NetIQ® AppManager® for Cisco Intelligent Contact Management

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 measureable 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 Intelligent Contact Management

This chapter introduces AppManager for Cisco Intelligent Contact Management, which is now known as Cisco Unified Contact Center Enterprise (UCCE). UCCE provides contact routing and call treatment across several geographically distributed call centers over an IP infrastructure.

1.1 Features and Benefits

AppManager is designed to help you gain easy access to UCCE data, and to help you analyze and manage that data. The AppManager for Cisco Intelligent Contact Management solution (the module) minimizes the cost of maintaining a UCCE system, aids in capacity planning, and can prevent downtime.

The module includes Knowledge Scripts to create jobs that monitor the health, availability, and performance of key services, applications, and the operating system. These scripts allow you to monitor and manage any or all of these crucial UCCE services at a depth unparalleled by any other solution. Each Knowledge Script can be configured to send an alert, collect data for reporting and perform automated problem management when an event occurs.

The following are just a few of the features and benefits of monitoring UCCE with AppManager:

- Reduces the time you spend diagnosing and resolving UCCE issues
- Monitors and manages the data in the entire UCCE system, including the local, historical, and central databases, skill groups, and the Call Router
- Automates system management issues that could affect UCCE performance
- Pinpoints problems wherever they originate
- Monitors for error, warning, and informational alarms
- Provides Knowledge Scripts for day-to-day and diagnostic monitoring, including a Knowledge Script Group composed solely of recommended Knowledge Scripts.

1.2 Counting AppManager Licenses

The module is licensed by the maximum number of agents logged on. For instance, if, at discovery, two agents are logged on, the license count is two. If, at a subsequent discovery, five agents are logged on, the license count is five. If the number of logged-on agents is reduced, the license count remains at five.

2 Installing AppManager for Cisco Intelligent Contact Management

This chapter provides installation instructions and describes system requirements for AppManager for Cisco Intelligent Contact Management.

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.

The module has the following system requirements:

Software/Hardware	Version
NetIQ AppManager installed on the AppManager repository (QDB) computers, and all agent and console computers	At minimum, 7.0
Cisco Unified Contact Center Enterprise installed on the computers you want to monitor	Versions 4.6 through 7.5
Microsoft Internet Explorer installed on the UCCE computers you want to monitor	Version 5.5 or later for support of the ICM_ProcessLog Knowledge Script
Internet Information Services installed on the UCCE computers you want to monitor	Version 5 or later for support of the IIS_ServiceUpTime Knowledge Script

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

Only the following AppManager modules should be installed on a UCCE server:

- Cisco ICM (qCiscoICMa4.dll)
- Dell (qdella4.dll)
- IBM Netfinity (qnfda4.dll)
- NT (qnta4.dll)
- WTS (qwtsa4.dll)
- SQL (qsqla4.dll)

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-CiscoICM-7.x.xx.0.msi`, which you downloaded from the Web. Save the module setup files on the distribution computer, and then delete 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 12.

To install the module:

1. Stop the Cisco Security Agent (CSA) service on each UCCE computer on which you want to install the module.
2. Run the module setup program on all repository computers to install the Knowledge Scripts and reports. For repositories running in a clustered environment, run the setup program on the node that currently owns the cluster resource.
3. Install the module on the UCCE computers you want to monitor (the agent computers). Use one of the following methods:
   - Run the module setup program.
   - Use Control Center to deploy the installation package.
4. Run the module setup program on all Operator Console and Control Center computers to install the Help.
5. Restart the CSA service on each agent computer.
6. If you have not discovered UCCE resources, run the Discovery_CiscoICM Knowledge Script on all agent computers where you installed the module. For more information, see Section 2.6, "Discovering UCCE Resources," on page 14.
7. Upgrade running jobs for any Knowledge Script changes. For more information, see Section 2.7, "Upgrading Knowledge Script Jobs," on page 15.

After the installation has completed, you can find a record of problems encountered in the `CiscoICM_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-CiscoICM-7.x.xx.0.msi`, 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-CiscoICM-7.x.xx.0.msi` and select the file.
5. Click **Open**. The Deployment Package Check in Status dialog box displays the status of the package check in.

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-CiscoICM-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-CiscoICM-7.x.x.0.msi.log"
```

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

2.5 Verifying Your Installed Module

To verify installation on many computers, run the ReportAM_CompVersion Knowledge Script. Ensure you discover a report-enabled agent before running this script. For more information, see the Help for the script.

To verify installation on one or only a few computers, use the Operator Console.

To verify your installed module with the Operator Console:

1. In the TreeView pane, select the computer for which you want to verify your installed module.
2. From the TreeView menu, select **Properties**. On the System tab, the System information pane displays the version numbers for all modules installed on the computer.
3. Verify that the version number from the *AppManager for Cisco Intelligent Contact Management Readme* matches the version number shown in the System information pane.

2.6 Discovering UCCE Resources

Use the Discovery_VirtualCenter Knowledge Script to discover UCCE resources. Run the script on UCCE computers.

This Knowledge Script can discover your Cisco Central Controller database automatically if it is on the Admin Workstation computer. You can also provide information to guide the discovery of the Central Controller database if the database is on a different computer. If you did not install the Central Controller Database on the Admin Workstation computer, create a user you need to

To discover a remote Central Controller database:

1. Create a user on the Central Controller database computer and on the computer you want to use to monitor the Central Controller. The user must have the same name and the same password on both computers.
2. On Central Controller database computer, grant the user read-only permission to the Central Controller database.
3. If you are using Windows authentication, perform the following steps:
   - **3a** On the Central Controller database computer, click Administrative Tools>Services.
   - **3b** Right-click NetIQ AppManager Client Resource Monitor.
   - **3c** In the Log on as field, enter the user you created in step 1
   - **3d** Restart the service.

4 If you are using SQL authentication, perform the following steps:

4a In the AppManager Security Manager utility, highlight the Central Controller database computer.

4b Add an entry on the SQL tab for the user you created in step 1.

5 Run Discovery_CiscoICM on the Central Controller database computer with the parameter Central controller database detection set to Manual and enter computer and database name.

Set the following parameters as necessary:

Description	How To Set It
Raise event if discovery succeeds? (y/n)	This script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery returns some data but also generates warning messages. The default is 15.
SQL User Name (leave blank to use Windows authentication)	If appropriate, provide your SQL user name. Leave this field blank to use Windows Authentication. Ensure the user has permission to access the database in read-only mode. If you want to use a specific SQL Server login account, use Security Manager to update the AppManager repository with the SQL Server login you want to use. For more information, see the *Installation Guide for AppManager*.
Central controller database detection	Select whether you want AppManager to automatically identify the Central Controller database or whether you want to enter the database name manually. AppManager can only detect the Central Controller database automatically if you installed the Central Controller on the Admin Workstation computer. The default is Automatic.
Name of server hosting central controller database	Enter the computer where the Central Controller database. You can enter a host name, IP address, or fully qualified domain name.
Name of central controller database	Enter the name of the Central Controller database.

2.7 Upgrading Knowledge Script Jobs

This release of AppManager for Cisco Intelligent Contact Management 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.

2.7.1 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.

2.7.2 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 16.

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.

3 CiscoICM Knowledge Scripts

Cisco Intelligent Contact Management is now known as Cisco Unified Contact Center Enterprise (UCCE). UCCE provides contact routing and call treatment across several geographically distributed call centers over an IP infrastructure.

AppManager Knowledge Scripts retrieve information from UCCE computers to help you better manage UCCE. You can use the retrieved information to identify when services are down, when events have been logged, and when performance-monitoring data exceeds thresholds.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and pressing F1. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press F1.

Knowledge Script	What It Does
ICM_AgentData	Monitors agent data from the UCCE database.
ICM_Alarms	Monitors the UCCE server for error, warning, and informational alarms.
ICM_EventGetViaFilter	Returns a formatted text version of matching events from the UCCE database, not the Windows event log.
ICM_EventLog	Monitors event log entries from UCCE during the past n hours.
ICM_ProcessLog	Searches a log file for a particular regular expression.
ICM_RouteData	Monitors Route data from the UCCE database.
ICM_RoutingClientData	Monitors Routing Client data from the UCCE database.
ICM_ScheduledTargetDataLocal	Monitors Scheduled Target data from the UCCE local database.
ICM_ScriptData	Monitors Script data from the UCCE database.
ICM_ServiceData	Monitors Service data from the UCCE database.
ICM_ServiceDataLocal	Monitors Service data from the UCCE local database.
ICM_SkillGroupData	Monitors Skill Group data from the UCCE database.
ICM_SkillGroupDataLocal	Monitors Skill Group data from the UCCE local database.
IIS_CpuHigh	Monitors CPU usage for IIS processes.
IIS_HealthCheck	Monitors the queue length for blocked I/O requests and the up-and-down status of IIS services and Web sites.
IIS_KillTopCPUProcs	Monitors the CPU usage of the dllhost and MTX processes.
IIS_MemoryHigh	Monitors memory usage and memory pool usage for IIS application processes.
IIS_RestartServer	Restarts an IIS server.

Knowledge Script	What It Does
IIS_ServiceUpTime	Monitors uptime for Web sites and Web services.
Router_AgentsLoggedOn	Monitors the total number of agents currently logged on to a router.
Router_CallsInProgress	Monitors the total number of calls in progress for a router.
Router_CallsPerSec	Monitors the number of calls per second for a router. I
SQL_Accessibility	Monitors whether the SQL Server database is accessible.
SQL_CPUUtil	Monitors CPU usage by SQL Server processes.
SQL_DataGrowthRate	Monitors data growth and shrink rates for all SQL Server databases.
SQL_DBGrowthRate	Monitors database growth and shrink rates.
SQL_MemUtil	Monitors memory usage by SQL Server processes.
SQL_RestartServer	Restarts a SQL Server computer.
Recommended Knowledge Script Group	Performs essential monitoring of your UCCE environment.

3.1 ICM_AgentData

Use this Knowledge Script to monitor agent data from the UCCE database. A separate event or data stream is generated for each agent. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for each monitored metric.

3.1.1 Resource Object

CISCOICM_CentralDB

3.1.2 Default Schedule

By default, this script runs every 30 minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will query the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

3.1.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database. For instance, if you specify 15, the script will search through the most recent 15 minutes of activity. The default is 60 minutes. **NOTE**: Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.
On subsequent runs, query database for extended time range?	Select **Yes** to search the database beginning with records that have timestamps that fall within a time range based on twice the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:15 through 9:45. In other words, the query searches 30 minutes' worth of records beginning 60 minutes (twice the Schedule) prior to the time the job runs. Disable this option to search the database beginning with records that have timestamps that fall within a time range that is the same as the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:45 through 10:15. In other words, the query searches the most recent 30 minutes' worth of records. **Important** Select the option appropriate for your UCCE environment. In newer versions of UCCE, records are not inserted in the database until 30 minutes after the timestamp. Therefore, a record with a timestamp of 9:00 is not inserted into the database until 9:30. This Knowledge Script queries for records that have timestamps that fall within the time frame of the query. To capture records that undergo a 30-minute delay between timestamp and database insertion, select **Yes**.
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Ensure the user has permission to access the database in read-only mode. Leave this parameter blank in order to use Windows authentication. To use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum agent logged-on time	Specify the maximum amount of time that agents can be logged on before an event is raised. The default is 1680 seconds.
Event severity when logged-on time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which logged-on time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.

Parameter	How To Set It
Collect data for agent logged-on time?	Set to **y** to collect data about the amount of time that agents are logged on. The default is n.
Threshold - Maximum agent available time	Specify the maximum amount of time that agents can be available before an event is raised. The default is 1680 seconds.
Event severity when available time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which available time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for agent available time?	Set to **y** to collect data about the amount of time that agents are available. The default is n.
Threshold - Maximum agent not-ready time	Specify the maximum amount of time that agents can be in a Not Ready state before an event is raised. The default is 120 seconds.
Event severity when not-ready time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which not-ready time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for agent not-ready time	Set to **y** to collect data about the amount of time that agents are in a Not Ready state. The default is n.

3.2 ICM_Alarms

Use this Knowledge Script to monitor the Cisco UCCE server for error, warning, and informational alarms. You can filter alarms by severity and alarm identifier. This script raises an event if an alarm is detected from SNMP traps that start with OID 1.3.6.1.4.1539.1.2. An event's short message contains the alarm identifier in the following format: `component_id:alarm_id`. For example, `4_5_IPCC-RGRA_ICM\netiq\LoggerA:0xA1028105`.

3.2.1 Resource Object

CISCOICM

3.2.2 Default Schedule

By default, this script runs on an asynchronous schedule.

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 severity level, from 1 to 40, to indicate the importance of an event in which the ICM_Alarms job fails for an unexpected reason. The default is 5.

Parameter	How To Set It
Monitor Error Alarms?	Set to **Yes** to monitor the UCCE log for error alarms. The default is Yes.
Include or exclude alarms	Select **Include only** to monitor *only* the error alarm identifiers you specify in the *Alarm identifiers* parameter. Select **Exclude** to exclude the specified error alarm identifiers from monitoring. The default is Exclude.
Alarm identifiers	Type a comma-separated list of the error alarm identifiers you want to include in or exclude from monitoring. The default is an empty list.
Event Notification	
Raise event if error alarms are detected?	Set to **Yes** to raise an event if the UCCE log contains error alarms. The default is Yes.
Event severity when error alarms are detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which an error alarm is found in the UCCE log. The default is 10.
Monitor Warning Alarms?	Set to **Yes** to monitor the UCCE log for warning alarms. The default is unchecked.
Include or exclude alarms	Select **Include only** to monitor *only* the warning alarm identifiers specified in the following parameter. Select **Exclude** to exclude the specified warning alarm identifiers from monitoring. The default is Exclude.
Alarm identifiers	Type a comma-separated list of the warning alarm identifiers you want to include in or exclude from monitoring. The default is an empty list.
Event Notification	
Raise event if warning alarms are detected?	Set to **Yes** to raise an event if the UCCE log contains warning alarms. The default is Yes.
Event severity when warning alarms are detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which a warning alarm is found in the UCCE log. The default is 15.
Monitor Informational Alarms?	Set to **Yes** to monitor the UCCE log for informational alarms. The default is unchecked.
Include or exclude alarms	Select **Include only** to monitor *only* the informational alarm identifiers specified in the following parameter. Select **Exclude** to exclude the specified informational alarm identifiers from monitoring. The default is Exclude.
Alarm identifiers	Type a comma-separated list of the informational alarm identifiers you want to include in or exclude from monitoring. The default is an empty list.
Event Notification	
Raise event if informational alarms are detected?	Set to **Yes** to raise an event if the UCCE log contains informational alarms. The default is Yes.

Parameter	How To Set It
Event severity when informational alarms are detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which an informational alarm is found in the UCCE log. The default is 20.

3.3 ICM_EventGetViaFilter

Use this Knowledge Script to create a formatted text version of matching events. These events are from the UCCE database, not the Windows event log. This script raises separate events for each event found in the database.

3.3.1 Resource Object

CISCOICM_CentralDB

3.3.2 Default Schedule

By default, this script runs every 30 minutes.

3.3.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Set this parameter to determine which events are searched the first time you run the Knowledge Script job. The default is 30 minutes. Subsequent searches begin where the previous one finished. The following entries are valid: ◆ **n** to search entries for the past n minutes (8 for the past 8 minutes, 50 for the past 50 minutes, etc.) ◆ **0** to search no previous entries (search from the current time forward) **NOTE**: Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.
Cisco ICM database username	Enter the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Event severity for error message	Set the severity level, from 1 to 40, to indicate the importance of an event in which an error message is found in the UCCE database. The default is 10.

Parameter	How To Set It
Event severity for warning message	Set the severity level, from 1 to 40, to indicate the importance of an event in which a warning message is found in the UCCE database. The default is 20.
Event severity for informational message	Set the severity level, from 1 to 40, to indicate the importance of an event in which an informational message is found in the UCCE database. The default is 30.

3.4 ICM_EventLog

Use this Knowledge Script to monitor event log entries from the UCCE database during the past *n* hours. This script raises an event if log entries are detected. In addition, this script generates data streams for log entries.

3.4.1 Resource Object

CISCOICM

3.4.2 Default Schedule

By default, this script runs every 10 minutes.

3.4.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event for log entries?	Set to **y** to raise an event when the log contains entries for which you have filtered. The default is y.
Collect data?	Set to **y** to collect data about log entries for charts and graphs. The default is n.
Separate data?	Set to **y** to separate events entries from different log files into different data streams. If set to **n**, all event entries matching your filtering criteria are placed in the same data stream and the data detail message may include event entries from multiple log sources. The default is n. For example, if you are monitoring both the System and Application logs, you may want to set this parameter to **y** so that events in the System log are tracked separately from events in the Application log.
Log source	Specify the event log you want to monitor. You can specify multiple event logs, separated by commas. For example: `System,Application`. The default is Application.
Type: Error	Set to **y** to monitor for error events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is y.

Parameter	How To Set It
Type: Warning	Set to **y** to monitor for warning events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is y.
Type: Information	Set to **y** to monitor for information events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is n.
Type: Success Audit	Set to **y** to monitor for success audit events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is n.
Type: Failure Audit	Set to **y** to monitor for failure audit events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is n.
Instructions for filters: To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log. The search string can contain criteria used to include entries, exclude entries, or both.· ◆ Separate include and exclude criteria with a colon (:). For example, `net:logon`. ◆ Separate multiple include or exclude entries with commas. For example, `finance,sales:corp00,HQ`. ◆ If you specify only include criteria, the colon is not necessary. For example, `SQL`. ◆ If you specify only exclude criteria, start the search string with a colon. For example, `:defragmentation,cleanup`.	
Event source filter	Specify one or more text strings to look for; separate multiple strings with commas. If your valid text string includes a comma, replace the comma with a tilde. For example: `GeoTel ICR,Cisco Systems~Inc.` The Knowledge Script will convert the tilde to a comma at runtime.
Event category filter	Specify one or more text strings to look for; separate multiple strings with commas.
Event ID filter	Specify a single event ID or a range of event IDs; separate multiple entries by commas. For example: `1094,1404-1463`
Event user filter	Specify a single or multiple user names to look for; separate multiple entries by commas. For example: `Pat,Chris,Alex`
Computer filter	Specify a single or multiple computer names to look for; separate multiple entries by commas. For example: `SHASTA,MARS`
Event description filter	Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods; separate multiple entries with commas. For example: `data loss during system failures,corrupt indices,Inter-Site Transport objects failed`

Parameter	How To Set It
Maximum number of entries per event report	Specify the maximum number of Application log events that can be returned in each event report. For example, if this value is set to 30 and 67 Application log events are found, three event reports are raised: two reports containing 30 events and one report containing seven events. The default is 30. The Message column on the Events tab in the Operator Console displays the number of events in each event report, the type of log the events are from, and the event report batch number. The batch number is the sequential number of the event report. Batch numbers start at 1 for each Knowledge Script iteration.
Event severity for log entries	Set the event severity level, from 1 to 40, to indicate the importance of an event. You may want to adjust the severity depending on the types of events for which you are checking. The default is 15.

3.5 ICM_ProcessLog

The UCCE Event Management System (EMS) logs events from processes throughout the system and stores the event data in the central database.

The EMS also saves events from individual processes in per-process log files on the local computer. These files document events for a specific process running on a specific computer. Use this Knowledge Script to search a log file for a particular regular expression.

3.5.1 Prerequisite

The UCCE computer on which you run this script must be running Internet Explorer 5.5 or later.

3.5.2 Resource Object

CiscoICM_Process

3.5.3 Default Schedule

By default, this script runs every 30 minutes.

3.5.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event for log entries?	Set to **y** to raise an event if the log contains entries for which you have filtered. The default is y.
Collect data for log entries?	Set to **y** to collect data about log entries for reports and graphs. The default is n.

Parameter	How To Set It
On first run, minutes to go back	Set this parameter to determine which events are searched the first time you run the Knowledge Script job. The default is 30 minutes. Subsequent searches begin where the previous one finished. The following entries are valid: ◆ **n** to search entries for the past n minutes (8 for the past 8 minutes, 50 for the past 50 minutes, etc.) ◆ **0** to search no previous entries (search from the current time forward) **NOTE**: Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.
Filter (regular expression)	Enter the expression by which you want to filter the process log. The default is error|warning|failed|unexpected.
Event severity when log entries present	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the log contains entries for which you have filtered. The default is 10.
Preceding lines to include	Enter the number of lines to include before the matching entry in the event text. The default is 2.
Following lines to include	Enter the number of lines to include after the matching entry in the event text. The default is 2.

3.6 ICM_RouteData

Use this Knowledge Script to monitor data from the Route_Half_Hour table in the UCCE database. This script raises an event if a threshold is exceeded. In addition, this script generates separate data streams for each agent.

3.6.1 Resource Object

CISCOICM_CentralDB

3.6.2 Default Schedule

By default, this script runs every 30 minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will query the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

3.6.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database.For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 60. **NOTE**: Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.
On subsequent runs, query database for extended time range?	Select **Yes** to search the database beginning with records that have timestamps that fall within a time range based on twice the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:15 through 9:45. In other words, the query searches 30 minutes' worth of records beginning 60 minutes (twice the Schedule) prior to the time the job runs. Disable this option to search the database beginning with records that have timestamps that fall within a time range that is the same as the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:45 through 10:15. In other words, the query searches the most recent 30 minutes' worth of records. **Important** Select the option appropriate for your UCCE environment. In newer versions of UCCE, records are not inserted in the database until 30 minutes after the timestamp. Therefore, a record with a timestamp of 9:00 is not inserted into the database until 9:30. This Knowledge Script queries for records that have timestamps that fall within the time frame of the query. To capture records that undergo a 30-minute delay between timestamp and database insertion, select **Yes**.
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the `sa` account or other user login accounts that have been set up in the managed client's SQL Server. Ensure the user has permission to access the database in read-only mode. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum handled calls	Specify the maximum amount of calls that can be handled before an event is raised. The default is 200 calls.
Event severity when handled calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of handles calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.

Parameter	How To Set It
Collect data for handled calls?	Set to **y** to collect data about handled calls for reports and graphs. The default is n.
Threshold - Service Level	Specify your UCCE Service Level threshold, which is the percentage of calls that are answered within the number of seconds you set as a goal for connecting a call with an agent. If the Service Level threshold is exceeded, an event is raised. The default is 20%.
Event severity when Service Level threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Service Level threshold is exceeded. Set to **0** if you want to ignore the event. The default is 20.
Collect data for Service Level?	Set to **y** to collect data about Service Level thresholds for reports and graphs. The default is n.
Threshold - Maximum Service Level calls	Specify the maximum number of calls that can experience a Service Level event before an event is raised. The default is 100 calls. A Service Level event occurs when one of three things happens to a call: ◆ It is answered within the Service Level threshold. ◆ It is abandoned within the Service Level threshold. ◆ It reaches the Service Level threshold without being answered or abandoned.
Event severity when Service Level calls exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of Service Level calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for Service Level calls?	Set to **y** to collect data about Service Level calls for reports and graphs. The default is n.
Threshold - Maximum call-delay time	Specify the maximum number of seconds that a call can wait to be answered before an event is raised. The default is 45 seconds.
Event severity when call delay exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which call delay time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for call delay time?	Set to **y** to collect data about call delay time for reports and graphs. The default is n.
Threshold - Maximum hold time	Specify the maximum number of seconds that a call can wait on hold before an event is raised. The default is 200 seconds.
Event severity when hold time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which hold time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for hold time?	Set to **y** to collect data about hold time for reports and graphs. The default is n.

3.7 ICM_RoutingClientData

Use this Knowledge Script to monitor data from the Routing_Client_Five_Minute table in the UCCE database. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for each routing client.

3.7.1 Resource Object

CISCOICM_CentralDB

3.7.2 Default Schedule

By default, this script runs every five minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will query the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

3.7.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 10 minutes. **NOTE**: Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.
On subsequent runs, query database for extended time range?	Select **Yes** to search the database beginning with records that have timestamps that fall within a time range based on twice the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:15 through 9:45. In other words, the query searches 30 minutes' worth of records beginning 60 minutes (twice the Schedule) prior to the time the job runs. Disable this option to search the database beginning with records that have timestamps that fall within a time range that is the same as the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:45 through 10:15. In other words, the query searches the most recent 30 minutes' worth of records. **Important** Select the option appropriate for your UCCE environment. In newer versions of UCCE, records are not inserted in the database until 30 minutes after the timestamp. Therefore, a record with a timestamp of 9:00 is not inserted into the database until 9:30. This Knowledge Script queries for records that have timestamps that fall within the time frame of the query. To capture records that undergo a 30-minute delay between timestamp and database insertion, select **Yes**.

Parameter	How To Set It
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Ensure the user has permission to access the database in read-only mode. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum errors	Specify the maximum number of errors that can occur before an event is raised. The default is 30 errors.
Event severity when errors exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of errors exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for errors?	Set to **y** to collect data about errors for reports and graphs. The default is n.
Threshold - Maximum timed-out calls	Specify the maximum number of calls that can timeout before an event is raised. The default is five calls.
Event severity when timed-out calls exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of timed-out calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for timed-out calls?	Set to **y** to collect data about timed-out calls for reports and graphs. The default is n.
Threshold - Maximum delay	Specify the maximum amount of delay that can occur before an event is raised. The default is 100 milliseconds.
Event severity when delay exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which delay exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for maximum delay?	Set to **y** to collect data about maximum delay for reports and graphs. The default is n.
Threshold - Maximum discarded calls	Specify the maximum number of calls that can be discarded before an event is raised. The default is 5 calls.
Event severity when discarded calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of discarded calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for discarded calls	Set to **y** to collect data about discarded calls for reports and graphs. The default is n.

3.8 ICM_ScheduledTargetDataLocal

Use this Knowledge Script to monitor data from the Scheduled_Target_Real_Time table in the UCCE local database. This script raises an event if a threshold is exceeded. In addition, this script generates a separate data stream for each scheduled target. All data values reflect the current real-time value.

3.8.1 Resource Object

CISCOICM_LocalDB

3.8.2 Default Schedule

By default, this script runs every five minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will query the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

3.8.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 5 minutes. **NOTE**: Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Ensure the user has permission to access the database in read-only mode. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum calls in progress	Specify the maximum number of calls that can be in progress before an event is raised. The default is 100 calls.
Event severity when in-progress calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-progress calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Threshold - Minimum calls in progress	Enter the minimum number of calls that can be in progress before an event is raised. The default is 1 call.
Event severity when in-progress calls fall below the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-progress calls falls below the threshold. Set to **0** if you want to ignore the event. The default is 20.

Parameter	How To Set It
Collect data for calls in progress?	Set to **y** to collect data about in-progress calls for reports and graphs. The default is n.
Threshold - Maximum queued router calls	Specify the maximum number of router calls that can be in queue before an event is raised. The default is 20 calls.
Event severity when queued router calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of queued router calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 28.
Collect data for queued router calls?	Set to **y** to collect data about queued router calls for reports and graphs. The default is n.

3.9 ICM_ScriptData

Use this Knowledge Script to monitor data from the Script_Five_Minute table in the UCCE database. This script raises an event if a threshold is exceeded. In addition, this script generates a separate data stream for each script.

3.9.1 Resource Object

CISCOICM_CentralDB

3.9.2 Default Schedule

By default, this script runs every five minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will query the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

3.9.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 10 minutes. **NOTE**: Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.

Parameter	How To Set It
On subsequent runs, query database for extended time range?	Select **Yes** to search the database beginning with records that have timestamps that fall within a time range based on twice the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:15 through 9:45. In other words, the query searches 30 minutes' worth of records beginning 60 minutes (twice the Schedule) prior to the time the job runs. Disable this option to search the database beginning with records that have timestamps that fall within a time range that is the same as the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:45 through 10:15. In other words, the query searches the most recent 30 minutes' worth of records. **Important** Select the option appropriate for your UCCE environment. In newer versions of UCCE, records are not inserted in the database until 30 minutes after the timestamp. Therefore, a record with a timestamp of 9:00 is not inserted into the database until 9:30. This Knowledge Script queries for records that have timestamps that fall within the time frame of the query. To capture records that undergo a 30-minute delay between timestamp and database insertion, select **Yes**.
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Ensure the user has permission to access the database in read-only mode. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum incoming calls	Specify the maximum number of calls that can be incoming before an event is raised. The default is 100 calls.
Event severity when incoming calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of incoming calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for incoming calls?	Set to **y** to collect data about incoming calls for reports and graphs. The default is n.
Threshold - Maximum routed calls	Specify the maximum number of calls that can be routed before an event is raised. The default is 100 calls.
Event severity when routed calls exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event. Set to **0** if you want to ignore the event. The default is 20.
Collect data for routed calls?	Set to **y** to collect data about routed calls for reports and graphs. The default is n.

3.10 ICM_ServiceData

Use this Knowledge Script to monitor data from the Service_Half_Hour table in the UCCE database. This script raises an event if a threshold is exceeded. In addition, this script generates a separate data stream for each service.

3.10.1 Resource Object

CISCOICM_CentralDB

3.10.2 Default Schedule

By default, this script runs every 30 minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will either the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

3.10.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 60 minutes. **NOTE**: Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.

Parameter	How To Set It
On subsequent runs, query database for extended time range?	Select **Yes** to search the database beginning with records that have timestamps that fall within a time range based on twice the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:15 through 9:45. In other words, the query searches 30 minutes' worth of records beginning 60 minutes (twice the Schedule) prior to the time the job runs. Disable this option to search the database beginning with records that have timestamps that fall within a time range that is the same as the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:45 through 10:15. In other words, the query searches the most recent 30 minutes' worth of records. **Important** Select the option appropriate for your UCCE environment. In newer versions of UCCE, records are not inserted in the database until 30 minutes after the timestamp. Therefore, a record with a timestamp of 9:00 is not inserted into the database until 9:30. This Knowledge Script queries for records that have timestamps that fall within the time frame of the query. To capture records that undergo a 30-minute delay between timestamp and database insertion, select **Yes**.
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Ensure the user has permission to access the database in read-only mode. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum outgoing calls	Specify the maximum number of calls that can be outgoing before an event is raised. The default is 25 calls.
Event severity when outgoing calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of outgoing calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for outgoing calls?	Set to **y** to collect data about outgoing calls for reports and graphs. The default is n.
Threshold - Maximum incoming calls	Specify the maximum number of calls that can be incoming before an event is raised. The default is 100 calls.
Event severity when incoming calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of incoming calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for incoming calls?	Set to **y** to collect data about incoming calls for reports and graphs. The default is n.
Threshold - Maximum handled calls	Specify the maximum number of calls that can be handled before an event is raised. The default is 100 calls.

Parameter	How To Set It
Event severity when handled calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of handled calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for handled calls?	Set to **y** to collect data about handled calls for reports and graphs. The default is n.
Threshold - Maximum abandoned calls	Specify the maximum number of calls that can be abandoned before an event is raised. The default is 5 calls.
Event severity when abandoned calls exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of abandoned calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for abandoned calls?	Set to **y** to collect data about abandoned calls for reports and graphs. The default is n.
Threshold - Maximum terminated calls	Specify the maximum number of calls that can be terminated before an event is raised. The default is 5 calls.
Event severity when terminated calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of terminated calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for terminated calls?	Set to **y** to collect data about terminated calls for reports and graphs. The default is n.
Threshold - Maximum average delay	Specify the maximum amount of average delay that can occur before an event is raised. The default is 15 milliseconds.
Event severity when average delay exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of average delay exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for average delay?	Set to **y** to collect data about average delay for reports and graphs. The default is n.
Threshold - Maximum average handling time	Specify the maximum average handling time that can occur before an event is raised. The default is 100 seconds.
Event severity when average handling time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average handling time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for average handling time?	Set to **y** to collect data about average handling time for reports and graphs. The default is n.
Threshold - Maximum call delay time	Specify the longest call delay time that can occur before an event is raised. The default is 30 seconds.
Event severity when call delay time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which call delay time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for call delay time?	Set to **y** to collect data about call delay time for reports and graphs. The default is n.
Threshold - Maximum hold time	Specify the maximum amount of hold time that can occur before an event is raised. The default is 15 seconds.

Parameter	How To Set It
Event severity when hold time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of hold time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for hold time?	Set to **y** to collect data about hold time for reports and graphs. The default is n.

3.11 ICM_ServiceDataLocal

Use this Knowledge Script to monitor data from the Service_Real_Time table in the UCCE local database. This script raises an event if a threshold is exceeded. In addition, this script generates a separate data stream for each service. All data values reflect the current real-time value.

3.11.1 Resource Object

CISCOICM_LocalDB

3.11.2 Default Schedule

By default, this script runs every five minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will query the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

3.11.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 5 minutes. **NOTE**: Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.

Parameter	How To Set It
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Ensure the user has permission to access the database in read-only mode. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum outgoing calls	Specify the maximum number of calls that can be outgoing before an event is raised. The default is 25 calls.
Event severity when outgoing calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of outgoing calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for outgoing calls?	Set to **y** to collect data about outgoing calls for reports and graphs. The default is n.
Threshold - Maximum incoming calls	Specify the maximum number of calls that can be incoming before an event is raised. The default is 100 calls.
Event severity when incoming calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of incoming calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for incoming calls?	Set to **y** to collect data about incoming calls for reports and graphs. The default is n.
Threshold - Maximum handled calls	Specify the maximum number of calls that can be handled before an event is raised. The default is 100 calls.
Event severity when handled calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of handled calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for handled calls?	Set to **y** to collect data about handled calls for reports and graphs. The default is n.
Threshold - Maximum abandoned calls	Specify the maximum number of calls that can be abandoned before an event is raised. The default is 5 calls.
Event severity when abandoned calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of abandoned calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for abandoned calls?	Set to **y** to collect data about abandoned calls for reports and graphs. The default is n.
Threshold - Maximum terminated calls	Specify the maximum number of calls that can be terminated before an event is raised. The default is 5 calls.
Event severity when terminated calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of terminated calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for terminated calls?	Set to **y** to collect data about terminated calls for reports and graphs. The default is n.

Parameter	How To Set It
Threshold - Maximum average delay	Specify the highest amount of average delay that can occur before an event is raised. The default is 15 milliseconds.
Event severity when average delay exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average delay exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for average delay?	Set to **y** to collect data about average delay for reports and graphs. The default is n.
Threshold - Maximum average handling time	Specify the highest amount of average handling time that can occur before an event is raised. The default is 100 seconds.
Event severity when average handling time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average handling time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for average handling time?	Set to **y** to collect data about handling time for reports and graphs. The default is n.
Threshold - Maximum call delay time	Specify the highest amount of call delay time that can occur before an event is raised. The default is 30 seconds.
Event severity when call delay time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which call delay time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for call delay time?	Set to **y** to collect data about call delay time for reports and graphs. The default is n.
Threshold - Maximum hold time	Specify the highest amount of hold time that can occur before an event is raised. The default is 15 minutes.
Event severity when hold time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which hold time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for hold time?	Set to **y** to collect data about hold time for reports and graphs. The default is n.

3.12 ICM_SkillGroupData

Use this Knowledge Script to monitor data from the Skill_Group_Five_Minute table in the UCCE database. This script raises an event if a threshold is exceeded. Configure thresholds for five-minute intervals regardless of how often the script runs. This script generates a separate data stream for each skill group.

3.12.1 Resource Object

CISCOICM_CentralDB

3.12.2 Default Schedule

By default, this script runs every five minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will query the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

3.12.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 10 minutes. **NOTE**: Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.
On subsequent runs, query database for extended time range?	Select **Yes** to search the database beginning with records that have timestamps that fall within a time range based on twice the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:15 through 9:45. In other words, the query searches 30 minutes' worth of records beginning 60 minutes (twice the Schedule) prior to the time the job runs. Disable this option to search the database beginning with records that have timestamps that fall within a time range that is the same as the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:45 through 10:15. In other words, the query searches the most recent 30 minutes' worth of records. **Important** Select the option appropriate for your UCCE environment. In newer versions of UCCE, records are not inserted in the database until 30 minutes after the timestamp. Therefore, a record with a timestamp of 9:00 is not inserted into the database until 9:30. This Knowledge Script queries for records that have timestamps that fall within the time frame of the query. To capture records that undergo a 30-minute delay between timestamp and database insertion, select **Yes**.

Parameter	How To Set It
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Ensure the user has permission to access the database in read-only mode. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum agents logged on	Specify the maximum number of agents that can be logged on before an event is raised. The default is 100 agents.
Event severity when logged-on agents exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of logged-on agents exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Threshold - Minimum agents logged on	Specify the minimum number of agents that can be logged on before an event is raised. The default is 1 agent.
Event severity when logged-on agents falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of logged-on agents falls below the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for logged-on agents?	Set to **y** to collect data about logged-on agents for reports and graphs. The default is n.
Threshold - Maximum time in Available state	Specify the maximum amount of time that agents can be in the Available state before an event is raised. The default is 20 seconds.
Event severity when time in Available state exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which time in the Available state exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for time in Available state?	Set to **y** to collect data about Available state time for reports and graphs. The default is n.
Threshold - Maximum time in Not Ready state	Specify the maximum amount of time that agents can be in the Not Ready state before an event is raised. The default is 20.
Event severity when time in Not Ready state exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which time in the Not Ready state exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for time in Not Ready state?	Set to **y** to collect data about agents in Not Ready state for reports and graphs. The default is n.
Threshold - Maximum time in Talking state	Specify the maximum amount of time that agents can be in the Talking state before an event is raised. The default is 20 seconds.
Event severity when time in Talking state exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which time in the Talking state exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for time in Talking state?	Set to **y** to collect data about agents in Talking state for reports and graphs. The default is n.
Threshold - Maximum handled calls	Specify the maximum number of calls that can be handled before an event is raised. The default is 100 calls.

Parameter	How To Set It
Event severity when handled calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of handled calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for handled calls?	Set to **y** to collect data about handled calls or reports and graphs. The default is n.
Threshold - Maximum average handling time	Specify the maximum amount of average handling time that can occur before an event is raised. The default is 30 seconds.
Event severity when average handling time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average handling time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for average handling time?	Set to **y** to collect data about average handling time for reports and graphs. The default is n.

3.13 ICM_SkillGroupDataLocal

Run this Knowledge Script to monitor data from the Skill_Group_Real_Time table in the UCCE local database. This script raises an event if a threshold is exceeded. In addition, this script generates a separate data stream for each skill group. All data values reflect the current real-time value.

3.13.1 Resource Object

CISCOICM_LocalDB

3.13.2 Default Schedule

By default, this script runs every five minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will either the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

3.13.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 5 minutes. **NOTE**: Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Ensure the user has sufficient rights to access the database when the database is in read only mode. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum agents logged on	Specify the maximum number of agents that can be logged on before an event is raised. The default is 100 agents.
Event severity when logged-on agents exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of logged-on agents exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for logged-on agents?	Set to **y** to collect data about logged-on agents for reports and graphs. The default is n.
Threshold - Maximum time in Available state	Specify the maximum amount of time that agents can be in Available state before an event is raised. The default is 20 seconds.
Event severity when time in Available state exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which time in Available state exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for time in Available state?	Set to **y** to collect data about agents in Available state for reports and graphs. The default is n.
Threshold - Maximum time in Not Ready state	Specify the maximum amount of time that agents can be in the Not Ready state before an event is raised. The default is 20 seconds.
Event severity when time in Not Ready state exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which time in Not Ready state exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for time in Not Ready state?	Set to **y** to collect data about agents in Not Ready state for reports and graphs. The default is n.
Threshold - Maximum time in Talking state	Specify the maximum amount of time that agents can be in Talking state before an event is raised. The default is 20.

Parameter	How To Set It
Event severity when time in Talking state exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which time in Talking state exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for time in Talking state?	Set to **y** to collect data about agents in Talking state for reports and graphs. The default is n.
Threshold - Maximum handled calls	Specify the maximum number of calls that can be handled before an event is raised. The default is 100 calls.
Event severity when handled calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of handled calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for handled calls?	Set to **y** to collect data about handled calls for reports and graphs. The default is n.
Threshold - Maximum average handling time	Specify the maximum amount of average handling time that can occur before an event is raised. The default is 30 seconds.
Event severity when average handling time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average handling time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for average handling time?	Set to **y** to collect data about average handling time for reports and graphs. The default is n.
Threshold - Maximum hold time	Specify the maximum amount of hold time that can occur before an event is raised. The default is 15 seconds.
Event severity when hold time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which hold time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for hold time?	Set to **y** to collect data about hold time for reports and graphs. The default is n.

3.14 IIS_CpuHigh

Use this Knowledge Script to monitor CPU usage for IIS application processes. This script raises an event if the threshold is exceeded. In addition, this script generates data streams for CPU usage (%).

3.14.1 Resource Object

CISCOICM_IIST_Server

3.14.2 Default Schedule

By default, this script runs every five minutes.

3.14.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if CPU usage exceeds the threshold?	Set to **y** to raise an event if CPU usage exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about CPU usage for reports and graphs. The default is n.
Process names	Enter the name of the application processes to monitor. Separate multiple entries with commas. For example: `inetinfo,dllhost`. The default is inetinfo. **NOTE**: Do not append .exe to the process names.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU resources the selected process can use before an event is raised. The default is 60%.
Event severity when CPU usage exceeds the 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 8.

3.15 IIS_HealthCheck

Use this Knowledge Script to check IIS servers, Web site status, and the queue length for blocked I/O requests. This script raises an event if any server or Web site is not running. In addition, you can choose to automatically restart the IIS server or Web site. This script also raises an event if the blocked I/O queue length is longer than the specified threshold.

This script monitors only Web sites (servers), not FTP sites, NNTP sites, or SMTP sites.

3.15.1 Resource Objects

CISCOICM_IIST_Server

CISCOICM_IIST_FTPSRV

CISCOICM_IIST_W3SRV

CISCOICM_IIST_WebInst

3.15.2 Default Schedule

By default, this script runs every five minutes.

3.15.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Auto-start monitored server(s)?	Set to **y** to automatically restart down servers. The default is y.

Parameter	How To Set It
Event severity when auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server was down and AppManager successfully restarted it. The default is 25.
Event severity when auto-start is set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager has not been set to restart the service. The default is 18.
Event severity for blocked I/O requests	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of blocked I/O requests exceeds the threshold. The default is 5.
Threshold - Maximum blocked I/O requests	Specify the maximum queue length for blocked I/O requests. The default is 0 requests.
Monitor IIS server?	Set to **y** to monitor the IIS server. The default is y.
Monitor FTP server?	Set to **y** to monitor the FTP server. The default is n.

3.16 IIS_KillTopCPUProcs

Use this Knowledge Script to monitor the CPU usage for the IIS `dllhost` and `mtx` processes. This script raises an event if one or both processes exceed the CPU usage threshold you set. You can set this script to automatically stop a process that exceeds the CPU usage threshold.

3.16.1 Resource Object

CISCOICM_IIST_Server

3.16.2 Default Schedule

By default, this script runs every three minutes.

3.16.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if kill is successful or unsuccessful?	Set to **y** to raise an event if the stop is successful or unsuccessful. The default is y.
Kill CPU intensive processes?	Set to **y** to automatically stop any process whose CPU usage exceeds the threshold. The default is n.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU usage allowed by the `dllhost` and `mtx` processes before an event is raised. The default is 90%.

Parameter	How To Set It
Event severity when CPU usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 10.
Event severity when kill fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop the process. The default is 10.
Event severity when kill succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stopped the service. The default is 20.

3.17 IIS_MemoryHigh

Use this Knowledge Script to detect whether an IIS application process has exceeded the memory usage threshold you set. This script raises an event if an application process exceeds the memory usage threshold you set. In addition, this script generates a data stream for memory usage (%).

3.17.1 Resource Object

CISCOICM_IIST_Server

3.17.2 Default Schedule

By default, this script runs every five minutes.

3.17.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to y, this script returns the named process's memory usage. The default is n.
Process names	Specify the name of the application process to monitor. Use a comma to separate multiple entries — do not use spaces. For example: `inetinfo,dllhost`. The default is inetinfo. **NOTE**: Do not append .exe to the process names.
Threshold - Maximum memory usage	Specify the maximum amount of memory the selected process can use before an event is raised. The default is 10000000 bytes.
Threshold - Maximum memory pool usage	Specify the maximum amount of memory pool the selected process can use before an event is raised. The default is 5000000 bytes.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.

3.18 IIS_RestartServer

Use this Knowledge Script to restart an IIS server. This script raises an event if the server either successfully restarts or fails to restart.

3.18.1 Resource Object

CISCOICM_IIST_Server

3.18.2 Default Schedule

By default, this script runs once.

3.18.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Restart server?	Set to **y** to automatically restart a down server. The default is y.
Wait N seconds before restarting	Specify the number of seconds to wait after the server is stopped before attempting to automatically restart the server. The default is 5 seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the stop attempt fails. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the restart attempt fails. The default is 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the service is unavailable. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the stop attempt succeeds. The default is 25.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the restart attempt succeeds. The default is 25.

3.19 IIS_ServiceUpTime

Use this Knowledge Script to monitor the uptime for Web sites and services. This script raises an event if the amount of time the sites and services are running is less than the threshold you set. In addition, this script generates data streams for uptime.

3.19.1 Prerequisite

The computers on which you run this script must be running IIS version 5 or later.

3.19.2 Resource Objects

CISCOICM_IIST_WebInst

CISCOICM_IIST_FTPInst

3.19.3 Default Schedule

By default, this script runs every hour.

3.19.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if uptime falls below threshold?	Set to **y** to raise an event if Web site or service uptime falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about uptime for reports and graphs. The default is n.
Threshold - Minimum uptime	Specify the minimum amount of time that discovered Web sites and services and FTP sites and services must be up to prevent an event from being raised. The default is 10000 seconds.
Event severity when uptime falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which uptime falls below the threshold. The default is 5.

3.20 Router_AgentsLoggedOn

Use this Knowledge Script to monitor the total number of agents logged on to a Call Router. This script raises an event if the number of agents exceeds the threshold. In addition, this script generates data streams for the number of logged-on agents.

3.20.1 Resource Object

CISCOICM_Router

3.20.2 Default Schedule

By default, this script runs every five minutes.

3.20.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of logged-on agents exceeds the threshold. The default is y.

Parameter	How To Set It
Collect data?	Set to **y** to collect data about logged-on agents for reports and graphs. The default is n.
Threshold - Maximum agents logged on	Specify the maximum number of agents that can be logged on before an event is raised. The default is 10 agents.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

3.21 Router_CallsInProgress

Use this Knowledge Script to monitor the number of calls in progress for a Call Router. This script raises an event if the number of calls exceeds the threshold. In addition, this script generates data streams for in-progress calls.

3.21.1 Resource Object

CISCOICM_Router

3.21.2 Default Schedule

By default, this script runs every five minutes.

3.21.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of in-progress calls exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about in-progress calls for reports and graphs. The default is n.
Threshold - Maximum calls in progress	Specify the maximum number of calls that can be in progress before an event is raised. The default is 10 calls.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

3.22 Router_CallsPerSec

Use this Knowledge Script to monitor the number of in-progress calls per second for a Call Router. This script raises an event if the number of calls exceeds the threshold. In addition, this script generates data streams for per-second calls.

3.22.1 Resource Object

CISCOICM_Router

3.22.2 Default Schedule

By default, this script runs every five minutes.

3.22.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of calls per second exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about per-second calls for reports and graphs. The default is n.
Threshold - Maximum in-progress calls per second	Specify the maximum number of in-progress calls that can occur per second before an event is raised. The default is 10 calls.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

3.23 SQL_Accessibility

Use this Knowledge Script to monitor SQL Server and database accessibility. This script raises an event if a SQL Server or a specified database is not accessible. In addition, this script generates data streams for database accessibility.

3.23.1 Resource Object

CISCOICM_SQLT_Server

3.23.2 Default Schedule

By default, this script runs every hour.

3.23.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Collect data?	Set to **y** to collect data for reports and graphs. If set to y, this script returns 100 if all specified databases are accessible, 50 if some of the specified databases are accessible and some are not, or 0 if none of the specified databases is accessible. The default is y.

Parameter	How To Set It
SQL login	Provide the database user login account that you want to use to access SQL Server. The user name you enter must have permission to access the database names for which you want to check accessibility. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Database name	Specify the database names you want to check access to, separated by commas. For example, enter `master,pubs,tempdb`. If you leave this field blank, the script checks access to all databases. The default is master.
Time out	Specify a timeout period in seconds. The timeout period is the number of seconds to wait for a response before retrying or determining the database is inaccessible. The default is 0 seconds. **NOTE**: Keep in mind when specifying a time out that the script continues waiting until it receives a response or the timeout is reached. During this waiting period, other jobs are blocked from execution. Therefore, you should limit your use of this parameter or keep the timeout period at a minimum for regular monitoring jobs. When you are running this script to troubleshoot a particular problem and not a regularly scheduled interval for ongoing maintenance, you may want to adjust this parameter to allow a longer timeout period.
Number of retries	Specify the number of times to retry connecting to the database before determining the database is inaccessible. The default is 0 retries. **NOTE**: Keep in mind when specifying this parameter that the script continues waiting until it receives a response or has made the specified number of retry attempts. During this waiting period, other jobs are blocked from execution. Therefore, you should limit your use of this parameter or keep retry attempts at a minimum for regular monitoring jobs. When you run this script to troubleshoot a particular problem and not a regularly scheduled interval for ongoing maintenance, you may want to adjust this parameter to allow more retry attempts.
Event severity when SQL Server or database is inaccessible	Set the severity level, from 1 to 40, to indicate the importance of an event in which SQL Server or the database is inaccessible. The default is 5.

3.24 SQL_CPUUtil

Use this Knowledge Script to monitor the percentage of CPU resources used by the `sqlservr` and `sqlagent` processes. This script raises an event if CPU usage exceeds the threshold you set. In addition, this script generates data streams for CPU usage (%).

3.24.1 Resource Object

CISCOICM_SQLT_Server

3.24.2 Default Schedule

By default, this script runs every 15 minutes.

3.24.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if CPU usage exceeds the threshold?	Set to **y** to raise an event if CPU usage exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about CPU usage for reports and graphs. The default is n.
Event severity when CPU usage exceeds the 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 8.
Monitor the SQL Server process?	Set to **y** to monitor SQL Server. The default is y.
Threshold - Maximum CPU usage for SQL Server process	Specify the maximum amount of CPU resources that can be consumed by the SQL process before an event is raised. The default is 10%.
Monitor the SQL Agent process?	Set to **y** to monitor SQL Agent. The default is y.
Threshold - Maximum CPU usage for SQL Agent process	Specify the maximum amount of CPU resources that can be consumed by the SQL Agent process before an event is raised. The default is 10%.

3.25 SQL_DataGrowthRate

Use this Knowledge Script to monitor the data growth and shrink rates for all SQL Server databases. Growth and shrink rates are calculated by taking the difference of the data space utilization from the current interval from the data space utilization from the last interval. This script raises an event if these rates exceed the thresholds you set. In addition, this script generates data streams for growth and shrink rates.

3.25.1 Resource Objects

CISCOICM_SQLT_DatabaseF

CISCOICM_SQLT_DatabaseObj

3.25.2 Default Schedule

By default, this script runs every hour.

3.25.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Dynamically enumerate at each interval?	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y.
Exclude these objects	Specify the name of any object you want to exclude. You can exclude multiple objects, separated by commas with no spaces. For example: `master,model,mdb`. **NOTE**: If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about data growth and shrink rates for reports and graphs. The default is n.
SQL login	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use. **NOTE**: If you are monitoring SQL Server 7, use a `sysadmin` role account. Only members of the `sysadmin` role can retrieve file statistics on SQL Server 7.0.
Threshold - Maximum growth rate	Specify the maximum rate of data growth that is allowed between the last and current interval before an event is raised. The default is 25%.
Threshold - Maximum shrink rate	Specify the maximum rate of data shrinkage that is allowed between the last and current interval before an event is raised. The default is 25%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

3.26 SQL_DBGrowthRate

Use this Knowledge Script to monitor database growth and shrink rates. Growth and shrink rates are calculated by taking the difference between the database space utilization from the current interval and the database space utilization from the last interval. This script raises an event if these rates exceed the thresholds you set. In addition, this script generates data streams for growth and shrink rates.

3.26.1 Resource Objects

CISCOICM_SQLT_DatabaseF

CISCOICM_SQLT_DatabaseObj

3.26.2 Default Schedule

By default, this script runs every hour.

3.26.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Dynamically enumerate at each interval	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y.
Exclude these objects	Specify the name of any object you want to exclude. You can exclude multiple objects, separated by commas with no spaces. For example: `master,model,mdb`. **NOTE**: If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about database growth and shrink rates for reports and graphs. The default is y.
SQL login	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use. **NOTE**: If you are monitoring SQL Server 7, use a `sysadmin` role account. Only members of the `sysadmin` role can retrieve file statistics on SQL Server 7.0.
Update usage	Set to **y** to have SQL Server recalculate the space usage. The default is n.
Threshold - Maximum growth rate	Specify the maximum percentage of database growth that is allowed between the last and current interval before an event is raised. The default is 25%.
Threshold - Maximum shrink rate	Specify the maximum percentage of database shrinkage that is allowed between the last and current interval before an event is raised. The default is 25%.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

3.27 SQL_MemUtil

Use this Knowledge Script to monitor the amount of memory that is used by Microsoft SQL Server processes: `sqlservr` and `sqlagent`.

If using SQL Server 7.0 or 2000, you can use this script to monitor total server memory usage, number of free buffers, and memory usage.

This script raises an event if memory usage exceeds the threshold you set. In addition, this script generates data streams for memory usage (%).

3.27.1 Resource Object

CISCOICM_SQLT_Server

3.27.2 Default Schedule

By default, this script runs every ten minutes.

3.27.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about memory usage for reports and graphs. The default is n.
Threshold - Maximum process memory usage	Specify the maximum amount of memory that can be consumed by SQL Server before an event is raised. The default is 50000000 bytes.
Threshold - Maximum number of free buffers	Specify the maximum number of buffers that can be in use before an event is raised. The default is 50 buffers.
Threshold - Maximum SQL Server memory usage	Specify the maximum amount of memory that can be in use by SQL Server and all related processes before an event is raised. The default is 30000000 bytes.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

3.28 SQL_RestartServer

Use this Knowledge Script to restart Microsoft SQL Server. This script raises an event if SQL Server either successfully restarts or fails to restart.

3.28.1 Resource Object

CISCOICM_SQLT_Server

3.28.2 Default Schedule

By default, this script runs once.

3.28.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Wait N seconds before restarting	Enter the number of seconds to wait after the server is stopped before attempting to automatically restart the server. The default is 5 seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop the server. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot restart the server. The default is 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot determine the status of the server. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops the server. The default is 25.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts the server. The default is 25.

3.29 Recommended Knowledge Script Group

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

- ICM_AgentData
- ICM_EventLog
- Router_AgentsLoggedOn
- Router_CallsInProgress
- SQL_DBGrowthRate

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 CiscoICM group on a Cisco UCCE resource.

The CiscoICM KSG enables a “best practices” usage of AppManager for monitoring your Cisco UCCE 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 CiscoICM tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the CiscoICM 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 CiscoICM KSG and want to restore it to its original form, you can reinstall the AppManager for Cisco Intelligent Contact Management module on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\CiscoICM` directory.