Best Practices for Monitoring Cisco Unity Devices with Cisco Unified Operations Manager

Contents

Introduction

This document highlights suggested best practices for field personnel and customers. It will enable you to effectively monitor Cisco Unity® devices. Other documents that address the management of the other Cisco Unified Communications components are available. This document does not replace the User Guide for Cisco Unified Operations Manager, which is available on Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/cisco_unified_operations_manager/2.0.1/user/guide/userguid.html.

In addition, you will find the best practices document for deployment topics such as initial device setup, installation guidelines, server sizing, and so on, at http://www.cisco.com/en/US/products/ps6535/prod_white_papers_list.html.

About Cisco Unified Operations Manager

Cisco® Unified Operations Manager (referred to as Operations Manager from this point forward) provides a unified view of the entire IP communications infrastructure. It presents the current operational status of each element of the IP communications network. Operations Manager continuously monitors the current operational status of different IP communications elements, such as:

- Cisco Unified Communications Manager
- Cisco Unified Communications Manager Express
- Cisco Unity devices
- Cisco Unity Express
- Cisco Unified Contact Center
- Cisco Unified Contact Center Express
- Cisco Unified Presence Server
- Cisco Emergency Responder
- Cisco Unified MeetingPlace® Express
- Cisco gateways, routers, switches, and IP phones

Cisco Unified Operations Manager (OM) also provides diagnostic capabilities for faster trouble isolation and resolution. It monitors and evaluates the current status of both the IP communications infrastructure and the underlying transport infrastructure in the network. It uses open interfaces such as Simple Network Management Protocol (SNMP), Hypertext Transfer Protocol (HTTP), and Windows Management Instrumentation (WMI) to remotely poll data from different devices in your IP communications deployment. Because Operations Manager does not deploy any agent software on the devices being monitored, it is nondisruptive to your system operations.

Managing Cisco Unity Devices

For Cisco Unified Operations Manager to manage a Cisco Unity device properly, the appropriate Remote Serviceability Kit (RSK) must be installed on the Cisco Unity device. You can load the RSK from http://www.ciscounitytools.com/App_RSK.htm. See the Appendix for a detailed installation guide.

After RSK is installed, you should add the Cisco Unity device to Operations Manager using **Devices** > **Device Management** > **Add Devices**. To add a Cisco Unity device, you need to keep the following information nearby:

- The IP address or hostname
- The SNMP read-only credentials
- The Windows login credentials: The OS credentials (the same credentials you enter when you log in to Windows)

Once the Cisco Unity device is added and Operations Manager has collected the required inventory details from the device, Operations Manager marks the device as Monitored. This signals that the Cisco Unity device has been successfully added and is being managed by Operations Manager.

For information on why your devices are not going into the Monitored state, see the following:

- Why Does a Device Go into the Partially Monitored State?
- Why Does a Device Go into the Unreachable State?

Once the Cisco Unity device is in the Monitored state, you can open the Service Level View from the Operations Manager Monitoring Dashboard. You can find the Cisco Unity device that you have just added in the tree view in the left corner, by navigating to **System Defined Groups** > **Cisco Unified Communications Applications** > **Unity**.

Figure 1. Entry Point for Managing Cisco Unity Devices

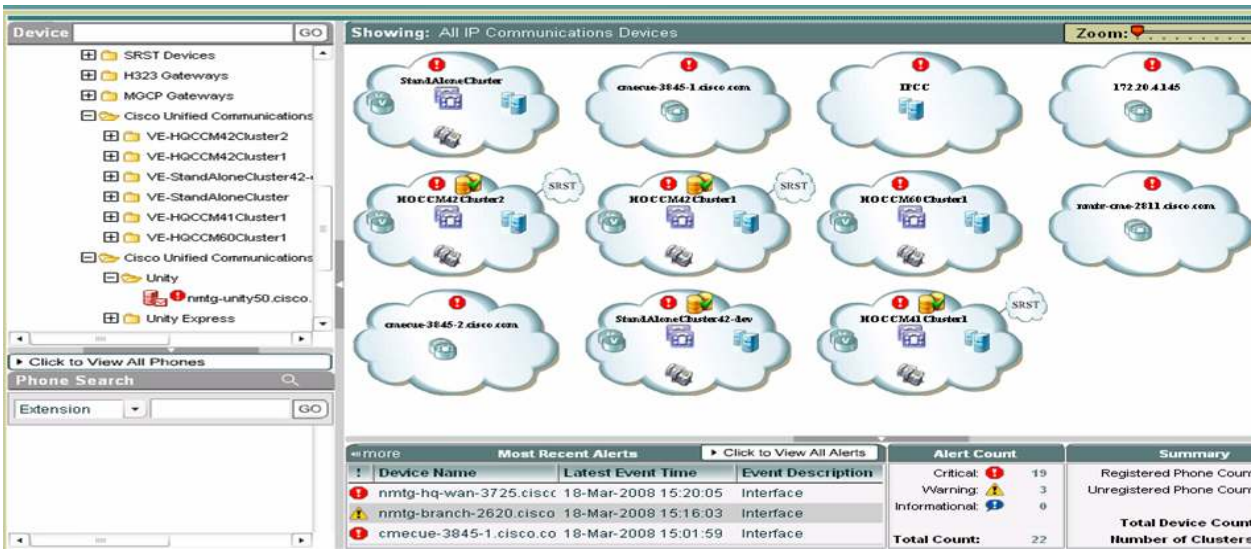


Figure 1 shows one of the main entry points for managing the devices. By right-clicking the device in the tree view, you can see a list of context-sensitive tools that can be performed on that device. Figure 2 shows the list of context-sensitive tools.

Figure 2. The List of Context-Sensitive Tools

In the remainder of this document, we will go through all of these tools in detail.

Basic Health Monitoring

Table 1 lists the system, environment, and application parameters that Operations Manager monitors on a Cisco Unity device.

Table 1. Basic Health Monitoring

Monitored Parameters	Description
System	Usage of processor, hard disk, virtual memory, and RAM, along with status of interfaces on the Media Convergence Server device hosting the Cisco Unity device
Environment	Status of system fan, system temperature sensor, and system power supply of the MCS device hosting the Cisco Unity device
Application	Status of all critical applications running on the Cisco Unity MCS device and the usage of the Cisco Unity ports configured on it

You can see the details of these parameters by launching the Detailed Device View right-click option on the device from the Service Level View.

Fault Monitoring

View the list of active alarms on a Cisco Unity device by launching the Alert Details right-click option on the device from the Service Level View. Clicking the event ID displays the event details, which indicate the exact nature of the event.

You can also view the alarm history on a Cisco Unity device by launching the Alert History right-click option on the device from the Service Level View.

Table 2 lists the fault conditions Operations Manager monitors and provides alerts for when they are detected on a Cisco Unity device.

Table 2. Fault Monitoring

Fault Condition	Event Details
High CPU utilization	**HighUtilization** **Event Description:** HighUtilization is raised when the CPU utilization at the system level exceeds the Processor Utilization Threshold. **Default Polling Interval:** 4 minutes **Default Threshold: 90%** **Recommended Actions:** Check the Cisco Unity Windows Task Manager to verify high CPU utilization. The most common reason is that one or more processes are using excessive CPU. Once the process is identified, you might want to take action, which could include restarting the process. **cpuUtilizationExceeded** **Event Description:** This event is raised when the CPU utilization at the process level exceeds the Processor Utilization Threshold. **Default Polling Interval:** 4 minutes **Default Threshold:** 90% **Recommended Actions:** Check the Cisco Unity Windows Task Manager to verify high CPU utilization. Check event details to identify the process that uses excessive CPU. Once the process is identified, you might want to take action, which could include restarting the process.
Insufficient physical memory (RAM)	**InsufficientFreeMemory** **Event Description:** This event indicates that the available physical memory is running low. The event is based on a comparison of the percentage of free physical memory against the Free Physical Memory Threshold. **Default Polling Interval:** 4 minutes **Default Threshold:** 15% **Recommended Actions:** Check the Cisco Unity Windows Task Manager to verify insufficient memory. It is important to identify which process is using excessive memory. Once the process is identified, if you suspect a memory leak (for example, if the memory usage for a process increases continually, or a process is using more memory than it should), you may want to restart that process.

Insufficient virtual memory	**InsufficientFreeVirtualMemory** **Event Description:** Check the Cisco Unity Windows Task Manager to verify insufficient memory. This event indicates that available virtual memory is running low. Virtual memory consists of physical memory and swap memory. The event is based on a comparison of the percentage of free virtual memory against the Free Virtual Memory Threshold. **Default Polling Interval:** 4 minutes **Default Threshold:** 15% **Recommended Actions**: See **Error! Reference source not found.**
System fan is down or degraded	• **FanDown** ◦ **Event Description:** This event indicates that a required fan is not operating correctly. The event is based on processing the SNMP trap cpqHeThermalSystemFanFailed received from the monitored device. ◦ **Default Threshold:** N/A ◦ **Recommended Actions:** Contact Cisco for hardware replacement. • **FanDegraded** ◦ **Event Description:** This event indicates that an optional fan is not operating correctly. The event is based on polling or processing the SNMP trap cpqHeThermalSystemFanDegraded received from monitored Cisco Unified Communications Managers. ◦ **Default Threshold:** N/A ◦ **Recommended Actions:** Monitor for recurrence.
System chassis temperature is high	**TemperatureHigh** **Event Description:** This event is generated if a temperature sensor's current temperature exceeds the Relative Temperature Threshold. **Default Polling Interval:** 4 minutes **Default Threshold:** 10% **Recommended Actions:** Verify that room temperatures are set up optimally. Check other events such as FanDown or FanDegraded to verify that fans are operating normally. If not, you should contact Cisco for hardware replacement.
System temperature sensor is down or degraded	• **TemperatureSensorDown** ◦ **Event Description:** This event indicates that the server temperature is outside of the normal operating range and the system will be shut down. The event is based on processing the SNMP trap cpqHeThermalTempFailed received from a monitored device. ◦ **Default Threshold:** N/A ◦ **Recommended Actions:** Verify that room temperatures are set up correctly. Check other events such as FanDown or FanDegraded to verify that system fans are operating normally. Contact Cisco for hardware replacement, if needed. • **TemperatureSensorDegraded** ◦ **Event Description:** This event indicates that the server temperature is outside of the normal operating range. The event is based on polling or processing the SNMP trap cpqHeThermalTempDegraded received from a monitored device. ◦ **Default Threshold: N/A** ◦ **Recommended Actions:** Check other events such as FanDown or FanDegraded to verify that system fans are operating normally. Contact Cisco for hardware replacement, if needed.
System power supply is down or degraded	• **PowerSupplyDown** ◦ **Event Description:** Power supply is down. ◦ **Default Polling Interval:** 4 minutes ◦ **Default Threshold:** N/A ◦ **Recommended Actions:** Contact Cisco for hardware replacement if the primary power supply is down. • **PowerSupplyDegraded** ◦ **Event Description:** Power supply state is degraded ◦ **Default Polling Interval:** 4 minutes ◦ **Default Threshold:** N/A ◦ **Recommended Actions:** Monitor for recurrence.
Any critical application stops running	**ServiceDown** **Event Description:** This event is generated when one of the critical services (any of the services in the Detailed Device View) is not running. The problem could be due to someone manually stopping the service. If you intend to stop the service for a long period of time, disabling monitoring for the service is highly recommended and is needed to avoid this alert. **Go to Service Level View** > **Detailed Device View**, select the specific service, and change the managed state to False. **Default Polling Interval:** 4 minutes **Default Threshold:** N/A **Recommended Actions:** Identify which service is not running. Monitor the Detailed Device View to see if the service comes back up. Restart the service if it is still down. Also, check to see if there are any user dumps, and examine the application event log for error messages.

High number of Cisco Unity ports (inbound or outbound) are active	**HighPortUtilization** **Event Description:** This event is generated when the percentage of Cisco Unity port utilization exceeds the Active InBound Ports Threshold or the Active OutBound Ports Threshold. **Default Polling Interval:** 4 minutes **Default Threshold:** 90% **Recommended Actions:** This event is a signal to assess whether you need additional voice mail ports.
Available inbox license low	**AvailableInboxLicenseLow** **Event Description:** The number of available inbox licenses is under the Unity Inbox License Threshold. **Default Polling Interval:** 4 minutes **Default Threshold:** 10% **Recommended Actions:** This event is a signal to assess whether you need additional inbox licenses.
Available license low	**AvailableLicenseLow** **Event Description:** Number of available licenses are fewer than Unity License Threshold **Default Polling Interval:** 4 minutes **Default Threshold:** 10% **Recommended Actions:** This event is a signal to assess whether you need additional licenses.
UMR communication error	**UMRCommunicationError** **Event Description:** This event is based on WMI. It indicates that the Cisco Unity Message Repository (UMR) cannot communicate with the Partner Mail Server to deliver messages. Messages will be held in the temporary store until the mail server is available. **Default Polling Interval:** N/A **Default Threshold:** N/A **Recommended Actions:** Verify that the partner mail server, including the mailstore, is online, and that Cisco Unity devices can connect to it. If the partner mail server is online and reachable, to diagnose the problem, enable all the micro traces for the AvUMRSyncSvr service, restart the service, and examine the logs.
Cisco Unity failover	**UnityFailOverOrRestart** **Event Description:** This event is based on WMI. The event is generated under one of the following conditions: • In a standalone Cisco Unity configuration: Indicates that the Cisco Unity system has rebooted or restarted. • In a Cisco Unity failover configuration: A failover between the primary and secondary Cisco Unity servers has occurred. **Note:** UnityFailOverOrRestart is automatically cleared after 30 minutes. Clearing of this event does not indicate that failback has occurred. When failback does occur from secondary to primary, you will see the UnityFailOverOrRestart event on the primary Cisco Unity server. **Default Polling Interval:** N/A **Default Threshold:** N/A **Recommended Actions:** This event indicates that Cisco Unity restarted or that failover occurred. Check the Cisco Unity window event view for any error messages related to failover or restart. When a failover occurs, the changes made to the data in the SQL Database (UnityDb) are replicated from the primary server to the secondary server. However, there might be instances when these changes are not replicated from the primary server to the secondary server. For more details, go to http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_tech_note09186a0080837de4.shtml.

Polling and Thresholds

You can configure the interval at which Operations Manager polls the specific information from the Cisco Unity device, as well as set the thresholds based on which alerts should be raised by Operations Manager.

Configure polling intervals by launching the Polling Parameters right-click option on the device from the Service Level View. The polling parameters are defined in the System Defined Groups/Cisco Unified Communications Applications/Unity group. Configure polling setting related to basic health monitoring by selecting the Voice Health Settings parameter type (Table 3).

Table 3. Configuring Polling Settings

Parameters	Polling Settings
System	• Hard disk and virtual memory settings • MCS processor and memory utilization settings • MCS Ethernet interface settings
Environment	Environment: Power supply, fan, and temperature sensor settings
Application	Application polling settings

You can configure the thresholds by launching the Threshold Parameters right-click option on the device from the Service Level View. The threshold parameters (Table 4) are defined in the System Defined, Cisco Unified Communications Applications, and Unity groups. You can configure the threshold setting related to basic health monitoring by selecting the Voice Health Settings parameter type. You can choose from four threshold categories depending on the exact threshold that you need to configure.

Table 4. Configuring Threshold Settings

Parameter	Threshold Settings
System	• Disk usage and virtual memory settings • Processor and memory settings
Environment	Environment: Temperature sensor settings
Application	Cisco Unity threshold settings

Performance Monitoring

Operations Manager performs trending of the following parameters on a Cisco Unity device:

- Total CPU usage
- Total memory usage
- Inbound port utilization
- Outbound port utilization

View the performance report or graphs over the past 72 hours by launching the Performance right-click option on the device from the Service Level View, and then selecting the appropriate performance parameter that you wish to view. You can view multiple performance reports or graphs in a single screen.

By default, performance polling for a Cisco Unity device is disabled in Operations Manager. To enable performance polling for a Cisco Unity device, launch the Polling Parameters Page, select the **Voice Utilization Settings** parameter type, and then check the **Polling Enabled** check box. Click **Apply** for the changes to take effect.

You can also configure the thresholds for the performance parameters by launching the Thresholds Parameter Page and selecting Voice Utilization Settings as the parameter type.

Synthetic Tests

You can perform an MWI Test on your Cisco Unity device to determine if there is any significant latency in the Cisco Unity device in handling voice messages. The MWI Test validates by placing a voice message for a phone and checking the time it takes for the MWI ON message to be sent by Cisco Unified Communications Manager from the instant the voice message is placed. If it takes too long and exceeds the configurable threshold for the time interval, a MWIOnTimeExceeded event is raised.

You can set up this test on your Cisco Unity device by launching the Message Waiting Indicator Test right-click option on the device from the Service Level View.

You can also configure the time for which the test waits to receive the MWI ON message by launching the Thresholds option, selecting Voice Health Settings as the parameter type, and selecting the MWI Threshold Settings as the threshold category.

Physical Connectivity

View the Layer 2 or Layer 3 connectivity of the network in which your Cisco Unity device resides by launching the Connectivity Details right-click option on the device from the Service Level View.

Logical View

View the association of a Cisco Unity device's ports with the Cisco Unified Communications Manager in the Service Level View. You can search for the Cisco Unity device in the Service Level View by providing the managed name of the device. If the Cisco Unity device is associated with a Cisco Unified Communications Manager cluster that is managed by Operations Manager, then upon searching, that Cisco Unity device is visible under the Application Servers of the Cisco Unified Communications Manager cluster to which it is associated. Clicking the device launches the Map View in the right pane, showing the Logical Connectivity View.

Device Troubleshooting

Open the Cisco Unity Administration Page by launching the Cisco Unity Administration right-click option on the device from the Service Level View.

Device Administration

Suspend or resume monitoring of a Cisco Unity device by launching the Suspend Device or Resume Device right-click option on the device from the Service Level View. When the device is in the Suspended state, it no longer communicates with Operations Manager. You might want to do this to avoid false alarms when the Cisco Unity device is in Maintenance mode. You can also delete the Cisco Unity device from Operations Manager by launching the Delete Device right-click option on the device from the Service Level View.

Recommendations on Monitoring Important Cisco Unity Components with Operations Manager

Recommendations on Performance Monitoring

We recommend that you generate daily graphs and seven-day reports for trend analysis. A seven-day report establishes baseline for the Cisco Unity system.

To generate a daily graph, go to the Service Level View and launch the Performance right-click option on the device, then select the appropriate metric and time that you want to view. Operations Manager gives you a real-time report over the past 72 hours.

You can generate a server-day (or longer) report using Cisco Unified Service Statistics Manager.

As part of the Cisco Unified Communications Management Suite, Cisco Unified Service Statistics Manager extracts the data from Operations Manager and provides advanced statistics analysis and reporting capabilities for Cisco Unified Communications deployments.

The performance data is stored as comma-separated values (CSV) files for a period of 72 hours, in the following location: C:\Program Files\CSCOpx\data\gsu_#GSUdata#_. If you want data for a period of more than 72 hours, you must manually copy the CSV files to another location.

CPU Usage

View the performance report or graphs for Total CPU Usage (Percentage) on a Cisco Unity device by launching the Performance right-click option on the device from the Service Level View. The Maximum and Average data provides trending information.

You can also view each processor's CPU utilization in 5-minute increments by launching the Detailed Device View right-click option on the device from the Service Level View.

Virtual Memory and Physical Memory Usage

View the performance report or graphs for Memory Usage (Percentage) on a Cisco Unity device by launching the Performance right-click option on the device from the Service Level View. Minimum and average values are used for establishing system growth needs. Maximum free memory values are used to detect memory leaks.

You can see Virtual Memory/Physical Memory Used, Virtual Memory/Physical Memory Total Size, and Free Virtual Memory/Physical Memory (%) by launching the Detailed Device View.

Hard Disk Status and Usage

You should closely monitor the usage of disk space on your Cisco Unity servers, especially if logs are activated. You can avoid many problems altogether if you proactively manage log file sizes.

View Hard Disk Used, Hard Disk Total Size, and Free Hard Disk (%) for each disk by launching the Detailed Device View

High Temperature Condition

View the current temperature and default threshold for each temperature sensor by launching the Detailed Device View.

Voice Mail Port Availability

The availability of voice mail ports is vital to the overall reliability that users expect from Cisco Unity.

View the performance report or graphs for Inbound Port Utilization (Percentage) or Outbound Port Utilization (Percentage) on a Cisco Unity device by launching the Performance right-click option on the device from the Service Level View.

You can also view the Cisco Unity Usage counters (Total Ports, Active Ports, Percentage of Active Ports, Total Inbound Ports, Active Inbound Ports, Percentage Active Inbound Ports, Total Outbound Ports, Active Outbound Ports, Percentage Active Outbound Ports) by launching the Detailed Device View right-click option on the device from the Service Level View.

Voice Mail Port Status

View current status of all voice mail ports by selecting the Unity Ports options in the Detailed Device View.

General Usage

You can view general statistics on the following in the Detailed Device View:

- Total number of Cisco Unity ports
- Number of ports that are currently active with calls
- Number of inbound ports
- Number of outbound ports
- Number of inbound ports that are currently active
- Number of outbound ports that are currently active
- Cisco Unity version
- Total Cisco Unity text-to-speech sessions
- Current number of licensed subscribers
- Maximum number of licensed subscribers
- Current number of Inbox licenses
- Maximum number of Inbox licenses

Recommendations on Events for Notification Service

The following are the most important Cisco Unity-related events, for which you can request email, e-page, or SNMP trap notification. See Fault Monitoring for recommended actions.

Caution: The following recommendations for critical items to be monitored are deployment specific and should be customized for individual customers. Based on bandwidth availability, especially slow speed WAN links, the polling intervals might need to be adjusted. Thresholds might need to be adjusted based on your baseline data.

Events Associated with CPU

HighUtilization

HighUtilization is raised when the CPU utilization at system level exceeds the threshold. The default polling interval is 4 minutes, and the default threshold is 90%. The polling interval can be tuned to as low as 1 minute. Cisco recommends a 2-minute polling interval.

Events Associated with Virtual Memory and Physical Memory

InsufficientFreeVirtualMemory

This event indicates that available virtual memory is running low. Virtual memory consists of physical memory and swap memory. The event is based on a comparison of the percentage of free virtual memory against a configured threshold. The default threshold is 15%. The polling interval can be tuned to as low as 1 minute. Cisco recommends a 2-minute polling interval

InsufficientFreeMemory

This event indicates that available physical memory is running low. The event is based on a comparison of the percentage of free physical memory against a configured threshold. The default threshold is 15%.

Events Associated with Hard Disk

InsufficientFreeHardDisk

This event indicates that available hard disk space is running low. The event is based on a comparison of the percentage of free hard disk against a configured threshold. The default threshold is 15%.

DataPhysicalDiskDown

A Cisco Unity hard-drive failure event has occurred.

Events Associated with High Temperature

TemperatureSensorDown

This event indicates that the server temperature is outside of the normal operating range and the system will be shut down.

TemperatureHigh

This event is generated if a temperature sensor’s current temperature is higher than the threshold.

Events Associated with Power Supply

PowerSupplyDown

This event is generated if the power supply is down.

Events Associated with Fan

FanDown

This event is generated if the primary fan is down.

Critical Service-Associated Events

ServiceDown

This event is generated when one of the critical services (any of the services in the Detailed Device View) is currently not running. This could be due to someone manually stopping the service. If you intend to stop the service for a long period of time, disabling monitoring for the service is highly recommended and is needed to avoid this alert.

Events Associated with Port Availability

HighPortUtilization

This event is generated when the percentage of Cisco Unity port utilization threshold exceeds the threshold.

Events Associated with Cisco Unity Failover

UnityFailOverOrRestart

This event is generated under one of the following conditions:

- In a standalone Cisco Unity configuration: Indicates that the Cisco Unity system has rebooted or restarted.
- In a Cisco Unity failover configuration: A failover between the primary and secondary Cisco Unity servers has occurred.

UMRCommunicationError

This event indicates that the Cisco Unity Message Repository cannot communicate with the Partner Mail Server to deliver messages. Messages will be held in the temporary store until the mail server is available.

Managing Events and Notifications

Steps to Take to Reduce False Alerts and Notifications

1. Disable polling for interfaces and services that are administratively down. Until you do this, Operations Managers will appear to report false alerts.

   Go to **Service Level View** > **Detailed Device View** (right-click option of the device), select the specific service, and change Managed State to False.

2. Reduce the notification to only critical events that are deemed to immediately affect voice services. See Recommendations on Events for Notification Service.
3. (Optional) Customize device thresholds to fine tune notification, if needed.

Note that alerts in Operations Manager are events. If both alerts and events are checked, when creating a notification, it may appear to a manager of managers (MOM) as if Operations Manager is sending duplicate alarms. Best practice is to select only Event Severity and not Alert Severity when creating a notification, especially for MOMs. You must also select Informational for cleared events to be included in the notification.

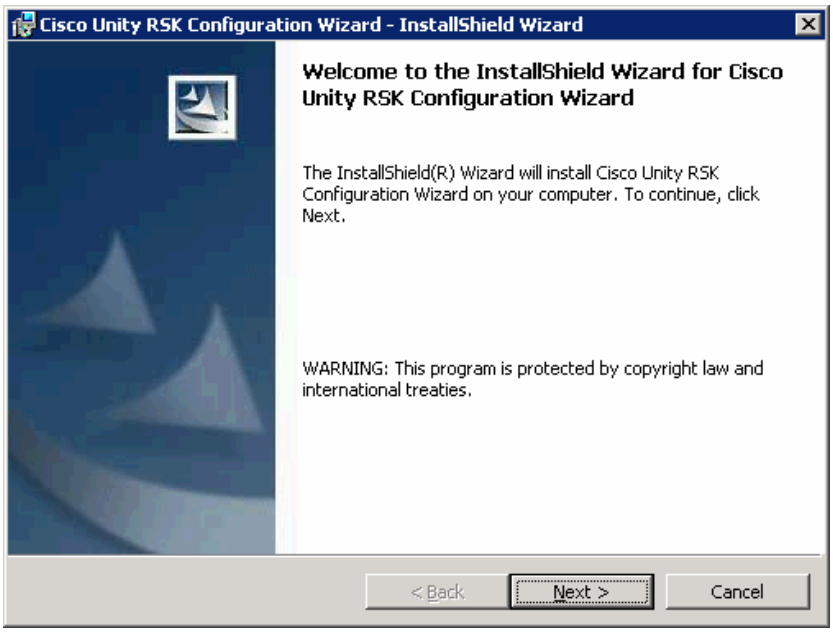
Appendix

Installing Cisco Unity Plug-Ins

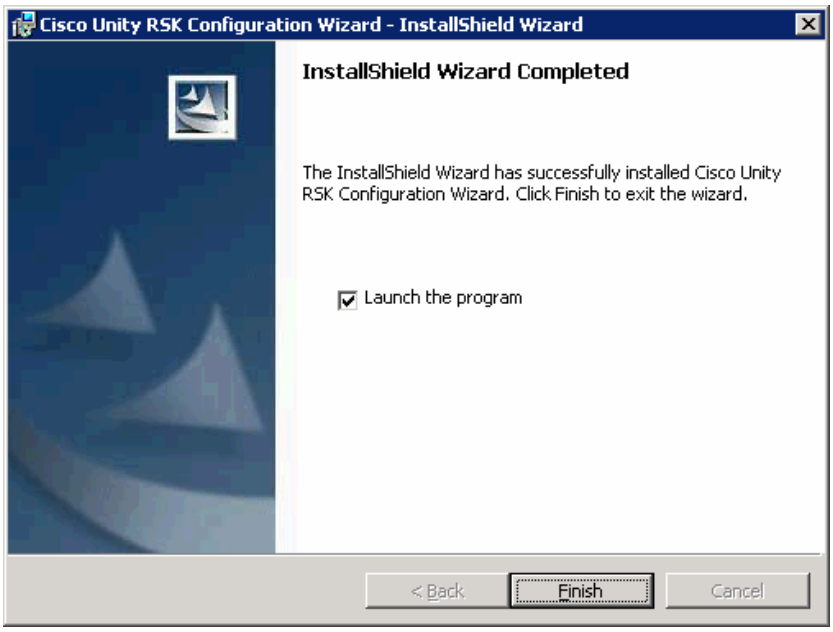
For Cisco Unity and Cisco Unity Connection, two plug-ins must be installed. The Event Monitoring Service (EMS) and the Remote Serviceability Kit (RSK) should be installed for Operations Manager, or any SNMP MIB poller, to fully manage Cisco Unity (RSK provides the Unity-MIB) devices. EMS is optional but highly recommended. Typically, you should install the EMS plug-in before the RSK; however, this is not mandatory.

For more information on installing Cisco Unity plug-ins, go to http://www.ciscounitytools.com/App_RSK.htm.

1. Install Cisco Unity RSK Configuration Wizard.

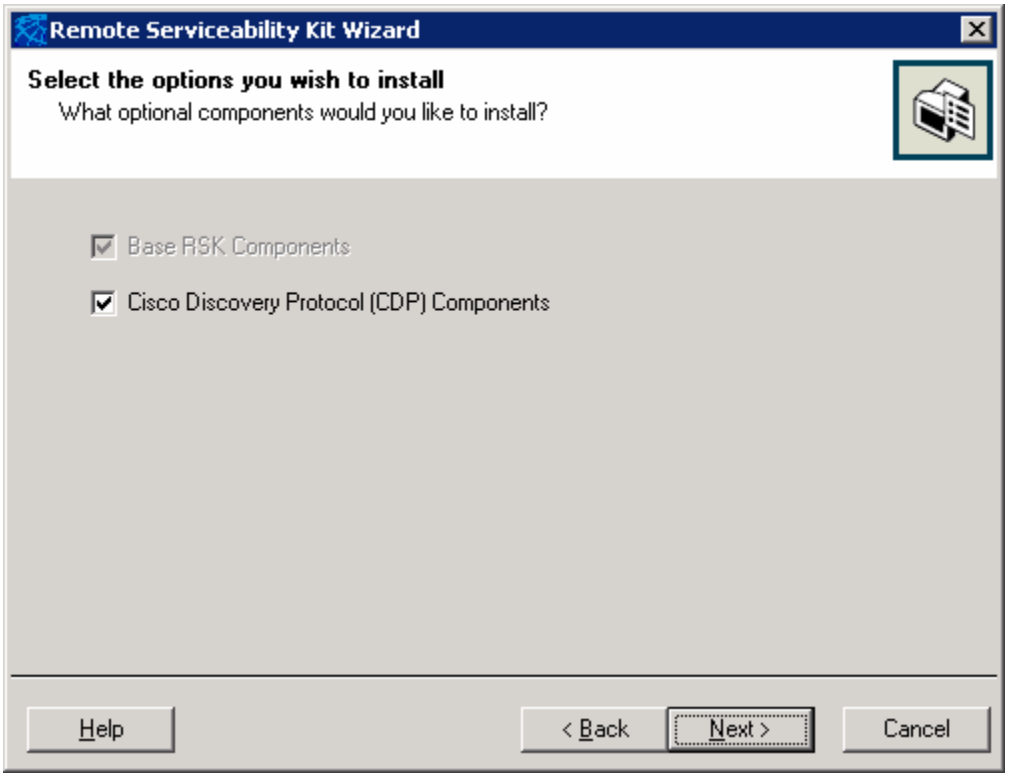


2. Configuration Wizard installation is complete. Now launch the RSK Wizard.

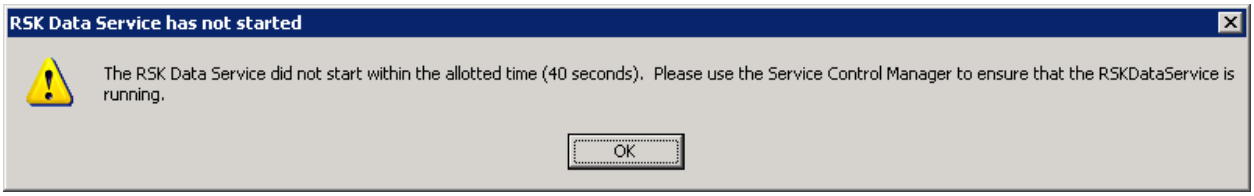


3. Install Unity RSK

4. Install CDP Components.



5. You will see the following error message. Click OK.



6. Once SNMP is started, the Next button is highlighted. Click **Next**.
7. RSK installation complete

8. After the RSK Wizard is completed, open Windows Services.
9. Change the RSKDataService to automatic from manual. Make sure that SNMP service is also automatic.
10. Start the RSKDataService. However, the RSK might not initially start.

    If the RSKDataService process does not start, do the following:

    a. Close all instances of Windows Services application. If you are connected through Terminal Service, make sure there is only one user session and no one is signed in to the console with Windows Services application running (make sure you the only one logged in).

    b. From the command prompt, enter **`net stop snmp`** (end the SNMP process if necessary). Alternatively, you can stop the SNMP service from Windows Services.

    c. Enter **`cd \commserver\utilties\remoteserviceabilitykit\bin`** (typically D: drive).

    d. Enter **`rskdataservice /unregserver`**.

    e. Enter **`rskdataservice /regserver`**.

    f. Enter **`rskdataservice /service`**.

g. Enter **`net start snm`**p.

11. At this point, the SNMP service and the RSKDataService should start.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-577464-00 01/10