NetIQ® AppManager® for Cisco Unity Express

Management Guide

February 2012

Legal Notice

Contents

About this Book and the Library

The NetIQ AppManager product (AppManager) is a comprehensive solution for managing, diagnosing, and analyzing performance, availability, and health for a broad spectrum of operating environments, applications, services, and server hardware.

AppManager provides system administrators with a central, easy-to-use console to view critical server and application resources across the enterprise. With AppManager, administrative staff can monitor computer and application resources, check for potential problems, initiate responsive actions, automate routine tasks, and gather performance data for real-time and historical reporting and analysis.

Intended Audience

This guide provides information for individuals responsible for installing an AppManager module and monitoring specific applications with AppManager.

Other Information in the Library

The library provides the following information resources:

Installation Guide for AppManager

Provides complete information about AppManager pre-installation requirements and step-by-step installation procedures for all AppManager components.

User Guide for AppManager Control Center

Provides complete information about managing groups of computers, including running jobs, responding to events, creating reports, and working with Control Center. A separate guide is available for the AppManager Operator Console.

Administrator Guide for AppManager

Provides information about maintaining an AppManager management site, managing security, using scripts to handle AppManager tasks, and leveraging advanced configuration options.

Upgrade and Migration Guide for AppManager

Provides complete information about how to upgrade from a previous version of AppManager.

Management guides

Provide information about installing and monitoring specific applications with AppManager.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

The AppManager library is available in Adobe Acrobat (PDF) format from the NetIQ Web site: www.netiq.com/support/am/extended/documentation/default.asp?version=AMDocumentation.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measurable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, please contact our Technical Support team.

Worldwide:	www.netiq.com/Support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit http://community.netiq.com.

1 Introducing AppManager for Cisco Unity Express

This chapter introduces AppManager for Cisco Unity Express, provides a brief overview of the module, and describes how you can use AppManager to better monitor vital Unity Express resources.

Cisco Unity Express is a voice mail solution for CallManager Express environments, and can be used only with CallManager and CallManager Express. Unity Express, which integrates voice mail and auto attendant services inside Cisco routers, runs on a network module (blade) or an advanced integration module (AIM). The blade or AIM integrates with many Cisco routers and can be plugged into a device that is acting as CallManager Express or in Survivable Remote Site Telephony (SRST) mode.

1.1 Features and Benefits

AppManager is designed to help you gain easy access to Unity Express data, and to help you analyze and manage that data. The AppManager for Cisco Unity Express solution minimizes the cost of maintaining Unity Express resources, aids in capacity planning, and can prevent downtime.

AppManager for Cisco Unity Express includes Knowledge Scripts for creating jobs that monitor the health, availability, and performance of key resources. These scripts allow you to monitor and manage crucial resource properties at a depth unparalleled by any other solution. You can configure each Knowledge Script to raise an event, collect data for reporting, and perform automated problem management when an event occurs.

With AppManager for Cisco Unity Express, you gain access to a new set of tools you can leverage to gather a wide range of diagnostic and management data, which can help prevent outages and keep things running smoothly.

The following are just a few of the features and benefits of monitoring Cisco Unity Express with AppManager:

- Reduces the time you spend diagnosing and resolving issues
- Monitors Unity Express resources, including the integrated voice mail system
- Monitors both call processing and voice mail usage through business branches
- Provides inventory capabilities by determining the number of Unity Express systems in the population of IOS Telephony Services (ITS) routers
- Provides “cross-launch” capabilities, which allow AppManager to make configuration changes to Unity Express by accessing the Unity Express Administrative Web page
- Automates system management issues that could affect device performance
- Pinpoints problems wherever they originate

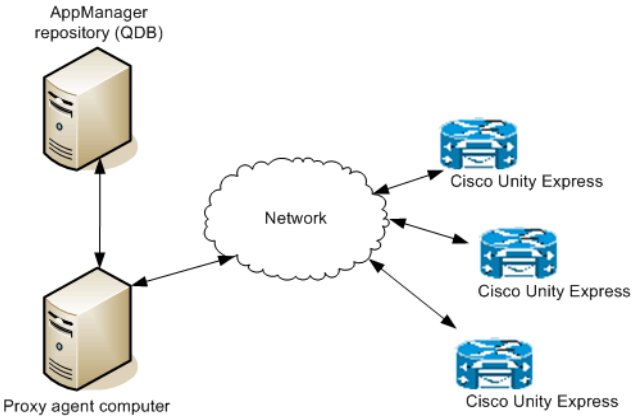
- Supports Network Address Translation (NAT) on remote Unity Express devices and host routers
- Provides Knowledge Scripts for day-to-day and diagnostic monitoring

1.2 Proxy Architecture

With AppManager proxy architecture support for Cisco Unity Express, the AppManager agent does not need to be installed on every device that you want to monitor.

Within the proxy architecture, the module is installed on the proxy agent computer. When you run a Knowledge Script job, the module sends messages to and from Unity Express devices.

The following diagram shows the relationship between Unity Express devices, the AppManager repository, and the proxy agent computer:



1.3 Scalability Considerations

Only one computer should act as a proxy for any given Unity Express device. In other words, two computers cannot be proxy for the same Unity Express device.

One computer should be the proxy for no more than 750 Unity Express devices. Of course, this number is only a recommendation and can vary based on the capabilities of your proxy agent computer.

The limit of 750 devices assumes that other non-Cisco Unity Express jobs may be running on the proxy agent computer, and that you may want to run other Cisco Unity Express jobs in addition to those included in the recommended Knowledge Script Group (KSG).

After you run Discovery_CiscoUE, you should create server groups in the TreeView pane. Each server group should contain no more than 250 Cisco Unity Express devices. With this setup, you can easily run the Recommended KSG on a single server group. If you run a Knowledge Script on too many Cisco Unity Express devices, AppManager raises an event indicating the maximum number of devices for your particular configuration.

NetIQ has verified successful performance using the following specifications on the proxy agent computer:

- Dual Pentium 4 processor
- 2.8 GHz

- 2 GB RAM
- Windows 2003 Server

On a 100-Mbps network, NetIQ has seen an average bandwidth of 0.1% and a maximum of 2.5%.

1.4 Counting AppManager Licenses

AppManager consumes one license for each discovered Cisco Unity Express mailbox.

2 Installing AppManager for Cisco Unity Express

This chapter lists system requirements and describes how to install AppManager for Cisco Unity Express.

This chapter assumes you have AppManager installed. For more information about installing AppManager or about AppManager system requirements, see the *Installation Guide for AppManager*, which is available on the AppManager Documentation page.

2.1 System Requirements

For the latest information about supported software versions and the availability of module updates, visit the AppManager Supported Products page. Unless noted otherwise, this module supports all updates, hotfixes, and service packs for the releases listed below.

AppManager for Cisco Unity Express has the following system requirements:

Software/Hardware	Version
NetIQ AppManager installed on the AppManager repository (QDB) computer, on the proxy agent computer, and on the console computers	At minimum, 7.0 For support of Windows Server 2008, hotfix 71704 is required. For more information, see the AppManager Suite Hotfixes Web page.
Microsoft operating system installed on the proxy agent computer	One of the following: ◆ 32- or 64-bit Windows Server 2003 ◆ 32- or 64-bit Windows Server 2008
Cisco Unity Express	Routers running version 2.2, 2.3, 3.0, 3.1, or 7.0.4
AppManager for Microsoft Windows module installed on repository, proxy agent, and console computers	The most recent version, for support of Windows Server 2008. For more information, see the AppManager Module Upgrades & Trials Web page.
NetIQ AppManager for Network Devices module installed on the repository, proxy agent, and console computers	For monitoring the network devices in a Cisco Unity Express environment

If you encounter problems using this module with a later version of your application, contact NetIQ Technical Support.

2.2 Installing the Module

The setup program automatically identifies and updates all relevant AppManager components on a computer. Therefore, run the setup program only once on any computer. The pre-installation check also runs automatically when you launch the setup program.

You can install the module in one of the following ways:

- Run the module setup program, `AM70-CiscoUE-7.x.xx.0.msi`, which you downloaded from the Web. Save the module setup files on the distribution computer, and then delete the older versions of the module setup files. For more information about the distribution computer, see the *Installation Guide for AppManager.*
- Use Control Center to install the module on the remote computer where an agent is installed. For more information, see Section 2.3, "Deploying the Module with Control Center," on page 14.

To install the module manually:

1. Run the module setup program on all AppManager repository (QDB) computers to install the Knowledge Scripts and reports.
   - Run the setup program on the primary repository computer first. Then run the setup program on all other repository computers.
   - For repositories running in active/active and active/passive clusters, run the setup program on the active node. Then, copy the following Registry key to the non-active node.

     `HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\AppManager\4.0`
2. Install the module on the proxy agent computer. Use one of the following methods:
   - Run the module setup program.
   - Use Control Center to deploy the installation package.

   NOTE: Do not install the module on a Cisco Unity server or any other computer running Cisco software.
3. Run the module setup program on all Operator Console and Control Center computers to install the Help and console extensions.
4. Enable SNMP on your Unity Express devices. For more information, see Section 2.5, "Enabling SNMP," on page 16.
5. Configure read-only SNMP community strings for your Unity Express devices. For more information, see Section 2.6, "Configuring SNMP Community Strings in Security Manager," on page 16.
6. If you have not already discovered Cisco Unity Express resources, run the Discovery_CiscoUE Knowledge Script on all proxy agent computers where you installed the module. For more information, see Section 2.7, "Discovering Cisco Unity Express Resources," on page 17.

After the installation has completed, you can find a record of problems encountered in the `CiscoUE_Install.log` file, located in the `\NetIQ\Temp\NetIQ_Debug\<`*ServerName*`>` folder.

2.3 Deploying the Module with Control Center

You can use Control Center to deploy the module on a remote computer where an agent is installed. This topic briefly describes the steps involved in deploying a module and provides instructions for checking in the module installation package. For more information, see the *Control Center User Guide for AppManager*, which is available on the AppManager Documentation page.

2.3.1 Deployment Overview

This section describes the tasks required to deploy the module on an agent computer.

To deploy the module on an agent computer:

1. Verify the default deployment credentials.
2. Check in an installation package.
3. Configure an email address to receive notification of a deployment.
4. Create a deployment rule or modify an out-of-the-box deployment rule.
5. Approve the deployment task.
6. View the results.

2.3.2 Checking In the Installation Package

You must check in the installation package, `AM70-CiscoUE-7.x.x.0.xml`, before you can deploy the module on an agent computer.

To check in a module installation package:

1. Log on to Control Center and navigate to the Administration pane.
2. In the Deployment folder, select **Packages**.
3. On the Tasks pane, click **Check in Packages**.
4. Navigate to the folder where you saved `AM70-CiscoUE-7.x.x.0.xml` and select the file.

2.4 Silently Installing the Module

To silently (without user intervention) install a module, create an initialization file (`.ini`) for this module that includes the required property names and values to use during the installation.

To create and use an initialization file for a silent installation:

1. Create a new text file and change the filename extension from `.txt` to `.ini`.
2. To specify the community string required to access hardware resources, include the following text in the `.ini` file:

   `MO_CommunityString=`*`string name`*

   where *string name* is the name of the community string, such as `public`.
3. Save and close the `.ini` file.
4. Run the following command from the folder in which you saved the module installer:

   `msiexec.exe /i "AM70-CiscoUE-7.`*`x.x`*`.0.msi" /qn MO_CONFIGOUTINI="`*`full path to the initialization file`*`"`

   where *x.x* is the actual version number of the module installer.

To create a log file that describes the operations of the module installer, add the following flag to the command noted above:

`/L* "AM70-CiscoUE-7.`*`x.x`*`.0.msi.log"`

The log file is created in the folder in which you saved the module installer.

2.5 Enabling SNMP

AppManager for Cisco Unity Express employs SNMP to facilitate communication between the proxy agent computer and Unity Express devices. However, SNMP is not enabled by default on Unity Express devices. Enable SNMP using the Unity Express IOS command line interface.

Enter the following commands at the command prompt:

```
configure terminal
snmp-server community <read-only community string> RO
end
write
```

2.6 Configuring SNMP Community Strings in Security Manager

AppManager uses SNMP queries to remotely access Unity Express devices. However, it cannot communicate with the devices unless it has permission to do so. You can grant that permission by configuring the appropriate community string information into AppManager Security Manager.

For each Unity Express device that you want to monitor, configure the SNMP community string information into Security Manager *before* discovering Unity Express resources.

In some cases, Unity Express can re-use the default community string that you may have already configured for the AppManager for Network Device module. Use the following table to determine which community string information you should enter:

If	And	Then
You have configured the community string for Network Device	The community string is the same for Unity Express	Do *not* re-enter the community string. AppManager can use the community string settings for Network Device.
You have *not* configured the community string for Network Device	The community string is the same for Unity Express	Use the following procedure to enter the community string for Network Device. AppManager can use the community string settings for Network Device.
You have *not* configured the community string for Network Device	The community string is *not* the same for Unity Express	Use the following procedure to enter the community strings for *both* Unity Express *and* Network Device.

In summary, you always need the community string information for AppManager for Network Device. If the community strings are different for the two modules, then you also need the community string information for Unity Express.

Complete the following fields in the Custom tab of Security Manager for the proxy agent computer.

Field	Description
Label	`CiscoUE` or `NetworkDevice`, as appropriate

Field	Description
Sub-label	Indicates whether the community string information will be used for a single Unity Express device or for all Unity Express devices associated with a particular proxy agent computer. ◆ For a single device with a NetworkDevice label, enter <*hostname or device IP address*>. ◆ For a single device with a CiscoUE label, enter <*device IP address*>. ◆ For all devices, enter `default`.
Value 1	Read-only community string, such as `public` or `private`.

2.7 Discovering Cisco Unity Express Resources

Use the Discvoery_CiscoUE Knowledge Script to discover Cisco Unity Express resources and configuration information.

AppManager uses SNMP queries to access remote Unity Express devices. However, it cannot communicate with the devices unless it has permission to do so. You can grant that permission by configuring the appropriate SNMP community string information into AppManager Security Manager.

For each Unity Express device that you want to monitor, enter the community string information into Security Manager before discovering Unity Express resources. For more information, see Section 2.6, "Configuring SNMP Community Strings in Security Manager," on page 16.

By default, this script runs every Sunday at 3 AM and also immediately on the first iteration of the job.

Set the Values tab parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the discovery job fails. The default is 5.
Raise event if discovery succeeds?	Select **Yes** to raise an event when the discovery process is successful. The default is unselected.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery succeeds. The default is 25.
Raise event if discovery fails?	Select **Yes** to raise an event when the discovery process fails to find some or all of your Unity Express resources. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery fails to find some or all of your Unity Express resources. The default is 10.
Discovery Details	

Parameter	How to Set It
Discover individual ... ?	Set any of the Discovery Details parameters to **Yes** to discover the following components: ◆ Interfaces ◆ LAN links ◆ WAN links ◆ Frame relay links ◆ ATM links ◆ FXS ports ◆ FXO ports ◆ ISDN channels
Auto Discovery	
Default gateway router	Enter the IP network address of the gateway router to query during discovery. The router you want to query is the router that hosts the Unity Express device that you want to monitor. **NOTE**: Use this parameter if you are not certain of all the relevant subnets that should be scanned during discovery. If you enter an IP address here, AppManager queries the gateway for its routing tables and then attempts to discover every device in the tables.
Maximum number of hops	Enter the maximum number of hops that you want discovery to make during auto-discovery. The default is one hop. Discovery considers the gateway router itself to be the first hop. Therefore, a *Maximum number of hops* setting of 1 means you will only discover the networks directly connected to the gateway router, but no other routers. To discover more, enter a *Maximum number of hops* setting of at least 2.
Discover Unity Express Devices	
Discovery timeout	Enter the number of minutes that the script should attempt discovery before stopping as an unsuccessful discovery. The maximum is 60 minutes. The default is 10 minutes.
Maximum number of concurrent discoveries	Specify the maximum number of Unity Express devices that can be queried for discovery at one time. No matter what value you enter, discovery is still performed for the entire list of devices that you specify in the following parameters. Setting this parameter to a low value throttles the number of SNMP requests performed at one time, but may increase the overall time it takes to discover a list of devices. The default is 10 concurrent discoveries.
List of IP telephony routers	Use this parameter if you know which IP telephony routers you want to discover, which are those routers that host Unity Express devices. Specify at least one router IP address or hostname, using a comma to separate multiple items. For example: `10.0.1.1,10.0.1.7` You can enter IP addresses or hostnames, but you *must* enter the same IP address or hostname for which you configured SNMP community string information. If you configured a community string for a hostname, then enter the *same* hostname; if you configured an IP address, then enter the *same* IP address.

Parameter	How to Set It
List of IP telephony router ranges	Enter a list of IP address ranges of the routers for which you want to discover resources. Spaces are invalid in the list; only numbers, dashes, periods, and commas are allowed. For example: `10.0.1.1-10.0.1.254,10.0.4.1-10.0.4.254` The routers you specify are those routers that host Unity Express devices. Their IP addresses *must* match the IP addresses for which you configured SNMP community string information. If you configured community strings for hostnames, then do not use this parameter. Use the following parameter or the preceding parameter. **NOTE**: Limit the number of IP addresses in each range to no more than 256. To scan more than 256 IP addresses, break a range into multiple ranges, each with no more than 256 IP addresses.

Full path to file with list of IP telephony routers	Instead of listing each router separately, you can specify the full path to a file on the agent computer that contains a list of IP addresses or hostnames of routers that host Unity Express devices. The list should contain the names or addresses on one or more lines.
	
	If you specify the routers on one line, separate each item with a comma. For example:
	
	`10.0.1.1-10.0.1.254,10.0.4.1-10.0.4.254`
	
	If you specify the routers on multiple lines, ensure that each line contains only one entry. For example:
	
	`routername01`
	`routername02`
	`routername10`
	
	You can enter IP addresses or hostnames, but you *must* enter the same IP address or hostname for which you configured SNMP community string information. If you configured a community string for a hostname, then enter the *same* hostname in the list; if you configured an IP address, then enter the *same* IP address in your list.

Parameter	How to Set It

Comma-separated list of Unity Express and host router NAT-enabled IP address pairs	MSPs (Managed Service Providers) frequently maintain distributed customer networks in which NAT (Network Address Translation) is used to translate the IP address ranges that are monitored from a single NOC (Network Operations Center). The use of NAT prevents AppManager from recognizing the actual IP addresses of the remote Unity Express devices and host routers.
	
	If your AppManager agent is located on a server in the NOC, but the monitored devices are located in the remote customer network, you need to provide AppManager with a list of the IP addresses of the remote monitored devices.
	
	Use this parameter to enable AppManager to recognize the IP addresses of the remote Unity Express devices and host routers.
	
	Type a list of IP address pairs for the remote Unity Express devices and host routers. Use commas to separate the addresses. A pair consists of the externally visible IP address for a Unity Express device and the externally visible IP address of its host router. Use the following format:
	
	`UEexternaladdress1,hostrouterexternaladdress1,UEexteral address2,hostrouterexternaladdress2`
	
	The following example shows how the pairs look when you use IP addresses:
	
	`10.41.1.10,10.41.1.11,10.41.1.12,10.41.1.13`

2.8 Upgrading Knowledge Script Jobs

This release of AppManager for Cisco Unity Express may contain updated Knowledge Scripts. You can push the changes for updated scripts to running Knowledge Script jobs in one of the following ways:

- Use the AMAdmin_UpgradeJobs Knowledge Script.
- Use the Properties Propagation feature.

2.8.1 Running AMAdmin_UpgradeJobs

The AMAdmin_UpgradeJobs Knowledge Script can push changes to running Knowledge Script jobs. Your AppManager repository (QDB) must be at version 7.0 or later. In addition, the repository computer must have hotfix 72040 installed, or the most recent AppManager Repository hotfix. To download the hotfix, see the AppManager Suite Hotfixes Web page.

Upgrading jobs to use the most recent script version allows the jobs to take advantage of the latest script logic while maintaining existing parameter values for the job.

For more information, see the Help for the AMAdmin_UpgradeJobs Knowledge Script.

2.8.2 Propagating Knowledge Script Changes

You can propagate script changes to jobs that are running and to Knowledge Script Groups, including recommended Knowledge Script Groups and renamed Knowledge Scripts.

Before propagating script changes, verify that the script parameters are set to your specifications. Customized script parameters may have reverted to default parameters during the installation of the module. New parameters may need to be set appropriately for your environment or application.

You can choose to propagate only properties (specified in the Schedule and Values tabs), only the script (which is the logic of the Knowledge Script), or both. Unless you know specifically that changes affect only the script logic, you should propagate both properties and the script.

For more information about propagating Knowledge Script changes, see the "Running Monitoring Jobs" chapter of the *Operator Console User Guide for AppManager*.

Propagating Changes to Ad Hoc Jobs

You can propagate the properties and the logic (script) of a Knowledge Script to ad hoc jobs started by that Knowledge Script. Corresponding jobs are stopped and restarted with the Knowledge Script changes.

To propagate changes to ad hoc Knowledge Script jobs:

1. In the Knowledge Script view, select the Knowledge Script for which you want to propagate changes.
2. Click **Properties Propagation** > **Ad Hoc Jobs**.
3. Select the components of the Knowledge Script that you want to propagate to associated ad hoc jobs:

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	Values from the Knowledge Script Schedule and Values tabs, such as schedule, monitoring values, actions, and advanced options.

Propagating Changes to Knowledge Script Groups

You can propagate the properties and logic (script) of a Knowledge Script to corresponding Knowledge Script Group members.

After you propagate script changes to Knowledge Script Group members, you can propagate the updated Knowledge Script Group members to associated running jobs. For more information, see "Propagating Changes to Ad Hoc Jobs" on page 21.

To propagate Knowledge Script changes to Knowledge Script Groups:

1. In the Knowledge Script view, select the Knowledge Script Group for which you want to propagate changes.
2. On the KS menu, select **Properties propagation** > **Ad Hoc Jobs**.
3. ***If you want to exclude a Knowledge Script member from properties propagation,*** deselect that member from the list in the Properties Propagation dialog box.

4 Select the components of the Knowledge Script that you want to propagate to associated Knowledge Script Groups:

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	Values from the Knowledge Script Schedule and Values tabs, including the schedule, actions, and Advanced properties.

5 Click **OK**. Any monitoring jobs started by a Knowledge Script Group member are restarted with the job properties of the Knowledge Script Group member.

2.9 Excluding Log Folders from Virus Scan

You should exclude your log files, specifically those under `c:\Program Files\NetIQ\temp`, from real-time virus scans. Virus scanning that is enabled on log files significantly increases processing time and drastically reduces the number of devices that can be supported by one proxy agent computer.

3 CiscoUE Knowledge Scripts

AppManager for Cisco Unity Express provides the following Knowledge Scripts for monitoring Unity Express resources. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
BackupAndRestoreStatus	Monitors the status of Unity Express Backup and Restore operations.
DeviceUptime	Monitors the number of hours that a Unity Express device has been operational.
GDMStorageUsage	Monitors the storage usage of Unity Express general delivery mailboxes.
OrphanedMailboxes	Monitors the operational status of the Unity Express Watchdog process.
LicenseCompliance	Monitors the number or percentage of in-use voice mail licenses on a Unity Express device.
MessageActivity	Monitors the number of new, read, and deleted messages on a Unity Express device since the last reboot.
OrphanedMailboxes	Monitors for mailboxes on a Unity Express device that are not associated with an owner.
PortStatus	Monitors the registration status of all Unity Express ports for an associated Unified Communications Manager.
SubscriberStorageUsage	Monitors the storage usage of one or more Unity Express Subscriber mailboxes.
SystemUsage	Monitors the total CPU usage for a Unity Express device.
TotalStorageUsage	Monitor+s the total storage usage for a Unity Express device.
VoiceMailLogins	Monitors the number of failed and total voice mail login attempts for a Unity Express device.
VoiceMailSessionsInUse	Monitors concurrent voice mail sessions that are in use on a Unity Express device.
Recommended Knowledge Script Group	Performs essential monitoring of your Cisco Unity Express environment.

3.1 BackupAndRestoreStatus

Use this Knowledge Script to monitor the status of Unity Express Backup and Restore operations. If a new Backup or Restore operation is discovered, then this script raises an event that identifies the operation type, the operation's date/time stamp, and the results of the operation. In addition, this script generates a data stream for successful (1) or failed (0) Backup and Restore operations.

3.1.1 Resource Object

CiscoUE

3.1.2 Default Schedule

By default, this script runs every 24 hours.

3.1.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BackupAndRestoreStatus job fails. The default is 5.
Monitor Backup/Restore Events	
Raise event if Backup/Restore succeeded?	Select **Yes** to raise an event if the Backup or Restore operation was successful. The default is Yes.
Event severity when Backup/ Restore succeeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Backup or Restore operation was successful. The default is 25.
Raise event if Backup/Restore failed?	Select **Yes** to raise an event if the Backup or Restore operation failed. The default is Yes.
Event severity when Backup/ Restore failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Backup or Restore operation failed. The default is 5.
Monitor Backup/Restore Status	
Data Collection	
Collect data for Backup/Restore history?	Select **Yes** to collect data about the history of the Backup or Restore operation for charts and reports. The default is unselected.

3.2 DeviceUptime

Use this Knowledge Script to monitor the number of hours that a Unity Express device has been operational. This script raises an event if the device reboots. In addition, this script generates a data stream for the number of hours a device has been operational.

3.2.1 Resource Object

CiscoUE

3.2.2 Default Schedule

By default, this script runs every five minutes.

3.2.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DeviceUptime job fails. The default is 5.
Monitor Unity Express Reboot Events	
Raise event if device reboots?	Select **Yes** to raise an event if the device reboots. The default is Yes.
Event severity when device reboots	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Unity Express device reboots. The default is 25.
Monitor Unity Express Device Uptime	
Data Collection	
Collect data for uptime?	Select **Yes** to collect data about device uptime for charts and reports. The default is Yes.

3.3 GDMStorageUsage

Use this Knowledge Script to monitor the storage usage of one or more Unity Express general delivery mailboxes. This script raises an event if the storage usage exceeds the threshold. In addition, this script generates data streams for the storage usage percentage of all monitored mailboxes.

3.3.1 Resource Object

CiscoUE General Delivery Mailboxes

3.3.2 Default Schedule

By default, this script runs every hour.

3.3.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	

Parameter	How to Set It
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the GDMStorageUsage job fails. The default is 5.
List of general delivery mailboxes to monitor	Provide a list of the owner names of the mailboxes that you want to monitor, separated by commas. If you want to monitor all mailboxes, leave this parameter blank.
Monitor General Delivery Mailbox Storage Usage	
Event Notification	
Raise event if storage usage exceeds threshold?	Select **Yes** to raise an event if the percentage of storage usage exceeds the threshold. The default is Yes.
Threshold - Maximum storage usage	Specify the maximum percentage of general delivery mailbox storage usage that can be detected before an event is raised. The default is 80%.
Event severity when storage usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of storage usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for storage usage?	Select **Yes** to collect data about storage usage for charts and reports. The default is Yes.

3.4 LicenseCompliance

Use this Knowledge Script to monitor the number or percentage of in-use voice mail licenses. This script raises an event if the number or percentage of in-use licenses exceeds the threshold. In addition, this script generates data streams for the total number of available licenses, the number of in-use licenses, and the percentage of in-use licenses.

3.4.1 Resource Object

CiscoUE

3.4.2 Default Schedule

By default, this script runs every 24 hours.

3.4.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the LicenseCompliance job fails. The default is 5.

Parameter	How to Set It
Monitor Total Voice Mail Licenses Available	
Data Collection	
Collect data for total voice mail licenses available?	Select **Yes** to collect data about available voice mail licenses for charts and reports. The default is unselected.
Monitor Number of Voice Mail Licenses in Use	
Event Notification	
Raise event if number of voice mail licenses in use exceeds threshold?	Select **Yes** to raise an event if the number of in-use voice mail licenses exceeds the threshold. The default is unselected
Threshold - Maximum number of voice mail licenses in use	Specify the maximum number of voice mail licenses that can be in use before an event is raised. The default is 25 licenses.
Event severity when number of voice mail licenses in use exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-use voice mail licenses exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of voice mail licenses in use	Select **Yes** to collect data about in-use voice mail licenses for charts and reports. The default is unselected.
Monitor Percent of Voice Mail Licenses in Use	
Event Notification	
Raise event if percent of voice mail licenses in use exceeds threshold?	Select **Yes** to raise an event if the percentage of in-use voice mail licenses exceeds the threshold. The default is Yes.
Threshold - Maximum percent of voice mail licenses in use	Specify the maximum percentage of voice mail licenses that can be in use before an event is raised. The default is 80%.
Event severity when percent of voice mail licenses in use exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of in-use voice mail licenses exceeds the threshold. The default is 5.
Data Collection	
Collect data for percent of voice mail licenses in use	Select **Yes** to collect data about in-use voice mail licenses for charts and reports. The default is unselected.

3.5 MessageActivity

Use this Knowledge Script to monitor the number of new, read, and deleted messages on a Unity Express device since the last polling interval. This script raises an event if the number of messages exceeds the threshold. In addition, this script generates data streams for new, deleted, and read messages.

3.5.1 Resource Object

CiscoUE Mailbox Folder

3.5.2 Default Schedule

By default, this script runs every 10 minutes.

3.5.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the MessageActivity job fails. The default is 5.
Monitor New Messages	
Event Notification	
Raise event if new messages exceed threshold?	Select **Yes** to raise an event if the number of new messages exceeds the threshold. The default is Yes.
Threshold - Maximum new messages	Specify the maximum number of new messages that can be detected before an event is raised. The default is 100 messages.
Event severity when new messages exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of new messages exceeds the threshold. The default is 15.
Data Collection	
Collect data for new messages?	Select **Yes** to collect data about new messages for charts and reports. The default is unselected.
Monitor Read Messages	
Event Notification	
Raise event if read messages exceed threshold?	Select **Yes** to raise an event if the number of read messages exceeds the threshold. The default is Yes.
Threshold - Maximum read messages	Specify the maximum number of read messages that can be detected before an event is raised. The default is 100 messages.
Event severity when read messages exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of read messages exceeds the threshold. The default is 15.
Data Collection	
Collect data for read messages?	Select **Yes** to collect data about read messages for charts and reports. The default is unselected.
Monitor Deleted Messages	
Event Notification	
Raise event if deleted messages exceed threshold?	Select **Yes** to raise an event if the number of deleted messages exceeds the threshold. The default is Yes.

Parameter	How to Set It
Threshold - Maximum deleted messages	Specify the maximum number of deleted messages that can be detected before an event is raised. The default is 100 messages.
Event severity when deleted messages exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of deleted messages exceeds the threshold. The default is 25.
Data Collection	
Collect data for deleted messages?	Select **Yes** to collect data about deleted messages for charts and reports. The default is unselected.

3.6 OrphanedMailboxes

Use this Knowledge Script to identify mailboxes that are not associated with an owner. This script raises an event if an orphaned mailbox is found. In addition, this script generates data streams for the number of orphaned mailboxes.

3.6.1 Resource Object

CiscoUE Mailbox Folder

3.6.2 Default Schedule

By default, this script runs every 24 hours.

3.6.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the OrphanedMailboxes job fails. The default is 5.
Monitor Orphaned Mailboxes	
Event Notification	
Raise event if orphaned mailboxes are found?	Select **Yes** to raise an event if an orphaned mailbox is found. The default is Yes.
Event severity when orphaned mailboxes are found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an orphaned mailbox is found. The default is 15.
Data Collection	
Collect data for orphaned mailboxes?	Select **Yes** to collect data about orphaned mailboxes for charts and reports. The default is unselected.

3.7 PortStatus

Use this Knowledge Script to monitor the registration status of all Unity Express CTI ports for an associated Unified Communications Manager. This script raises an event if the status of any port changes. In addition, this script generates a data stream for the percentage of registered ports.

3.7.1 Resource Object

CiscoUE

3.7.2 Default Schedule

By default, this script runs every five minutes.

3.7.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the PortStatus job fails. The default is 5.
Monitor Port Status Events	
Raise event if a port is not registered?	Select **Yes** to raise an event if a monitored port is not registered. The default is Yes.
Event severity when a port is not registered	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored port is not registered. The default is 5.
Raise event if an unregistered port becomes registered?	Select **Yes** to raise an event if the status of a monitored port changes from unregistered to registered. The default is Yes.
Event severity when an unregistered port becomes registered	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a monitored port changes from unregistered to registered. The default is 25.
Monitor Percentage of Ports Registered	
Data Collection	
Collect data for percentage of ports registered?	Select **Yes** to collect data about registered ports for charts and reports. The default is unselected.

3.8 SubscriberStorageUsage

Use this Knowledge Script to monitor the storage usage of one or more Unity Express subscriber mailboxes. This script raises an event if the percentage of mailbox storage usage exceeds the threshold. In addition, this script generates data streams for the percentage of individual mailbox storage usage for all monitored mailboxes.

3.8.1 Resource Object

CiscoUE Subscriber Mailboxes

3.8.2 Default Schedule

By default, this script runs every hour.

3.8.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SubscriberStorageUsage job fails. The default is 5.
List of mailboxes to monitor	Enter a list of the owner names of the mailboxes that you want to monitor, separated by commas. To monitor all mailboxes, leave this parameter blank.
Monitor Subscriber Mailbox Storage Usage	
Event Notification	
Raise event if storage usage exceeds threshold?	Select **Yes** to raise an event if the percentage of Subscriber mailbox storage usage exceeds the threshold. The default is Yes.
Threshold - Maximum storage usage	Specify the maximum percentage of Subscriber mailbox storage usage that can be detected before an event is raised. The default is 80%.
Event severity when storage usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of Subscriber mailbox storage usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for storage usage?	Select **Yes** to collect data about Subscriber storage usage for charts and reports. The default is Yes.

3.9 SystemUsage

Use this Knowledge Script to monitor total CPU usage for a Unity Express device. This script raises an event if CPU usage exceeds the threshold. In addition, this script generates a data stream for the percentage of total CPU usage.

3.9.1 Resource Object

CiscoUE

3.9.2 Default Schedule

By default, this script runs every five minutes.

3.9.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SystemUsage job fails. The default is 5.
Monitor Unity Express CPU Usage	
Event Notification	
Raise event if total CPU usage exceeds threshold?	Select **Yes** to raise an event if the total percentage of CPU usage exceeds the threshold. The default is Yes.
Event severity when total CPU usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 10.
Threshold - Maximum total CPU usage	Specify the maximum percentage of CPU usage that can occur before an event is raised. The default is 80%.
Data Collection	
Collect data for total CPU usage?	Select **Yes** to collect data about CPU usage for charts and reports. The default is unselected.

3.10 TotalStorageUsage

Use this Knowledge Script to monitor the total storage usage for a Unity Express device. This script raises an event if the percentage of storage usage exceeds the threshold. In addition, this script generates data streams for the percentage of total storage usage.

3.10.1 Resource Object

CiscoUE Storage Capacity

3.10.2 Default Schedule

By default, this script runs every hour.

3.10.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the TotalStorageUsage job fails. The default is 5.
Monitor Total Storage Usage	
Event Notification	
Raise event if storage usage exceeds threshold?	Select **Yes** to raise an event if the percentage of storage usage exceeds the threshold. The default is Yes.
Threshold - Maximum storage usage	Specify the maximum percentage of storage usage that can occur before an event is raised. The default is 80%.
Event severity when storage usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of storage usage exceeds the threshold. The default is 5.
Data Collection	
Collect data for storage usage?	Select **Yes** to collect data about storage usage for charts and reports. The default is Yes.

3.11 VoiceMailLogins

Use this Knowledge Script to monitor the number of failed and total voice mail login attempts for a Unity Express device. This script raises an event if the number of failed attempts exceeds the threshold. In addition, this script generates data streams for total Web and phone login attempts, and for password and username failures on Web and phone login attempts.

3.11.1 Resource Object

CiscoUE

3.11.2 Default Schedule

By default, this script runs every hour.

3.11.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	

Parameter	How to Set It
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VoiceMailLogins job fails. The default is 5.
Monitor Total Voice Mail Web Login Attempts	
Event Notification	
Raise event if login attempts exceed threshold?	Select **Yes** to raise an event if the number of Web login attempts exceeds the threshold. The default is Yes.
Threshold - Maximum login attempts	Specify the maximum number of Web logins that can be attempted before an event is raised. The default is 50 attempts.
Event severity when login attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of Web login attempts exceeds the threshold. The default is 15.
Data Collection	
Collect data for total voice mail Web login attempts?	Select **Yes** to collect data about Web login attempts for charts and reports. The default is unselected.
Monitor Total Voice Mail Phone Login Attempts	
Event Notification	
Raise event if login attempts exceed threshold?	Select **Yes** to raise an event if the number of phone login attempts exceeds the threshold. The default is Yes.
Threshold - Maximum login attempts	Specify the maximum number of phone logins that can be attempted before an event is raised. The default is 50 attempts.
Event severity when login attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of phone login attempts exceeds the threshold. The default is 15.
Data Collection	
Collect data for total voice mail phone login attempts?	Select **Yes** to collect data about phone login attempts for charts and reports. The default is unselected.
Monitor Password Failures on Voice Mail Web Login Attempts	
Event Notification	
Raise event if failed attempts exceed threshold?	Select **Yes** to raise an event if the number of password failures on Web login attempts exceeds the threshold. The default is Yes.
Threshold - Maximum failed attempts	Specify the maximum number of password failures on Web login attempts that can occur before an event is raised. The default is 3 failures.
Event severity when failed attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of password failures on Web login attempts exceeds the threshold. The default is 5.
Data Collection	
Collect data for password failures on voice mail Web login attempts?	Select **Yes** to collect data about password failures on Web login attempts for charts and reports. The default is unselected.
Monitor Username Failures on Voice Mail Web Login Attempts	

Parameter	How to Set It
Event Notification	
Raise event if failed attempts exceed threshold?	Select **Yes** to raise an event if the number of username failures on Web login attempts exceeds the threshold. The default is Yes.
Threshold - Maximum failed attempts	Specify the maximum number of username failures on Web login attempts that can occur before an event is raised. The default is 3 failures.
Event severity when failed attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of username failures on Web login attempts exceeds the threshold. The default is 5.
Data Collection	
Collect data for username failures on voice mail Web login attempts?	Select **Yes** to collect data about username failures on Web login attempts for charts and reports. The default is unselected.
Monitor Password Failures on Voice Mail Phone Login Attempts	
Event Notification	
Raise event if failed attempts exceed threshold?	Select **Yes** to raise an event if the number of password failures on phone login attempts exceeds the threshold. The default is Yes.
Threshold - Maximum failed attempts	Specify the maximum number of password failures on phone login attempts that can occur before an event is raised. The default is 3 failures.
Event severity when failed attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of password failures on phone login attempts exceeds the threshold. The default is 5.
Data Collection	
Collect data for password failures on voice mail phone login attempts?	Select **Yes** to collect data about password failures on phone login attempts for charts and reports. The default is unselected.
Monitor Username Failures on Voice Mail Phone Login Attempts	
Event Notification	
Raise event if failed attempts exceed threshold?	Select **Yes** to raise an event if the number of username failures on phone login attempts exceeds the threshold. The default is Yes.
Threshold - Maximum failed attempts	Specify the maximum number of username failures on phone login attempts that can occur before an event is raised. The default is 3 failures.
Event severity when failed attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of username failures on phone login attempts exceeds the threshold. The default is 5.
Data Collection	
Collect data for username failures on voice mail phone login attempts?	Select **Yes** to collect data about username failures on phone login attempts for charts and reports. The default is unselected.

3.12 VoiceMailSessionsInUse

Use this Knowledge Script to monitor concurrent voice mail sessions that are in use on a Unity Express device. This script raises an event if the number or percentage of sessions exceeds the threshold. In addition, this script generates data streams for maximum allowed sessions and for the number and percentage of in-use sessions.

3.12.1 Resource Object

CiscoUE Voicemail Ports

3.12.2 Default Schedule

By default, this script runs every five minutes.

3.12.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VoiceMailSessionsInUse job fails. The default is 5.
Monitor Maximum Allowed Voice Mail Sessions	
Data Collection	
Collect data for maximum allowed voice mail sessions?	Select **Yes** to collect data about allowed voice mail sessions for charts and reports. The default is Yes.
Monitor Number of Voice Mail Sessions in Use	
Event Notification	
Raise event if number of voice mail sessions in use exceeds threshold?	Select **Yes** to raise an event if the number of in-use voice mail sessions exceeds the threshold. The default is unselected.
Threshold - Maximum number of voice mail sessions in use	Specify the maximum number of voice mail sessions that can be in use before an event is raised. The default is 6 sessions.
Event severity when number of voice mail sessions in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-use voice mail sessions exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of voice mail sessions in use?	Select **Yes** to collect data about the number of in-use voice mail sessions for charts and reports. The default is Yes.
Monitor Percent of Voice Mail Sessions in Use	
Event Notification	

Parameter	How to Set It
Raise event if percent of voice mail sessions in use exceeds threshold?	Select **Yes** to raise an event if the percentage of in-use voice mail sessions exceeds the threshold. The default is Yes.
Threshold - Maximum percent of voice mail sessions in use	Specify the maximum percentage of voice mail sessions that can be in use before an event is raised. The default is 80%. **NOTE**: For a four-port Unity Express device, assigning a threshold of 80% results in an event being raised when all four ports are in use. When three out of four ports are in use, the percentage drops to 75.
Event severity when percent of voice mail sessions in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of in-use voice mail sessions exceeds the threshold. The default is 5.
Data Collection	
Collect data for percent voice mail sessions in use?	Select **Yes** to collect data about the percentage of in-use voice mail sessions for charts and reports. The default is Yes.

3.13 Recommended Knowledge Script Group

The following Knowledge Scripts are members of the CiscoUE recommended Knowledge Script Group. You can find these scripts individually on the CiscoUE tab and in a group on the RECOMMENDED tab of the Operator Console.

- DeviceUptime
- PortStatus
- SystemUsage
- TotalStorageUsage
- VoiceMailLogins
- VoiceMailSessionsInUse

NOTE: Cisco Unified Communications Manager Express routers do not provide the data the PortStatus script monitors. If you are running the Recommended KSG on a Unified Communications Manager Express router, remove the PortStatus script from the group. For more information, see PortStatus.

All scripts in the KSG have their parameters set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab and run the KSG on a Cisco Unity Express resource.

The KSG enables a “best practices” usage of AppManager for monitoring your Cisco Unity Express environment. You can use this KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView.

A KSG is composed of a subset of a module’s Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the CiscoUE tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the CiscoUE tab are not affected.

In some cases, default script parameter settings are different when the script is deployed as part of a KSG, as opposed to when it is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the CiscoUE KSG and want to restore it to its original form, you can reinstall AppManager for Cisco Unity Express on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\CiscoUE` directory.