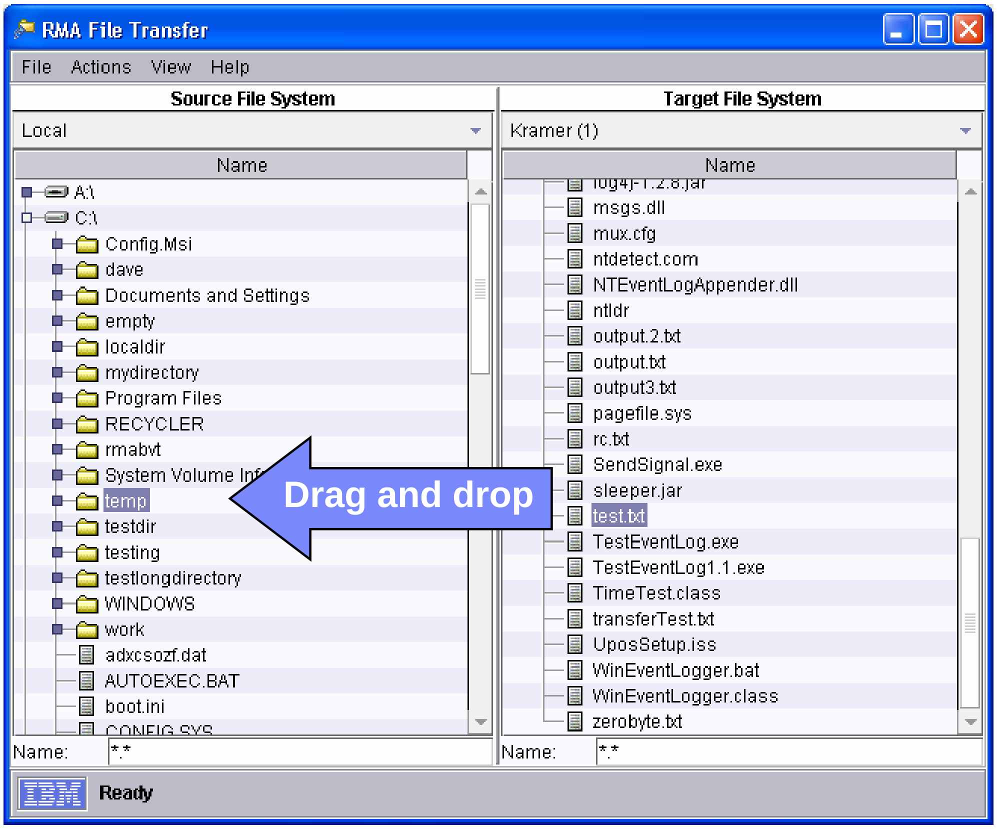


```
ve C is WEPOS
l Number is 4C0C-FED1

Directory of C:\Program Files\IBM\StoreI
```

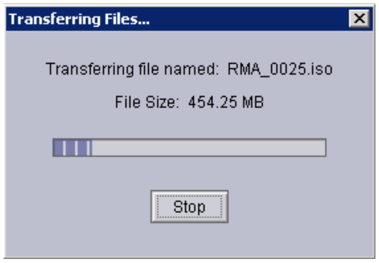
Transferring Files and Folders

To transfer files and folders between the target file system running an RMA Agent and the source file system on your local system or Director Server, either right-click and select the transfer option or simply drag and drop between the two columns:





Either of these options will initiate a file transfer between the systems. While the file is being transferred you will see a progress bar indicating what percentage of the transfer is complete:

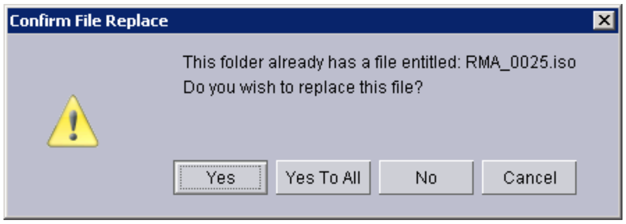

Transferring Files...

Transferring file named: RMA_0025.iso

File Size: 454.25 MB

At any point the transfer can be canceled by clicking the “Stop” button in the “Transferring Files” window.

If a file or folder already exists on the system where it is getting transferred, then a pop-up will be displayed with options as to how to proceed:


Confirm File Replace

This folder already has a file entitled: RMA_0025.iso
Do you wish to replace this file?

Chapter 13 – Getting Support

How to open a PMR for RMA

If you encounter a problem that you believe is due to a defect in the software, then you should open a PMR (Problem Management Record). Follow the instructions below to open a PMR and to include the necessary documentation.

1. Contact your geography-specific IBM support representative. In the United States, call 1-888-IBM-HELP. It's also possible to open a PMR on the web, using the instructions below: http://www-1.ibm.com/support/docview.wss?rs=219&&uid=pos1R1003779

2. To speed up the process, tell your support representative that you would like to open a PMR with component ID "5639ff100". (This will be routed to the "SIF,112" queue.) Please include as much detail as possible when opening the PMR.

3. After you've been given a PMR number, you must submit any additional documentation for your PMR using the documentation standards described below: http://www-01.ibm.com/support/docview.wss?rs=219&uid=pos1R1001365

> **Note**: It is very important to submit all the relevant documentation (including screenshots, log files, config files, etc.). It is also very important that you use the naming conventions described in the article above, as this will prevent any unnecessary delays in the process.

4. At a minimum, you should collect RMA and IBM Director logs that demonstrate the problem. (Use the documentation standards above to submit this information.) You should also report the exact version numbers that are being used for all relevant software components. See the example below ("**How to Collect RMA and Director Log Files for Problem Analysis**") for more information on collecting the necessary log files.

5. It's also a good idea to include any configuration files or screenshots that demonstrate the problem. Include any additional information you can provide to help the support team understand and reproduce your problem.

How to Collect RMA and Director Log Files for Problem Analysis

If you experience a problem with RMA and/or the Retail Extensions for IBM Director, the instructions below will help you collect the necessary log files to troubleshoot the problem.

Note: This article assumes that Director is installed in "C:\Program Files\IBM\Director", and all paths are given using Windows path formatting. If you've installed Director to a different location within Windows, or if you're running Director on Linux, then you'll need to take note of the path differences as you follow these instructions.

Note: This article does not cover advanced logging configuration, or how to take javacore or javaheap dumps. This article also does not cover how to configure advanced logging for RMA. If this additional information is needed, IBM technical support will give you additional instructions to collect the extra information. (You can also refer to the RMA user's guide for additional information.)

Collecting logs from IBM Director:

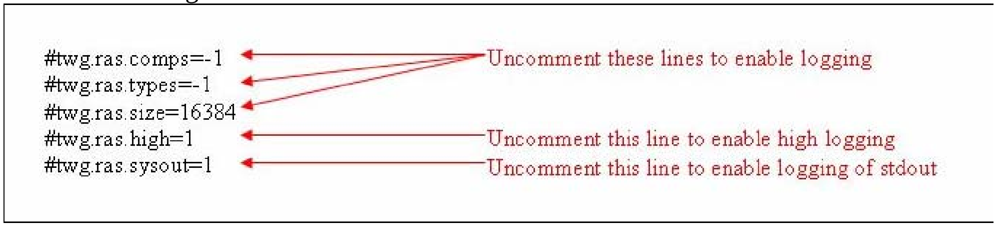
1. Enable RAS logging on the IBM Director Server and/or Console. (If you are using the Director Console on a separate system, this step should be done separately for both the Director Server and the Director Console; otherwise, it only needs to be done once.)

   Note: Logging should never be enabled in a production environment except when gathering data for a problem. The performance impact of enabling logging in IBM Director is quite high.

   To enable RAS logging, do the following:

   - Make a backup copy of the file "C:\Program Files\IBM\Director\data\twgras.properties". (After you are finished collecting data, you will restore this backup file.)

   - Open the file "twgras.properties" using the text editor of your choice. Typically, you will only need to remove the "#" symbols at the beginning of each line in this file. Be sure to save your changes when you are finished editing. When you are finished, the file should look like the following:



```
#twg.ras.comps=-1
#twg.ras.types=-1
#twg.ras.size=16384
#twg.ras.high=1
#twg.ras.sysout=1
```

Uncomment these lines to enable logging
Uncomment this line to enable high logging
Uncomment this line to enable logging of stdout

Note: Later, when you are completely finished collecting log files from Director, you should restore your backup copy of the original

> “twgras.properties” file, then close the Director Console and restart the Director Server. (If you do not restore your backup copy, you will experience performance problems with Director!)

2. After you’ve enabled RAS logging (on both the Director Server and on the Director Console if you are using a separate system for the Console), close the Director Console and restart the Director Server.

3. Launch the Director Console using the following commands:

   ```
   cd “C:\Program Files\IBM\Director”
   twgjava com.tivoli.console.ConsoleLauncher > console.log
   ```

4. Log into the Director Console, and perform any steps needed to recreate your problem (i.e. reproduce the problem for which you want to collect log information). If possible, close the Director Console when finished reproducing the problem.

5. After you’ve reproduced your problem, run the following commands on the Director Server:

   ```
   cd “C:\Program Files\IBM\Director\log”
   rasdump –high > server.log
   ```

6. Collect all the following files (for both the Console and the Server, if running on separate systems):
   a. C:\Program Files\IBM\Director\console.log (for the Console only)
   b. C:\Program Files\IBM\Director\log\server.log (for the Server only)
   c. C:\Program Files\IBM\Director\log\*.err (if any exist)

Collecting logs from RMA master and general agents:

1. Reproduce the problem using the steps described above.

2. Collect the following files from the relevant RMA master and general agents
   a. “%SI_HOME%\silogs\simgmt.*”
   b. “%SI_HOME%\silogs\simgmt_m.*”
   c. “%SI_HOME%\silogs\rma.stderr”
   d. “%SI_HOME%\silogs\rma.stdout”
   e. “%SI_HOME%\silogs\rmacimtrc.log”

   Note that you can also replace “%SI_HOME%” in the paths above with the location of your SI home directory, which is typically “C:\Program Files\IBM\StoreIntegrator”.

3. If you would rather collect these RMA log files remotely (i.e. using Director), you can use RMA data capture to collect them. (See “**Chapter 11 – Data Capture**” for an example.)

Note: If you are debugging a problem related to connections, file transfer, software distribution, or data capture, it is not a good idea to collect the log files remotely – you should get them manually from each system.