Management Guide

NetIQ® AppManager® for Microsoft Lync

Jan 2017

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 for Microsoft Lync library is available in Adobe Acrobat (PDF) format from the AppManager Documentation page of the NetIQ Web site.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

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

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, 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. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, 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, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

1 Introducing AppManager for Microsoft Lync

Microsoft Lync, formerly known as Office Communications Server (OCS), presently known as Skype for Business, integrates enterprise-ready instant messaging, presence, conferencing, and unified communications in a single offering. Lync comes in a Standard Edition for smaller companies and an Enterprise Edition for larger companies.

AppManager for Microsoft Lync provides performance and availability management for the following components:

Instant Messaging (IM) Conferencing server

This server provides server-managed instant messaging sessions for two users and instant message conferences for more than two users.

Audio/Video (A/V) Conferencing server

This server provides audio and video peer-to-peer and conferencing capabilities.

Web Conferencing server

This server provides data collaboration and application-sharing capabilities.

Teleconferencing server

This server enables audio conference integration with audio conferencing providers, or ACPs.

Enterprise pool

An Enterprise pool is a collection of Enterprise Edition servers running behind a load balancer for increased performance and availability.

Front-end server

This server hosts the various conference servers, which Microsoft calls Multipoint Control Units, or MCUs.

AppManager for Microsoft Lync also monitors the following optional components:

Mediation server

This server provides signaling and media translation between the enterprise voice infrastructure and a basic media gateway.

Edge server

This server connects external users with the system so they can participate in meetings and conferences. The following Edge servers allow specific types of multimedia conferences:

Access Edge server

This server handles Session Initiation Protocol (SIP) traffic for calls from Lync users from outside the corporate firewall.

Web Conferencing Edge server

This server connects traffic between the Web Conferencing Server and external clients.

A/V Conferencing Edge server

This server provides a single, trusted connection point through which both inbound and outbound media traffic can securely traverse network address translators, or NATs, and firewalls.

Director

This element authenticates users. If Director is not present, the front-end server handles authentication.

Archiving server

This server archives instant messages for compliance purposes. Note that the AppManager for Microsoft Lync module discovers this component, but does not monitor it.

Monitoring server

This server gathers call data record (CDR) data, Quality of Service (QoS) data, and Quality of Experience (QoE) data.

Back-end server

This server tracks all data and interactions.

NOTE: The Archiving, Monitoring, and Back-end servers require SQL Server database software. Supported versions include:

- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008 with Service Pack 1 or the latest service pack (64-bit only)
- Microsoft SQL Server 2005 with Service Pack 3 or the latest service pack (64-bit only)

Note that the Archiving and Monitoring Server databases can reside on the same computer.

For more information about configuring servers, see Installing SQL Server for the Archiving Database article.

Features and Benefits

The following are some of the features and benefits of using AppManager for Microsoft Lync:

- Monitors the availability of Lync servers and the health of all services running on Lync servers
- Monitors the total CPU usage of a server using Lync
- Monitors the VoIP call metrics contained in the Monitoring (CDR) database
- Monitors the current call activity and call failure metrics of Edge Servers and Mediation Servers
- Monitors QoS metrics to predict call quality
- Monitors end-user experience by using Lync synthetic transactions
- Tracks server uptime since last reboot
- Tracks the number and duration of all sessions occurring on Lync servers
- Tracks the load placed on servers by ongoing conferences and sessions
- Tracks any failed conferences or sessions

Understanding Features Specific to This Module

The following features will help you maximize your usage of AppManager for Microsoft Lync.

Lync Knowledge Script Group

A Knowledge Script Group, or KSG, is a set of scripts that have their parameters already set to recommended values. To run all of the recommended scripts in a KSG at one time, simply drag and drop the **KSG** group onto a Lync resource in the left pane.

The Lync KSG provides an easy way to get started, right out of the box. This KSG is displayed on the RECOMMENDED tab of the Knowledge Script pane, and includes the following scripts:

- HealthCheck, which monitors the active status of services on a Lync server.
- MCUStatus, which monitors the health and draining state of a Multipoint Control Unit (MCU).
- MediationServerHealth, which measures the global health and connectivity status of a Mediation server.
- SystemUptime, which monitors how long a server remains up and running after a reboot.
- SystemUsage, which monitors CPU usage of a Lync server and the processor time per service.

Call Activity Knowledge Script Group

Another Knowledge Script Group is the CallActivity KSG, which enables you to monitor call activity across all the server components that have been discovered. This KSG is displayed on the Lync tab, and contains the following scripts:

- ArchivedVoIPCallActivity, which monitors the various VoIP call metrics contained in the Monitoring database.
- ConferenceCallActivity, which monitors conferences and users in conferences on a Lync server.
- EdgeServerCallActivity, which monitors current call activity metrics for the Edge server.
- MediationServerCallActivity, which monitors inbound and outbound calls of a Mediation server.
- SessionCallActivity, which monitors the number of current sessions on a Lync server.

New AppManager TreeView Objects

Lync discovery generates a new application view in the Operator Console. All the new objects that can be displayed as a result of discovery will rarely be contained under a single machine in the TreeView of AppManager.

Note that you must run the Discovery script on each server hosting a Lync server component so that AppManager discovers each one separately. After discovery, AppManager displays the various Lync components under the server in the TreeView on the left side of the AppManager window.

SystemUptime Knowledge Script

To ensure that your monitored systems are being tracked after you install AppManager for Microsoft Lync, set up the parameters for the SystemUptime Knowledge Script immediately after installation. For more information, see SystemUptime.

Counting AppManager Licenses

AppManager for Microsoft Lync consumes one license for each agent computer on which Lync is discovered.

2 Installing AppManager for Microsoft Lync

This chapter provides installation instructions and describes system requirements for AppManager for Microsoft Lync.

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.

NOTE

- This release of AppManager for Microsoft Lync does not support an upgrade from the AppManager for Microsoft Office Communications Server (OCS) module.
- This module does not discover or monitor OCS components. If you plan to retain OCS components on any of your servers, run the AppManager for OCS module for those components.
- AppManager for Microsoft OCS does not support Microsoft Lync. To discover and monitor Lync components, use the AppManager for Microsoft Lync module.

System Requirements

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

AppManager for Microsoft Lync has the following system requirements:

Software	Version
NetIQ AppManager installed on the AppManager repository (QDB) computer, on the Lync computers you want to monitor (AppManager agents), and on all console computers	8.0.3, 8.2, 9.1, or later One of the following AppManager agents are required: ◆ AppManager agent 7.0.4 with hotfix 72616 or later ◆ AppManager agent 8.0.3, 8.2, 9.1, or later
Microsoft Windows operating system on the agent computers	One of the following: ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (64-bit only)
Microsoft Lync on the agent computers	2010 or 2013
Microsoft Skype for Business on agent computers	2015

Software	Version
AppManager for Microsoft Windows module installed on repository, agent, and console computers	8.0.104.0 or later. For more information, see the AppManager Module Upgrades & Trials page.
Microsoft SQL Server for Lync Supplemental Database	◆ SQL Server 2012 or SQL Server 2012 Express ◆ SQL Server 2008 R2 (32-bit and 64-bit) ◆ SQL Server 2008 (32-bit and 64-bit) or SQL Server 2008 Express (32-bit and 64-bit) ◆ SQL Server 2005 (32-bit and 64-bit) Service Pack 4 or SQL Server 2005 Express (32-bit and 64-bit) Service Pack 4
Microsoft .NET Framework installed on the Lync trusted application server	3.5

Installing the Module

Run the module installer on the Microsoft Lync computers you want to monitor (agents) to install the agent components, and run the module installer on all console computers to install the Help and console extensions.

Access the `AM70-Lync-8.x.x.0.msi` module installer from the `AAM70_Lync_8.x.x.0` self-extracting installation package on the AppManager Module Upgrades & Trials page.

For Windows environments where User Account Control (UAC) is enabled, install the module using an account with administrative privileges. Use one of the following methods:

- Log in to the server using the account named Administrator. Then, run the module installer `Lync.msi` file from a command prompt or by double-clicking it.
- Log in to the server as a user with administrative privileges and run the module installer `Lync.msi` file as an administrator from a command prompt. To open a command-prompt window at the administrative level, right-click a command-prompt icon or a Windows menu item and select **Run as administrator**.

You can install the Knowledge Scripts into local or remote AppManager repositories (QDBs). The module installer installs Knowledge Scripts for each module directly into the QDB instead of installing the scripts in the `\AppManager\qdb\kp` folder as in previous releases of AppManager.

You can install the module manually, or you can use Control Center to deploy the module to a remote computer where an agent is installed. For more information, see "Deploying the Module with Control Center" on page 15. However, if you use Control Center to deploy the module, Control Center only installs the *agent* components of the module. The module installer installs the QDB and console components as well as the agent components on the agent computer.

To install the module manually:

1. Double-click the module installer `.msi` file.
2. Accept the license agreement.
3. Review the results of the pre-installation check. You can expect one of the following three scenarios:
   - **No AppManager agent is present:** In this scenario, the pre-installation check fails, and the installer does not install agent components.

- **An AppManager agent is present, but some other prerequisite fails:** In this scenario, the default is to not install agent components because of one or more missing prerequisites. However, you can override the default by selecting **Install agent component locally**. A missing application server for this particular module often causes this scenario. For example, installing the AppManager for Microsoft SharePoint module requires the presence of a Microsoft SharePoint server on the selected computer.
- **All prerequisites are met:** In this scenario, the installer installs the agent components.

4 To install the Knowledge Scripts into the QDB:

4a Select **Install Knowledge Scripts** to install the repository components, including the Knowledge Scripts, object types, and SQL stored procedures.

4b Specify the SQL Server name of the server hosting the QDB, as well as the case-sensitive QDB name.

NOTE: Microsoft .NET Framework 3.5 is required on the computer where you run the installation program for the QDB portion of the module. For computers running more recent versions of Windows operating systems that use a newer version of .NET, install .NET 3.5 with the Add Roles and Features wizard in Windows Server Manager, as described in this Microsoft article.

---

5 (Conditional) If you use Control Center 7.x, run the module installer for each QDB attached to Control Center.

6 (Conditional) If you use Control Center 8.x or later, run the module installer only for the primary QDB. Control Center automatically replicates this module to secondary QDBs.

7 Run the module installer on all console computers to install the Help and console extensions.

8 Run the module installer on the Lync computers you want to monitor (agents) to install the agent components.

9 Set up the proper user permissions on the various Lync servers and SQL servers you will be using. For more information, see “Setting Up User Permissions for Lync” on page 17.

10 (Conditional) If you have not discovered Microsoft Lync resources, run the Discovery_Lync Knowledge Script on all agent computers where you installed the module. For more information, see “Discovering Lync Resources” on page 23.

After the installation has completed, the `Lync_Install.log` file, located in the `\NetIQ\Temp\NetIQ_Debug\`<*ServerName*> folder, lists any problems that occurred.

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.

In environments running Microsoft Windows Server 2012 with versions of AppManager prior to 8.2, you cannot remotely deploy this module and must install it manually.

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. For more information, see “Checking In the Installation Package” on page 16.
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.

Checking In the Installation Package

You must check in the installation package, `AM70-Lync-8.x.x.0.xml`, before you can deploy the module on an agent computer.

To check in a module installation package:

1. Log on to Control Center using an account that is a member of a user group with deployment permissions.
2. Navigate to the **Deployment** tab (for AppManager 8.x or later) or **Administration** tab (for AppManager 7.x).
3. In the Deployment folder, select **Packages**.
4. On the Tasks pane, click **Check in Deployment Packages** (for AppManager 8.x or later) or **Check in Packages** (for AppManager 7.x).
5. Navigate to the folder where you saved `AM70-Lync-8.x.x.0.xml` and select the file.
6. Click **Open**. The Deployment Package Check in Status dialog box displays the status of the package check in.
7. To get the updates provided in this release, upgrade any running Knowledge Script jobs. For more information, see “Upgrading Knowledge Script Jobs” on page 25.

Silently Installing the Module

To silently (without user intervention) install a module on an agent computer using the default settings, run the following command from the folder in which you saved the module installer:

```
msiexec.exe /i "AM70-Lync-8.x.x.0.msi" /qn
```

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-Lync-8.x.x.0.msi.log"
```

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

NOTE: To perform a silent install on an AppManager agent running Windows Server 2008 R2 or Windows Server 2012, open a command prompt at the administrative level and select **Run as administrator** before you run the silent install command listed above.

To silently install the module on a remote AppManager repository, you can use Windows authentication or SQL authentication.

Windows authentication:

```
AM70-Lync-8.x.x.0.msi /qn MO_B_QDBINSTALL=1 MO_B_MOINSTALL=0 MO_B_SQLSVR_WINAUTH=1
MO_SQLSVR_NAME=SQLServerName MO_QDBNAME=AM-RepositoryName
```

SQL authentication:

```
AM70-Lync-8.x.x.0.msi /qn MO_B_QDBINSTALL=1 MO_B_MOINSTALL=0 MO_B_SQLSVR_WINAUTH=0
MO_SQLSVR_USER=SQLLogin MO_SQLSVR_PWD=SQLLoginPassword
MO_SQLSVR_NAME=SQLServerName MO_QDBNAME=AM-RepositoryName
```

Setting Up User Permissions for Lync

After installing AppManager for Microsoft Lync, you will need to establish special permissions for your user accounts.

Creating a New Account

Before you can begin discovering servers with AppManager for Microsoft Lync, you need to create a domain-based account with the minimum permissions on the following servers:

- **Front-end Server**: Domain user must be a member of the **Local Administrators** group. Also the user must have Windows authentication rights on the SQL Server hosting the LcsCDR and the QoEMetrics databases with the db_datareader permission for the LcsCDR and the QoEMetrics databases.
- **Edge Server**: Domain or local user must be a member of **Local Administrators** group.
- **Mediation Server**: Domain or local user must be a member of **Local Administrators** group.
- **Trusted Application Server**: Domain user must be a member of the **Local Administrators** group and the **RTCUniversalAdminReadOnly** group.

Setting Up the NetIQmc Service

For every Lync server you are monitoring, configure the NetIQ AppManager Client Resource Monitoring (NetIQmc) service to run under the new account you created in “Creating a New Account” on page 17.

To set up the NetIQmc service:

1. On the Lync server, select the **Services** option from the **Administrative Tools** section of the Control Panel.
2. From the list of services, right-click **NetIQ AppManager Client Resource Monitor** and select **Properties**.

3 On the **Log On** tab, select **This account** and type the domain name and username of the user you created to run **NetIQ AppManager Client Resource Monitor**, such as `LYNCENT\NetIQService`. You can also use an account name that fits your company standards, as needed.

NOTE: You will need to be logged in as an administrator to update this setting.

4 Type the password you created for the new user and click **OK**.

5 Right-click **NetIQ AppManager Client Resource Monitor** from the list of services and select **Restart** to restart the service.

6 Repeat this procedure on all the Lync servers you will be monitoring.

Setting up SQL Servers

The final step for user configuration is to give your user account Read access to the relevant Microsoft SQL servers. You will need to repeat this procedure on every SQL server hosting a Monitoring database.

To set up SQL servers:

1 In SQL Server Management Studio or SQL Server Configuration Manager, navigate to the **Logins** directory from the **Security** directory of the relevant SQL server.

2 Right-click **Logins** and select **New Login**.

3 On the General page of the Login - New dialog box, type the domain name and username of the user you created to run **NetIQ AppManager Client Resource Monitor**, such as `LYNCENT\NetIQService`.

4 Select **Windows authentication**.

5 In the Default database list, select the name of the Monitoring database, such as **LcsCDR** and **QoEMetrics**, the default name for the Monitoring database.

6 On the User Mappings page of the Login - New dialog box, select the **LcsCDR** and **QoEMetrics** databases from the Users mapped to this login table.

7 Select **db_datareader access** and click **OK**.

8 Repeat this procedure for all the SQL servers hosting Monitoring databases you will be using with Lync.

Configuring the PowerShell Execution Policy

This chapter describes the procedure for configuring the Microsoft PowerShell Execution Policy. The PowerShell Execution Policy determines if PowerShell scripts are allowed to run.

Understanding PowerShell Cmdlets

Microsoft Lync server uses the Microsoft scripting and command environment known as PowerShell. PowerShell is made up of hundreds of executable objects called **cmdlets**, pronounced **command-lets**.

When running the Lync Synthetic Transaction Knowledge Scripts, AppManager makes a series of calls to PowerShell and the Lync cmdlets. For more information about using PowerShell, see your Microsoft PowerShell documentation.

Configuring the PowerShell Execution Policy

The PowerShell Execution Policy determines whether PowerShell scripts are allowed to run. By default, the Execution Policy is set to `Restricted`. If you try to run scripts under the `Restricted` policy, AppManager generates error messages.

The Execution Policy directly affects the Lync Synthetic Transaction Knowledge Scripts. Although the scripts that ship with AppManager for Lync are written in VBScript and installed as `<scriptname>.qml`, the logic for the Lync Synthetic Transaction scripts are contained in complementary PowerShell scripts that are installed on the agent computer along with the module. The PowerShell scripts use the same name as the Lync Knowledge Scripts, but with a `.ps1` extension.

NOTE: The digital signature encoded in a Lync Synthetic Transaction Knowledge Script is tied to the contents of the script. If you change the script, the signature is no longer valid and you cannot execute the script. If you change a Lync Synthetic Transaction Knowledge Script, you must do one of the following:

- Re-sign the scripts using your own digital certificate.
- Change the Execution Policy to either **RemoteSigned** or **Unrestricted**.
  A group policy that governs script execution overrides any policy changes you make with the `Set-ExecutionPolicy` cmdlet. For example, if the group policy forbids script execution, you cannot change the policy by running `Set-ExecutionPolicy`. First change the group policy to allow script execution, and then run `Set-ExecutionPolicy` to select a specific Execution Policy.

Before AppManager can execute the PowerShell scripts, you must change the Execution Policy from `Restricted` to one of the following policy options:

- **AllSigned**, which allows execution of scripts that have been digitally signed by a trusted publisher. If you select the **AllSigned** policy, perform the steps outlined in “Trusting Lync Synthetic Transaction Scripts” on page 19.
- **RemoteSigned**, which allows local scripts to run regardless of signature, and requires trusted digital signatures only for remote scripts. Lync Synthetic Transaction Knowledge Scripts are local scripts.
- **Unrestricted**, which allows both local and remote scripts to run, regardless of signature.

To change the PowerShell Execution Policy:

1. Open the Lync Command Shell on the agent computer.
2. Run the following cmdlet:

   ```
   Set-ExecutionPolicy <policy>
   ```

   where `<policy>` is the name of the Execution Policy you choose.

Trusting Lync Synthetic Transaction Scripts

When a PowerShell script is executed under an AllSigned policy, PowerShell verifies that the script contains a digital signature and that the signature is associated with a trusted publisher. NetIQ Corporation signs the Lync Synthetic Transaction scripts. If you use the **AllSigned** policy, you must

choose to trust NetIQ Corporation by importing the NetIQ Corporation digital certificate into the local certificate store on the Lync trusted application server where you plan to execute Lync synthetic transactions.

You can import the digital certificate by running one of the Lync PowerShell scripts from the command line.

To import the digital certificate:

1. Open the Lync Command Shell on the agent computer.
2. Change to the `AppManager\bin\PowerShell\Scripts` directory.
3. Type `.\Lync_SyntheticTransaction.ps1`
4. Press `Enter`.
5. Type `A` at the prompt asking whether the script should be allowed to run.
6. Press `Enter`.

These steps allow the NetIQ Corporation digital certificate to be imported into the certificate store for the user running the script. Run any script once to establish trust.

At this point, trust is established *only* between NetIQ Corporation and the user running the script. Trust is not established for any other user. If the AppManager agent runs under a different user account, such as Local System, a domain account, or a local computer account, the agent will not have a trust relationship and will not be allowed to execute the Lync Synthetic Transaction scripts.

To extend trust to all other user accounts, see “Extending Trust to All User Accounts” on page 20.

Extending Trust to All User Accounts

To execute PowerShell scripts under the **AllSigned** Execution Policy, extend trust to all user accounts. Extending trust is a two-phase process that involves exporting the digital certificate from the current user and importing the digital certificate to all users on the local computer.

Exporting the NetIQ Corporation Digital Signature Certificate

To extend trust to all user accounts, first export the NetIQ Corporation digital signature certificate from the current user using the Microsoft Management Console.

To export the NetIQ Corporation digital signature certificate from the current user:

1. On the Start menu, click **Run**.
2. In the **Open** field, type `mmc.exe`, and then click **OK**.
3. On the File menu in the Microsoft Management Console window, click **Add/Remove Snap-in**.
4. Click **Add** and then select the **Certificates** snap-in.
5. Click **Add**, select **My user account**, and then click **Finish**.
6. Click **Close** and then click **OK**. The **Certificates-Current User** node is displayed in the tree view of the Console window.
7. Expand **Certificates - Current User**.
8. Expand **Trusted Publishers** and select **Certificates**.
9. In the right pane, right-click the **NetIQ** certificate, select **All Tasks**, and then select **Export**.
10. Click **Next** in the Certificate Export Wizard.
11. Select **DER encoded binary** and then click **Next**.

12. Click **Browse**, select the **Desktop** icon, type `NetIQ` in the **File name** field, and then click **Save**.
13. Click **Next**, and then click **Finish**.

Importing the NetIQ Corporation Digital Signature

The next phase of extending trust to all user accounts involves importing the NetIQ Corporation digital signature to all users on the local computer. Use the Microsoft Management Console to execute the import procedure.

To import the NetIQ Corporation digital certificate to all users on the local computer:

1. On the File menu in the Microsoft Management Console window, click **Add/Remove Snap-in**.
2. Click **Add** and then select the **Certificates** snap-in.
3. Click **Add**, select **Computer account**, and then click **Next**.
4. Select **Local computer** and then click **Finish**.
5. Click **Close** and then click **OK**.
6. Expand **Certificates (Local Computer)** and select **Trusted Publishers**.
7. Right-click in the right pane, select **All Tasks**, and then select **Import**.
8. Click **Next** in the Certificate Import Wizard.
9. Click **Browse**, click the **Desktop** icon, select **NetIQ.cer**, and then click **Open**.
10. Click **Next** in the Wizard.
11. Select **Place all certificates in the following store**.
12. Click **Browse** and then select **Show physical stores**.
13. Expand **Trusted Publishers** and select **Local Computer**.
14. Click **OK**.
15. Click **Next** in the Certificate Import Wizard, and then click **Finish**.

After you complete both the phases of the trust process, the NetIQ Corporation certificate is contained in the certificate store for the local computer, allowing all users to execute the PowerShell scripts.

Setting Up Lync Trusted Application Server

To run the Lync_SyntheticTransaction Knowledge Script, you must configure a Lync trusted application server that is capable of executing the Lync synthetic transaction PowerShell commandlets. The Lync synthetic transactions are executed on the Lync trusted application server.

To set up trusted application server:

1. Add the agent computer on which you want to run the Lync_SyntheticTransaction Knowledge Script to the Lync Topology and then publish the topology.
2. Install local configuration store on the agent computer by using the Lync deployment wizard.
3. Assign the default certificate to the agent computer by using the Lync deployment wizard.
4. Launch the Lync management PowerShell and execute the following commandlet to create new trusted application:

   ```
   New-CsTrustedApplication -ApplicationID <ApplicationID> -
   TrustedApplicationPoolFqdn <FQDN of the trusted application server> -Port 5061
   ```

5 Execute `Enable-CsTopology` from the Lync management PowerShell to enable the topology.

6 Create two Lync test users for each monitored Lync FrontEnd pools.

7 Execute the following commandlet from the Lync management PowerShell to set up the monitoring configuration for each Lync FrontEnd pool, which is monitored using synthetic transactions:

```
New-CsHealthMonitoringConfiguration -TargetFqdn <FQDN of the FrontEnd pool> -
FirstTestUserSipUri "<Test user 1 SIP URI>" -FirstTestSamAccountName
"<DOMAIN\TestUser1>" -SecondTestUserSipUri "<Test User 2 SIP URI>" -
SecondTestSamAccountName "<DOMAIN\TestUser2>"
```

Configuring Security Manager Settings for the Supplemental Database

To measure the call quality of the Lync deployment, you need to store the call detail records (audio, video, and call sharing) in the supplemental database. To avoid getting an error message when running the Discovery_Lync script, with *Setup supplemental database* parameter selected, or when running the Lync_SetupSupplementalDB Knowledege Script, use AppManager Security Manager to store the SQL user name and password information for the SQL Server.

NOTE

- You can create the supplemental database only when you run the discovery or the Lync_SetupSupplementalDB Knowledge Script on a front-end pool server.
- The following configuration is required only when you want to set up the supplemental database on a SQL server configured for SQL authentication.

On the **Custom** tab in Security Manager, complete the following fields for the SQL Server where you want to create the supplemental database:

Field	Description

Label	Specify the SQL Server name and the instance name of the SQL Server hosting the Lync supplemental database.
	
	Use the following structure:
	
	`SQL$SQL Server Name\Instance Name`
	
	For example:
	
	`SQL$HOUSERVER2\DB1`

Sub-Label	Specify the username. The user should have proper permissions to create the database on the SQL server.
Value1	Specify the password for the user specified in the *Sub-Label* field.
Extended application support	Select this option to encrypt the password in Security Manager. This option is required.

Discovering Lync Resources

Use the Discovery_Lync Knowledge Script to discover all known resources on a Lync server. The script discovers Lync Enterprise and Standard editions, Mediation servers, and Edge servers. When AppManager discovers a Lync component, that component is displayed under the relevant server in the TreeView on the left side of the AppManager window.

Before running discovery, ensure you have set up the proper user permissions on the various Lync servers and SQL servers you will be using. For more information, see "Setting Up User Permissions for Lync" on page 17.

The default interval for this script is weekly; the default is Sundays at 3 A.M.

If you delete or add a resource object, or if you make any other kind of change that might affect the monitoring of your resources, run the Discovery_Lync Knowledge Script again to update your list of resource objects. In addition, if you are running this module on AppManager 8 or later, you can use the delta discovery feature in Control Center to run discovery on a schedule to more quickly detect changes to your environment.

Set the **Values** tab parameters as needed:

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the discovery job fails. The default is 5.
Raise event if discovery succeeds?	Select **Yes** to raise an event when the discovery process is successful. The default is unchecked.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when discovery succeeds. The default is 25.
Raise event if discovery succeeds with warnings?	Select **Yes** to raise an event when the discovery process succeeds but generates some warnings. The default is Yes.
Event severity when discovery succeeds with warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when discovery succeeds with warnings. The default is 15.
Raise event if discovery fails?	Select **Yes** to raise an event when the discovery process fails. The default is Yes.
Event severity when discovery fails	If you set this Knowledge Script to raise an event when the job fails, set the event severity level for a failed discovery. The default is 10.
Set up supplemental database?	Select **Yes** to set up Lync supplemental database to store call quality detail records (audio, video, and application sharing calls) on a server where SQL database exists. You need to configure the SQL server credentials in the Security Manager to create a supplemental database. For more information, see "Configuring Security Manager Settings for the Supplemental Database" on page 22.
Raise event if database setup succeeds?	Select **Yes** to raise an event if creation of the Lync supplemental database is successful. The default is unselected.

Description	How To Set It
Event severity when database setup succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Lync supplemental database is created successfully. The default is 25.
Raise event if database setup fails?	Select **Yes** to raise an event if creation of the Lync supplemental database fails. The default is unselected.
Event severity when database setup fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Lync supplemental database is not created. The default is 15. It is possible that the supplemental database was not created because of one of the following reasons: ◆ The Discovery job was run with the *Set up supplemental database* parameter selected on a computer other than a front-end pool server ◆ The Discovery job was run on a computer with the *Set up supplemental database* parameter selected on which SQL Server is not installed ◆ The Discovery job was run on a computer with the *Set up supplemental database* parameter selected where Lync supplemental database was already created
Start pruning job on supplemental database?	Select **Yes** to create a SQL job that deletes data from the supplemental database. The SQL job runs every night. The default is Yes. Data is deleted from the supplemental database based on the value you specify in the *Number of days to keep call detail records* parameter.
Number of days to keep call detail records	Specify the number of days' worth of call detail records to keep in the Lync supplemental database. Data older than what you specify is discarded. The default is 7 days. You can specify a maximum of 30 days.
SQL Server Information	
SQL Server \instance name	Specify the SQL Server name where you want to create the new Lync Server supplemental database along with the instance if any. If you specify both the SQL Server instance name for this parameter and the SQL Server database user name in the following parameter, these values must match the values you specified in "Configuring Security Manager Settings for the Supplemental Database" on page 22. If this field is left blank, then the script uses the default SQL server on the agent computer to create the supplemental database in the Lync agent where you run the discovery or the Lync_SetupSupplementalDB script. If SQL database is not present on Lync agent, then the script fails to create the database. If you do not specify the instance name, the script creates the database in the default instance.
SQL database user name	Specify the user name for the SQL Server where you want to create the new Lync Server supplemental database. Leave this parameter blank to use Windows authentication instead of SQL authentication.

Upgrading Knowledge Script Jobs

If you are using AppManager 8.x or later, the module upgrade process now *retains* any changes you might have made to the parameter settings for the Knowledge Scripts in the previous version of this module. Before AppManager 8.x, the module upgrade process *overwrote* any settings you might have made, changing the settings back to the module defaults.

As a result, if this module includes any changes to the default values for any Knowledge Script parameter, the module upgrade process ignores those changes and retains all parameter values that you updated. Unless you review the management guide or the online Help for that Knowledge Script, you will not know about any changes to default parameter values that came with this release.

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.

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. 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.

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. You might need to appropriately set new parameters for your environment or application.

If you are not using AppManager 8.x or later, customized script parameters might have reverted to default parameters during the installation of the module.

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 the properties and the script.

For more information about propagating Knowledge Script changes, see the “Running Monitoring Jobs” chapter of the *Control Center User Guide for AppManager*.

Propagating Changes to Ad Hoc Jobs or Knowledge Script Groups

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.

You can also propagate the properties and logic 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. Any monitoring jobs started by a Knowledge Script Group member are restarted with the job properties of the Knowledge Script Group member.

To propagate changes to ad hoc Knowledge Script jobs or Knowledge Script Groups:

1. In the Knowledge Script view, select the Knowledge Script or Knowledge Script Group for which you want to propagate changes.
2. Right-click the script or group and select **Properties propagation** > **Ad Hoc Jobs**.
3. Select the components of the Knowledge Script that you want to propagate to associated ad hoc jobs or groups and click **OK**:

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. If you are using AppManager 8.x or later, the module upgrade process now *retains* any changes you might have made to the parameter settings for the Knowledge Scripts in the previous version of this module.

3 Lync Knowledge Scripts

Microsoft Lync combines enterprise-ready instant messaging, presence capabilities, conferencing, unified communications, and administrative controls in a single offering. Lync adds real-time conferencing hosted on servers inside the corporate firewall to existing features such as federation and public instant-messaging connectivity.

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

Knowledge Script	What It Does
ArchivedVoIPCallActivity	Monitors the various VoIP call metrics contained in the Monitoring (CDR) database.
CallActivity	Group of all CallActivity Knowledge Scripts.
CallQuality	Monitors call quality metrics such as MOS, round trip, jitter, and packet loss.
CollectCallData	Polls Lync Quality of Experience (QoE) metrics databases for call quality metrics and saves the data to the Lync supplemental database.
ConferenceCallActivity	Monitors the number of active conferences and the number of users in those conferences.
EdgeServerCallActivity	Monitors current call activity metrics of an Edge server.
EdgeServerCallFailures	Monitors current call failure metrics of an Edge server.
ExtendedSyntheticTransaction	Monitors the health of the Lync deployment by executing extended Lync synthetic transaction test against the Lync Front End pools. Reports the test result and latency, which helps in understanding the end-user experience.
HealthCheck	Monitors the active status of Lync server services.
MCUStatus	Monitors the health and draining state of a Multipoint Control Unit (MCU).
MediationServerCallActivity	Monitors the current inbound and outbound calls of a Mediation server.
MediationServerCallFailures	Monitors the session failure metrics of a Mediation server.
MediationServerHealth	Monitors the server health metrics of a Mediation server.
MediationServerUsage	Monitors the server resource usage of a Mediation server.
SessionCallActivity	Monitors the session initiation rate of a Lync server.
SessionCallFailures	Monitors session failure metrics of a Lync server.
SetupSupplementalDB	Creates a Lync supplemental database to store call quality metrics (audio, video, and application sharing).

Knowledge Script	What It Does
SyntheticTransaction	Monitors the health of the Lync deployment by executing Lync synthetic transaction test against the Lync Front End pools. Reports the test result and latency, which helps in understanding the end-user experience.
SystemUptime	Monitors the length of time a system has been up and running since a reboot.
SystemUsage	Monitors the total CPU and memory usage of a Lync server.

ArchivedVoIPCallActivity

Use this Knowledge Script to monitor the various Voice over IP (VoIP) call metrics contained in the Monitoring database. This script monitors the number of total VoIP calls made, the types of calls made, the average duration of calls, the number of redirected calls, and the number of calls per gateway.

A gateway is third-party hardware that connects Microsoft Lync with a public switched telephone network (PSTN), private branch exchange (PBX), or other phone system.

Resource Objects

Monitoring Server

Default Schedule

The default interval for this script is 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the ArchivedVoIPCallActivity job fails. The default is 5.
Monitor Total Number of VoIP Calls	
Event Notification	
Raise event if total number of VoIP calls exceeds the threshold?	Select **Yes** to raise an event if the number of VoIP calls exceeds the threshold. The default is Yes.
Threshold - Maximum total number of VoIP calls	Specify the maximum number of VoIP calls that can be active before an event is raised. The default is 20.

Description	How to Set It
Event severity when total number of VoIP calls exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of VoIP calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for total number of VoIP calls?	Select **Yes** to collect data about the number of VoIP calls. The default is Yes.
Monitor Total Number of UC to PSTN Calls	
Event Notification	
Raise event if total number of UC to PSTN calls exceeds threshold?	Select **Yes** to raise an event if the number of unified communications (UC) calls to public switched telephone network (PSTN) calls exceeds the threshold. The default is Yes.
Threshold - Maximum total number of UC to PSTN calls	Specify the maximum number of UC to PSTN calls that can be active before an event is raised. The default is 20.
Event severity when total number of UC to PSTN calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for total number of UC to PSTN calls?	Select **Yes** to collect data about the number of UC to PSTN calls. The default is Yes.
Monitor Total Number of PSTN to UC Calls	
Event Notification	
Raise event if total number of PSTN to UC calls exceeds threshold?	Select **Yes** to raise an event if the number of PSTN to UC calls exceeds the threshold. The default is Yes.
Threshold - Maximum total number of PSTN to UC calls	Specify the maximum number of PSTN to UC calls that can be active before an event is raised. The default is 20.
Event severity when total number of PSTN to UC calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for total number of PSTN to UC calls?	Select **Yes** to collect data about the number of PSTN to UC calls. The default is Yes.
Monitor Average Duration of Calls	
Event Notification	
Raise event if average duration of calls exceeds threshold?	Select **Yes** to raise an event if the average duration of calls exceeds the threshold. The default is Yes.
Threshold - Maximum average duration of calls	Specify the maximum average call duration that can occur before an event is raised. The default is 20.
Event severity when the average duration of calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the average duration of calls exceeds the threshold. The default is 15.

Description	How to Set It
Data Collection	
Collect data for average duration of calls?	Select **Yes** to collect data about the average duration of calls. The default is Yes.
Monitor Number of Redirected Calls	
Event Notification	
Raise event if total number of redirected calls exceeds threshold?	Select **Yes** to raise an event if the number of redirected, or transferred, calls exceeds the threshold. The default is Yes.
Threshold - Maximum total number of redirected calls	Specify the maximum number of calls that can be redirected before an event is raised. The default is 20.
Event severity when total number of redirected calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of redirected calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of redirected calls?	Select **Yes** to collect data about the number of redirected calls. The default is Yes.
Monitor Number of Calls per Gateway	
Event Notification	
Raise event if total number of calls per gateway exceeds threshold?	Set to **Yes** to raise an event if the number of calls per gateway exceeds the threshold. The default is Yes.
Threshold - Maximum total number of calls per gateway	Specify the maximum number of calls that the gateway can handle before an event is raised. The default is 20.
Event severity when total number of calls per gateway exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of calls per gateway?	Select **Yes** to collect data about the number of calls per gateway. The default is Yes.

CallActivity

Call Activity is a Knowledge Script Group that enables you to monitor call activity across all the server components that have been discovered. This KSG includes all the CallActivity Knowledge Scripts, such as ConferenceCallActivity, EdgeServerCallActivity, MediationServerCallActivity, and SessionCallActivity. Refer to the appropriate Knowledge Scripts for detailed description.

CallQuality

Use this Knowledge Script to monitor Lync call quality information stored in the Lync supplemental database for call quality statistics for audio, video, and application sharing calls. The statistics include round trip, jitter, packet loss, and Mean Opinion Score (MOS). The script raises an event if a monitored call quality statistic falls below or exceeds a threshold. The script generates data streams for all monitored call quality statistics of audio, video and application sharing calls.

This script checks the supplemental database tables at each specified interval for new records that match your query.

Understanding Data Streams and Threshold Events

This script generates data streams for average round trip, jitter, and packet loss for audio, video, and application sharing calls. This script also generates data streams for average MOS for audio calls. These average values are based on data from each call that passes through the Lync Server during the script's interval, which is, by default, every 5 minutes. For example, in an audio call, if the jitter of any audio stream (incoming/outgoing) is greater that 60 milliseconds, AppManager raises an event for that audio call.

Prerequisites

- Run Lync SetupSupplementalDB to create the Lync Server supplemental database.
- Because the Lync_CallQuality script reports on data stored in the supplemental database by a data collector service, data must exist in the supplemental database before the reporting can be successful. To place data in the supplemental database, run Lync_CollectCallData on the Lync Server being monitored before you run the CallQuality script. If the CollectCallData script stops, the data collection also stops, even if the CallQuality script is still running.

Resource Object

Monitoring Server

Default Schedule

By default, this script runs **every 5 minutes**.

NOTE: Ensure that Lync_CollectCallData Knowledge Script runs at a faster interval than this script.

Setting Parameter Values

Set the following parameters as needed:

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

Parameter	How to Set It
Raise event if no records found?	Select **Yes** to raise an event if there are no records in the Lync supplemental database or when no records exist in the database that matches the filter criteria. If you select Yes and this script raises this event, check the status of the job run by the Lync_CollectCallData Knowledge Script. The default is unselected.
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no Lync packets were found. The default is 25.
Call Details	
Include call details?	Select **Yes** to include call details in the events raised by this script. The default is Yes. Leave this parameter unselected to suppress the following call details: ◆ Calling Party ◆ Called Party ◆ Caller and Called Average MOS ◆ Caller and Called Average Round Trip ◆ Caller and Called Jitter ◆ Caller and Called Lost Packets ◆ Start Time ◆ End Time ◆ Duration Calling Party and Called Party details usually contain SIP address, such as sip:example@example.com.
Query Filters	
Minimum duration	Use this parameter to filter out records whose call duration is less than the value you specify. Accept the default of 0 seconds to ignore the filter for minimum duration.
Maximum table size	Specify the maximum number of detail rows to include in an event message. The default is 50 rows.
Maximum duration	Use this parameter to filter out records whose call duration is greater than or equal to the value you specify. Accept the default of 0 seconds to ignore the filter for maximum duration.
Calling party	Specify the calling party SIP address that you want to find in the supplemental database. You can use a percentage (%) as a wildcard character. For example, if you specify `%@netiq.corp`, the script will search for all reported calling parties within the netiq.corp domain. Leave this parameter blank to search for any calling party.
Party connector	Set this parameter only if you specified a party for both the *Calling party* parameter and the *Called party* parameter. Your selection indicates how the script will connect the two parameters: AND or OR. The default is AND.

Parameter	How to Set It
Called party	Specify the called party SIP address that you want to find in the supplemental database. You can use an percentage (%) as a wildcard character. For example, if you specify `%@netiq.corp`, the script will search for all reported called parties within the netiq.corp domain. Leave this parameter blank to search for any called party.
Monitor Audio Call	
Monitor Average MOS	
Event Notification	
Raise event if average MOS falls below threshold?	Select **Yes** to raise an event if the average MOS value falls below the threshold. The default is Yes.
Threshold - Average MOS	Specify the lowest average MOS value, from 0.0 to 5.0, that must occur to prevent an event from being raised. The default is 3.60.
Event severity when average MOS falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average MOS value falls below the threshold. The default is 5.
Data Collection	
Collect data for average MOS?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average MOS value during the monitoring period. The default is unselected.
Monitor Average Round Trip	
Event Notification	
Raise event if average round trip exceeds threshold?	Select **Yes** to raise an event if the average round trip value exceeds the threshold. The default is Yes.
Threshold - Average round Trip	Specify the highest average round trip value, in milliseconds, that can occur before an event is raised. The default is 50 milliseconds.
Event severity when average round trip exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average round trip value exceeds the threshold. The default is 15.
Data Collection	
Collect data for average round trip?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of average round trip that occurred during the monitoring period. The default is unselected.
Monitor Average Jitter	
Event Notification	
Raise event if jitter exceeds threshold?	Select **Yes** to raise an event if the average jitter value exceeds the threshold. The default is Yes.
Threshold - Maximum jitter	Specify the highest average jitter value, in milliseconds, that can occur before an event is raised. The default is 60 milliseconds.
Event severity when jitter exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average jitter value exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for jitter?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of average jitter that occurred during the monitoring period. The default is unselected.
Monitor Average Packet Loss	
Event Notification	
Raise event if packet loss exceeds threshold?	Select **Yes** to raise an event if the average packet loss value exceeds the threshold. The default is Yes.
Threshold - Maximum packet loss	Specify the highest percentage of average packet loss that can occur before an event is raised. The default is 1%.
Event severity when packet loss exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the packet loss value exceeds the threshold. The default is 15.
Data Collection	
Collect data for packet loss?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of packet loss that occurred during the monitoring period. The default is unselected.
Monitor Video Call	
Monitor Average Round Trip	
Event Notification	
Raise event if average round trip exceeds threshold?	Select **Yes** to raise an event if the average round trip value exceeds the threshold. The default is Yes.
Threshold - Average round trip	Specify the highest average round trip value, in milliseconds, that can occur before an event is raised. The default is 50 milliseconds.
Event severity when average round trip exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average round trip value exceeds the threshold. The default is 15.
Data Collection	
Collect data for average round trip?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of average round trip that occurred during the monitoring period. The default is unselected.
Monitor Average Jitter	
Event Notification	
Raise event if jitter exceeds threshold?	Select **Yes** to raise an event if the average jitter value exceeds the threshold. The default is Yes.
Threshold - Maximum jitter	Specify the highest average jitter value, in milliseconds, that can occur before an event is raised. The default is 30 milliseconds.
Event severity when jitter exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average jitter value exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for jitter?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of average jitter that occurred during the monitoring period. The default is unselected.
Monitor Average Packet Loss	
Event Notification	
Raise event if packet loss exceeds threshold?	Select **Yes** to raise an event if the average packet loss value exceeds the threshold. The default is Yes.
Threshold - Maximum packet loss	Specify the highest percentage of average packet loss that can occur before an event is raised. The default is 1%.
Event severity when packet loss exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the packet loss value exceeds the threshold. The default is 15.
Data Collection	
Collect data for packet loss?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of packet loss that occurred during the monitoring period. The default is unselected.
Monitor Application Sharing Call	
Monitor Average Round Trip	
Event Notification	
Raise event if average round trip exceeds threshold?	Select **Yes** to raise an event if the average round trip value exceeds the threshold. The default is Yes.
Threshold - Average round trip	Specify the highest average round trip value, in milliseconds, that can occur before an event is raised. The default is 50 milliseconds.
Event severity when average round trip exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average round trip value exceeds the threshold. The default is 15.
Data Collection	
Collect data for average round trip?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of average round trip that occurred during the monitoring period. The default is unselected.
Monitor Average Jitter	
Event Notification	
Raise event if jitter exceeds threshold?	Select **Yes** to raise an event if the average jitter value exceeds the threshold. The default is Yes.
Threshold - Maximum jitter	Specify the highest average jitter value, in milliseconds, that can occur before an event is raised. The default is 100 milliseconds.
Event severity when jitter exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average jitter value exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for jitter?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of average jitter that occurred during the monitoring period. The default is unselected.

CollectCallData

Use this Knowledge Script to poll Lync Quality of Experience (QoE) metrics databases for call quality metrics to store the data in Lync supplemental database. This Knowledge Script raises an event when the Knowledge Script fails or when the Lync call quality metrics data collection fails.

Prerequisite

Run SetupSupplementalDB to create the Lync supplemental database.

Resource Object

Monitoring Server Object

Default Schedule

By default, this script runs every 1 minute.

Setting Parameter Values

Set the following parameters as needed:

Description	How to set it
General Settings	
Job Failure Notification	
Event Severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Call Data Collection	
Call Data Collection Failure Notification	
Event severity when Call Data Collection fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when call data collection fails. The default is 5.
Raise event when Call Data Collection succeeds	Select **Yes** to raise an event if the job is successful. The default is Yes.
Event severity when Call Data Collection succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when call data collection is successful. The default is 25.

ConferenceCallActivity

Use this Knowledge Script to monitor the number of active conferences, and the number of users involved in those conferences, on a Lync server. The conference type can be instant message (IM), telephony, A/V, or Web.

Resource Object

Conferences Object

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor IM Conferences	
Event Notification	
Raise event if number of IM conferences exceeds threshold?	Select **Yes** to raise an event if the number of instant message conferences exceeds the threshold. The default is Yes.
Threshold - Maximum number of IM conferences	Specify the maximum number of IM conferences that can be active before an event is raised. The default is 25.
Event severity when number of IM conferences exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of IM conferences exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of IM conferences?	Select **Yes** to collect data about the number of IM conferences. The default is unchecked.
Monitor A/V Conferences	
Event Notification	
Raise event if number of A/V conferences exceeds threshold?	Select **Yes** to raise an event if the number of A/V conferences exceeds the threshold. The default is Yes.
Threshold - Maximum number of A/V conferences	Specify the maximum number of A/V conferences that can be active before an event is raised. The default is 25.

Description	How to Set It
Event severity when number of A/V conferences exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of A/V conferences exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of A/V conferences?	Select **Yes** to collect data about the number of A/V conferences. The default is unchecked.
Monitor Telephony Conferences	
Event Notification	
Raise event if number of telephony conferences exceeds threshold?	Select **Yes** to raise an event if the number of telephony conferences exceeds the threshold. The default is Yes.
Threshold - Maximum number of telephony conferences	Specify the maximum number of telephony conferences that can be active before an event is raised. The default is 25.
Event severity when number of telephony conferences exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of telephony conferences exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of telephony conferences?	Select **Yes** to collect data about the number of telephony conferences. The default is Yes.
Monitor Web Conferences	
Event Notification	
Raise event if number of Web conferences exceeds threshold?	Select **Yes** to raise an event if the number of Web conferences exceeds the threshold. The default is Yes.
Threshold - Maximum number of Web conferences	Specify the maximum number of Web conferences that can be active before an event is raised. The default is 25.
Event severity when number of Web conferences exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of Web conferences exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of Web conferences?	Select **Yes** to collect data about the number of Web conferences. The default is Yes.
Monitor IM Conference Users	
Event Notification	
Raise event if number of IM conference users exceeds threshold?	Select **Yes** to raise an event if the number of IM conference users exceeds the threshold. The default is Yes.
Threshold - Maximum number of IM conference users	Specify the maximum number of IM conference users that can be active before an event is raised. The default is 10.
Event severity when number of IM conference users exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of IM conference users exceeds the threshold. The default is 15.

Description	How to Set It
Data Collection	
Collect data for number of IM conference users?	Select **Yes** to collect data about the number of IM conference users. The default is Yes.
Monitor A/V Conference Users	
Event Notification	
Raise event if number of A/V conference users exceeds threshold?	Select **Yes** to raise an event if the number of A/V conference users exceeds the threshold. The default is Yes.
Threshold - Maximum number of A/V conference users	Specify the maximum number of A/V conference users that can be active before an event is raised. The default is 10.
Event severity when number of A/V conference users exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of A/V conference users exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of A/V conference users?	Select **Yes** to collect data about the number of A/V conference users. The default is Yes.
Monitor Telephony Conference Users	
Event Notification	
Raise event if number of telephony conference users exceeds threshold?	Select **Yes** to raise an event if the number of telephony conference users exceeds the threshold. The default is Yes.
Threshold - Maximum number of telephony conference users	Specify the maximum number of telephony conference users that can be active before an event is raised. The default is 10.
Event severity when number of telephony conference users exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of telephony conference users exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of telephony conference users?	Select **Yes** to collect data about the number of telephony conference users. The default is Yes.
Monitor Web Conference Users	
Event Notification	
Raise event if number of Web conference users exceeds threshold?	Select **Yes** to raise an event if the number of Web conference users exceeds the threshold. The default is Yes.
Threshold - Maximum number of Web conference users	Specify the maximum number of Web conference users that can be active before an event is raised. The default is 10.
Event severity when number of Web conference users exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of Web conference users exceeds the threshold. The default is 15.
Data Collection	

Description	How to Set It
Collect data for number of Web conference users?	Select **Yes** to collect data about the number of Web conference users. The default is Yes.

EdgeServerCallActivity

Use this Knowledge Script to monitor call activity metrics of an Edge Server, including the number of active server connections. This script also monitors the number of connections that are slow because they are overloaded, also known as throttling. In addition, this script monitors the number of disconnected server connections.

Resource Object

Edge Server

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Active Server Connections	
Event Notification	
Raise event if the number of active server connections exceeds threshold?	Select **Yes** to raise an event if the number of active server connections exceeds the threshold. The default is Yes.
Threshold - Maximum active server connections	Specify the maximum number of active server connections that can occur before an event is raised. The default is 100.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of active server connections exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of active server connections?	Select **Yes** to collect data about the active server connections. The default is Yes.
Monitor Throttled Connections	

Description	How to Set It
Event Notification	
Raise event if number of throttled connections exceeds threshold?	Select **Yes** to raise an event if the number of throttled connections exceeds the threshold. Throttled connections are when connections are slow as a result of being overloaded. The default is Yes.
Threshold - Maximum number of throttled connections	Specify the maximum number of throttled connections that can occur before an event is raised. The default is 15.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of throttled connections exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of throttled server connections?	Select **Yes** to collect data about the number of throttled server connections. The default is Yes.
Monitor Disconnected Server Connections	
Event Notification	
Raise event if number of disconnected server connections exceeds threshold?	Select **Yes** to raise an event if the number of disconnected server connections exceeds the threshold. The default is Yes.
Threshold - Maximum disconnected server connections	Specify the maximum number of disconnected server connections that can occur 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 that is raised when the number of disconnected server connections exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of server connections disconnected due to throttling?	Select **Yes** to collect data about the number of server connections disconnected because of throttling. The default is Yes.

EdgeServerCallFailures

Use this Knowledge Script to monitor current call failure metrics of an Edge server. This script generates a data stream for the number of connection failures and raises an event if the number of connection failures exceeds the specified threshold.

Resource Object

Edge Server

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Connection Failures	
Event Notification	
Raise event if the number of connection failures exceeds threshold?	Select **Yes** to raise an event if the number of connection failures exceeds the threshold. The default is Yes.
Threshold - Maximum connection failures	Specify the maximum number of connections that can fail before an event is raised. The default is 15.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of connection failures exceeds the threshold. The default is 15.
Data Collection	
Collect data for the number of connection failures?	Select **Yes** to collect data about the number of connection failures. The default is Yes.

ExtendedSyntheticTransaction

Use this Knowledge Script to monitor the health of a Lync deployment by executing the Lync extended synthetic transaction test on the Lync Front End pool. This Knowledge Script reports the result and latency of the Lync extended synthetic transaction test, which helps in understanding the end-user experience. This script generates relevant data streams for the test latency.

Before running this Knowledge Script, you need to set up and configure Lync Trusted Application Server. For more information about configuring a trusted application server, see “Setting Up Lync Trusted Application Server” on page 21.

To run this Knowledge Script, you should first discover the Lync trusted application server and every Lync FrontEnd pool within the server.

Resource Objects

Front End Pool

Default Schedule

The default interval for this script is 1 hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the ExtendedSyntheticTransaction job fails. The default is 5.
Extended Lync Test	
Test Peer-To-Peer PSTN Call	Select **Yes** to run the test for Peer-To-Peer PSTN Call against your Lync Pool.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Peer-To-Peer PSTN Call test fails. The default is 5.
Peer-To-Peer PSTN Call Latency	
Raise event if latency exceeds the threshold	Select this option to raise an event when the peer-to-peer PSTN call latency exceeds the threshold. This option is selected by default.
Latency threshold	Specify the threshold in milliseconds for the latency of the Peer-To-Peer PSTN Call test. The default is 1000.
Event severity when Latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the latency of Peer-To-Peer PSTN call exceeds the threshold. The default is 10.
Collect data for latency	Select **Yes** to collect the data stream for the Peer-To-Peer PSTN Call latency.
Test Conference Join Launcher	Select **Yes** to run the test for Conference Join Launcher against your Lync Pool. **NOTE:** This test is not supported for Lync 2010.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Conference Join Launcher test fails. The default is 5.
Conference Join Launcher Latency	
Raise event if latency exceeds the threshold	Select this option to raise an event when the Conference Join Launcher latency exceeds the threshold. This option is selected by default.
Latency threshold	Specify the threshold in milliseconds for the latency of the Conference Join Launcher test. The default is 1000.
Event severity when Latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the latency of the Conference Join Launcher exceeds the threshold. The default is 10.
Collect data for latency	Select **Yes** to collect the data stream for the Conference Join Launcher latency.
Test Audio Conferencing Provider	Select **Yes** to run the test for Audio Conferencing Provider against your Lync Pool. **NOTE:** This test is not supported for Lync 2010.

Parameter	How to Set It
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event when the Audio Conferencing Provider test fails. The default is 5.
Audio Conferencing Provider Latency	
Raise event if latency exceeds the threshold	Select **Yes** to raise an event when the latency of Audio Conferencing Provider exceeds the threshold. This option is selected by default.
Latency threshold (milliseconds)	Specify the threshold in milliseconds for the latency of the Audio Conferencing Provider test. The default is 1000.
Event severity when Latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Audio Conferencing Provider latency exceeds the threshold. The default is 10.
Collect data for latency	Select **Yes** to collect the data stream for the Audio Conferencing Provider latency.
Test Audio/Video Edge Connectivity	Select **Yes** to run the test for Audio/Video Edge Connectivity against your Lync Pool. **NOTE:** This test is not supported for Lync 2010.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Audio/Video Edge Connectivity test fails. The default is 5.
Audio/Video Edge Connectivity Latency	
Raise event if latency exceeds the threshold	Select **Yes** to raise an event when the latency of Audio/Video Edge Connectivity exceeds the threshold. This option is selected by default.
Latency threshold (milliseconds)	Specify the threshold in milliseconds for the latency of Audio/Video Edge Connectivity test. The default is 1000.
Event severity when latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Audio/Video Edge Connectivity latency exceeds the threshold. The default is 10.
Collect data for latency	Select **Yes** to collect the data stream for the Audio/Video Edge Connectivity latency.
Test Data Conference	Select **Yes** to run the test for Data Conference against your Lync Pool. **NOTE:** This test is not supported for Lync 2010.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Data Conference test fails. The default is 5.
Data Conference Latency	
Raise event if latency exceeds the threshold	Select **Yes** to raise an event when the latency of Data Conference exceeds the threshold. This option is selected by default.
Latency threshold	Specify the threshold in milliseconds for the latency of Data Conference test. The default is 1000.
Event severity when Latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Data Conference latency exceeds the threshold. The default is 10.
Collect data for latency	Select **Yes** to collect the data stream for the Data Conference latency.

Parameter	How to Set It
Test Exchange Unified Messaging Connectivity	Select **Yes** to run the test for Exchange Unified Messaging Connectivity against your Lync Pool. **NOTE:** This test is not supported for Lync 2010.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Exchange Unified Messaging Connectivity test fails. The default is 5.
Exchange Unified Messaging Connectivity Latency	
Raise event if latency exceeds the threshold	Select **Yes** to raise an event when the latency of Exchange Unified Messaging connectivity exceeds the threshold. This option is selected by default.
Latency threshold	Specify the threshold in milliseconds for the latency of Exchange Unified Messaging Connectivity test. The default is 1000.
Event severity when latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Exchange Unified Messaging Connectivity latency exceeds the threshold. The default is 10.
Collect data for latency	Select **Yes** to collect the data stream for the Exchange Unified Messaging Connectivity latency.
Test Persistent Chat	Select **Yes** to run the test for Persistent Chat against your Lync Pool. **NOTE:** This test is not supported on Lync 2010.
Test failure event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Persistent Chat test fails. The default is 5.
Persistent Chat Latency	
Raise event if latency exceeds the threshold	Select **Yes** to raise an event when the latency of Persistent Chat exceeds the threshold. This option is selected by default.
Latency threshold	Specify the threshold in milliseconds for the latency of the Persistent Chat test. The default is 1000.
Event severity when latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Persistent Chat latency exceeds the threshold. The default is 10.
Collect data for latency	Select **Yes** to collect the data stream for the Persistent Chat latency.
Test Unified Contact Store Access	Select **Yes** to run the test for Unified Contact Store Access against your Lync Pool. **NOTE:** This test is not supported on Lync 2010.
Test failure event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Unified Contact Store Access test fails. The default is 5.
Unified Contact Store Access Latency	
Raise event if latency exceeds the threshold	Select **Yes** to raise an event when the latency of Unified Contact Store Access exceeds the threshold. This option is selected by default.
Latency threshold	Specify threshold in milliseconds for the latency of the Unified Contact Store Access test. The default is 1000.

Parameter	How to Set It
Event severity when Latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Unified Contact Store Access latency exceeds the threshold. The default is 10.
Collect data for latency	Select **Yes** to collect the data stream for the Unified Contact Store Access latency.
Test Mobile IM	Select **Yes** to run the test for Mobile IM against your Lync Pool. **NOTE:** This test is not supported for Lync 2010.
Sender's SIP address	Specify the Sender's SIP address in the following format: *SIP:username@domain.extension*. For example, *SIP:testuser@testdomain.com*
Receiver's SIP address	Specify the Receiver's SIP address in the following format: *SIP:username@domain.extension* For example, *SIP:testuser@testdomain.com*
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Mobile IM test fails. The default is 5.
Mobile IM Latency	
Raise event if the latency exceeds the threshold	Select **Yes** to raise an event when the latency of Mobile IM exceeds the threshold. This option is selected by default.
Latency threshold	Specify the threshold in milliseconds for the latency of the Mobile IM test. The default is 1000.
Event severity when latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Mobile IM latency exceeds the threshold. The default is 10.
Collect data for latency	Select **Yes** to collect the data stream for the Mobile IM latency.
Test XMPP IM	Select **Yes** to run the test for XMPP IM against your Lync Pool to determine that the instant message can be sent over Extensible Messaging and Presence Protocol gateway. **NOTE:** This test is not supported for Lync 2010.
Receiver's address	Specify the address of the receiver on which the test for XMPP IM is to be sent in the following format: *username@domain.extension*. For example, *testuser@testdomain.com*
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the XMPP IM test fails. The default is 5.
XMPP IM Latency	
Raise event if latency exceeds the threshold	Select **Yes** to raise an event when the latency of XMPP IM exceeds the threshold. This option is selected by default.
Latency threshold	Specify the threshold milliseconds for the latency of the XMPP IM test. The default is 1000.

Parameter	How to Set It
Event severity when latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the XMPP IM latency exceeds the threshold. The default is 10.
Collect data for latency	Select **Yes** to collect the data stream for the XMPP IM latency.

HealthCheck

Use this Knowledge Script to monitor the active status of Lync server services. You can run this script on a Front-end server, a Mediation server, or an Edge server to monitor the services on that server. This script raises an event if a service fails to start, stops and then starts again, or is disabled. This script generates a data stream for service availability.

Resource Object

Services Object

Default Schedule

The default interval for this script is one minute.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Services	
Start a service if it is stopped?	Select **Yes** if you want to start a stopped service. The default is Yes.
Data Collection	
Collect data for service availability?	Select **Yes** to collect data about service availability. The default is Yes.
Raise event if a service fails to start?	Select **Yes** to raise an event if the service fails to start. The default is Yes.
Event severity when service fails to start	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the service fails to start. The default is 5.
Raise event if a stopped service has been started?	Select **Yes** to raise an event if the service has been started. The default is Yes.

Description	How to Set It
Event severity when a stopped service has been started	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when a stopped service has been started again. The default is 25.
Raise event if service is disabled?	Select **Yes** to raise an event if the service is disabled. The default is unchecked.
Event severity when service is disabled	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the service is disabled. The default is 15.

MCUStatus

Use this Knowledge Script to monitor the health and draining state of a Multipoint Control Unit, or MCU. For example, IMMCU is an IM Conferencing server that runs as an IM service, and this script monitors the load for that server.

The different health states display the level of use as well as the number of users on the server.

Resource Object

MCUs

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor MCU Health State	
Raise event if health state is Loaded?	Select **Yes** to raise an event if the health state is Loaded. The default is unchecked.
Event severity when health state is Loaded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the health state is Loaded. The default is 20.
Raise event if health state is Full?	Select **Yes** to raise an event if the health state is Full. The default is Yes.
Event severity when health state is Full	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the health state is Full. The default is 15.
Monitor MCU Draining State	

Description	How to Set It
Raise event if draining state is Requesting to Drain?	Select **Yes** to raise an event if the draining state is Requesting to Drain, or attempting to close MCU services to reduce the load. The default is Yes.
Event severity when draining state is Requesting to Drain	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the draining state is Requesting to Drain. The default is 15.
Raise event if draining state is Draining?	Select **Yes** to raise an event if the draining state is set to Draining, the process of closing MCU services to reduce the load. The default is Yes.
Event severity when draining state is Draining	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the draining state is set to Draining. The default is 10.

MediationServerCallActivity

Use this Knowledge Script to monitor inbound and outbound calls of a Mediation server, an optional component that connects Lync to a phone system, such as a PSTN, POTS, PBX, or some other legacy system.

Resource Object

Mediation Server

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Inbound Calls	
Event Notification	
Raise event if number of inbound calls exceeds threshold?	Select **Yes** to raise an event if the number of inbound calls exceeds the threshold. The default is Yes.
Threshold - Maximum number of inbound calls	Specify the maximum number of inbound calls that can occur before an event is raised. The default is 25.

Description	How to Set It
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of inbound calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of current inbound calls?	Select **Yes** to collect data about the number of current inbound calls. The default is Yes.
Monitor Outbound Calls	
Event Notification	
Raise event if number of outbound calls exceeds threshold?	Select **Yes** to raise an event if the number of outbound calls exceeds the threshold. The default is Yes.
Threshold - Maximum number of outbound calls	Specify the maximum number of outbound calls that can occur 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 that is raised when the number of outbound calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of current outbound calls?	Select **Yes** to collect data about the number of current outbound calls. The default is Yes.
Monitor Rejected Inbound Calls	
Event Notification	
Raise event if number of rejected inbound calls exceeds threshold?	Select **Yes** to raise an event if the number of rejected inbound calls exceeds the threshold. Calls can be rejected if the Mediation server or the third-party gateway is over capacity. The default is Yes.
Threshold - Maximum number of rejected inbound calls	Specify the maximum number of rejected inbound calls that can occur 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 that is raised when the number of rejected inbound calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of rejected inbound calls?	Select **Yes** to collect data about the number of rejected inbound calls. The default is Yes.
Monitor Rejected Outbound Calls	
Event Notification	
Raise event if number of rejected outbound calls exceeds threshold?	Select **Yes** to raise an event if the number of rejected outbound calls exceeds the threshold. Calls can be rejected if the Mediation server or the third-party gateway is over capacity. The default is Yes.
Threshold - Maximum number of rejected outbound calls	Specify the maximum number of rejected outbound calls that can occur 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 that is raised when the number of rejected outbound calls exceeds the threshold. The default is 15.

Description	How to Set It
Data Collection	
Collect data for number of rejected outbound calls?	Select **Yes** to collect data about the number of current rejected outbound calls. The default is Yes.

MediationServerCallFailures

Use this Knowledge Script to monitor current call failure metrics of a Mediation server, an optional component that connects Lync to a phone system, such as a PSTN, POTS, PBX, or some other legacy system.

Resource Object

Mediation Server

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Call Failures	
Event Notification	
Raise event if number of call failures exceeds threshold?	Select **Yes** to raise an event if the number of call failures exceeds the threshold. The default is Yes.
Threshold - Maximum call failures	Specify the maximum number of calls that can fail before an event is raised. The default is 10 percent.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of call failures exceeds the threshold. The default is 10.
Data Collection	
Collect data for number of call failures?	Select **Yes** to collect data about the number of call failures. The default is Yes.

MediationServerHealth

Use this Knowledge Script to track the global health of a Mediation server, an optional component that connects Lync to a phone system, such as a PSTN, POTS, PBX, or some other legacy system. Health statuses include Disabled, Normal, Light Load, Heavy Load, and Overload. This script also monitors total packet drops and TCP disconnects because the received packet is out of sync.

Resource Object

Mediation Server

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Health State	
Raise event if global health status is Heavy Load?	Select **Yes** to raise an event if the global health status is heavy load. A health status of Heavy Load occurs when attempts to initiate new calls through the Mediation server fail. The default is Yes.
Event severity when global health status is Heavy Load	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of conferences exceeds the threshold. The default is 15.
Raise event if global health status is Overloaded?	Select **Yes** to raise an event if the global health status is Overloaded. The default is Yes.
Event severity when global health status is Overloaded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of conferences exceeds the threshold. The default is 10.
Monitor Dropped RTP Packets	
Event Notification	
Raise event if number of dropped RTP packets exceeds threshold?	Select **Yes** to raise an event if the number of dropped RTP packets exceeds the threshold. The default is Yes.
Threshold - Maximum dropped RTP packets	Specify the number of dropped RTP packets that can occur before an event is raised. The default is 5.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the threshold is exceeded. The default is 15.

Description	How to Set It
Data Collection	
Collect data for number of dropped RTP packets per second?	Select **Yes** to collect data about dropped RTP packets per second. The default is Yes.
Monitor TCP Disconnects	
Event Notification	
Raise event if number of TCP disconnects exceeds threshold?	Select **Yes** to raise an event if the number of TCP disconnects exceeds the threshold. The default is Yes.
Threshold - Maximum number of TCP disconnects	Specify the number of TCP disconnects that can occur before an event is raised. The default is 10.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the threshold is exceeded. The default is 15.
Data Collection	
Collect data for number of TCP disconnects?	Select **Yes** to collect data about number of TCP disconnects. The default is Yes.

MediationServerUsage

Use this Knowledge Script to monitor the overall resource usage of a Mediation server, an optional component that connects Lync to a phone system, such as a PSTN, POTS, PBX, or some other legacy system. Server usage data includes the number of overloaded conferences and the average time for processing audio packets.

Resource Object

Mediation Server

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Overloaded Conferences	

Description	How to Set It
Event Notification	
Raise event if the number of overloaded conferences exceeds threshold?	Select **Yes** to raise an event if the number of overloaded conferences exceeds the threshold. The default is Yes.
Threshold - Maximum overloaded conferences	Specify the maximum number of overloaded conferences that can occur before an event is raised. The default is 50.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of overloaded conferences exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of overloaded conferences?	Select **Yes** to collect data about the number of overloaded conferences. The default is Yes.
Monitor Average Audio Packet Processing Time	
Event Notification	
Raise event if the average processing time exceeds threshold?	Select **Yes** to raise an event if the average audio packet processing time exceeds the threshold. The default is Yes.
Threshold - Maximum average time	Specify the highest average processing time that can occur before an event is raised. The default is one second.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the average time exceeds the threshold. The default is 10.
Data Collection	
Collect data for average time to process audio packets?	Select **Yes** to collect data about the average processing time. The default is Yes.

SessionCallActivity

Use this Knowledge Script to monitor the session initiation rate of a Lync server. These sessions can include the following types: instant message (IM), file transfer, remote assistance, application sharing, audio, video, or telephony sessions.

This script gets session initiation data from the SessionDetails and Media Tables of the `LcsCDR` back-end database of the Lync Monitoring server. This script reports the number of sessions initiated per minute between two consecutive job iterations.

NOTE: In Lync, sessions have two users, and conferences contain three or more users.

Resource Object

Monitoring Server

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor IM Sessions	
Event Notification	
Raise event if number of IM sessions exceeds threshold?	Select **Yes** to raise an event if the number of IM sessions exceeds the threshold. The default is Yes.
Threshold - Maximum number of IM sessions	Specify the maximum number of IM sessions that can occur before an event is raised. The default is 25.
Event severity when number of IM sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of IM sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of IM sessions?	Select **Yes** to collect data about the number of IM sessions. The default is unchecked.
Monitor File Transfer Sessions	
Event Notification	
Raise event if number of file transfer sessions exceeds threshold?	Select **Yes** to raise an event if the number of file transfer sessions exceeds the threshold. The default is Yes.
Threshold - Maximum number of file transfer sessions	Specify the maximum number of file transfer sessions that can occur before an event is raised. The default is 25.
Event severity when number of file transfer sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of file transfer sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of file transfer sessions?	Select **Yes** to collect data about the number of file transfer sessions. The default is unchecked.
Monitor Remote Assistance Sessions	
Event Notification	
Raise event if number of remote assistance sessions exceeds threshold?	Select **Yes** to raise an event if the number of remote assistance sessions exceeds the threshold. The default is Yes.

Description	How to Set It
Threshold - Maximum number of remote assistance sessions	Specify the maximum number of remote assistance sessions that can occur before an event is raised. The default is 25.
Event severity when number of remote assistance sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of remote assistance sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of remote assistance sessions?	Select **Yes** to collect data about the number of remote assistance sessions. The default is Yes.
Monitor Application Sharing Sessions	
Event Notification	
Raise event if number of application sharing sessions exceeds threshold?	Select **Yes** to raise an event if the number of application sharing sessions exceeds the threshold. The default is Yes.
Threshold - Maximum number of application sharing sessions	Specify the maximum number of application sharing sessions that can occur before an event is raised. The default is 25.
Event severity when number of application sharing sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of application sharing sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of application sharing sessions?	Select **Yes** to collect data about the number of application sharing sessions. The default is unchecked.
Monitor Audio Sessions	
Event Notification	
Raise event if number of audio sessions exceeds threshold?	Select **Yes** to raise an event if the number of audio sessions exceeds the threshold. The default is Yes.
Threshold - Maximum number of audio sessions	Specify the maximum number of audio sessions that can occur before an event is raised. The default is 25.
Event severity when number of audio sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of audio sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of audio sessions?	Select **Yes** to collect data about the number of audio sessions. The default is unchecked.
Monitor Video Sessions	
Event Notification	
Raise event if number of video sessions exceeds threshold?	Select **Yes** to raise an event if the number of video sessions exceeds the threshold. The default is Yes.
Threshold - Maximum number of video sessions	Specify the maximum number of video sessions that can occur before an event is raised. The default is 25.

Description	How to Set It
Event severity when number of video sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of video sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of video sessions?	Select **Yes** to collect data about the number of video sessions. The default is Yes.
Monitor Telephony Sessions	
Event Notification	
Raise event if number of telephony sessions exceeds threshold?	Select **Yes** to raise an event if the number of telephony sessions exceeds the threshold. The default is Yes.
Threshold - Maximum telephony sessions	Specify the maximum number of telephony sessions that can occur before an event is raised. The default is 15.
Event severity when number of telephony sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of telephony sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of telephony sessions?	Select **Yes** to collect data about the number of telephony sessions. The default is Yes.
Monitor Meeting Sessions	
Event Notification	
Raise event if number of meeting sessions exceeds threshold?	Select **Yes** to raise an event if the number of meeting sessions exceeds the threshold. The default is Yes.
Threshold - Maximum number of meeting sessions	Specify the maximum number of meeting sessions that can occur before an event is raised. The default is 15.
Event severity when number of meeting sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of meeting sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of meeting sessions?	Select **Yes** to collect data about the number of meeting sessions. The default is Yes.

SessionCallFailures

Use this Knowledge Script to monitor the session failure metrics of a Lync server. This script queries the Call Detail Record server to find any known session failures. These sessions can include the following types: instant message (IM), file transfer, remote assistance, application sharing, audio, video, or telephony sessions.

NOTE: In Lync, sessions have two users, and conferences contain three or more users.

This script calculates failed sessions from the SessionDetails and Media Tables of the `LcsCDR` back-end database of the Lync Monitoring server. This script reports the number of session failures per minute between two consecutive job iterations.

The SessionCallFailures script considers sessions with the following SIP Status codes as failed:

400, 401, 402, 403, 405, 406, 407, 408, 410, 413, 414, 415, 416, 420, 421, 423, 481, 482, 483, 485, 488, 493, 500, 501, 502, 503, 504, 505, 513, 600, 606

For more information about SIP status codes, see http://tools.ietf.org/html/rfc3261#page-182.

Resource Object

Monitoring Server

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Session Failures	
Event Notification	
Raise event if number of session failures exceeds threshold?	Select **Yes** to raise an event if the number of session failures exceeds the threshold. The default is Yes.
Threshold - Maximum session failures	Specify the maximum number of session failures that can occur before an event is raised. The default is 5.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of session failures exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of session failures?	Select **Yes** to collect data about the number of session failures. The default is unchecked.

SetupSupplementalDB

Use this Knowledge Script to create a Lync supplemental database, including the tables and stored procedures needed to store call quality detail records (CDRs). In addition, this script creates a SQL Server job that removes old records from the supplemental database.

You can also create the Lync supplemental database using the *Set up supplemental database?* parameter in the Discovery_Lync Knowledge Script.

For more information, see "Discovering Lync Resources" on page 23.

Resource Object

Monitoring Server

Default Schedule

The default interval for this script is three hours.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the SetupSupplementalDB job fails. The default is 5.
Raise event if database setup fails?	Select **Yes** to raise an event if creation of the Lync supplemental database fails. The default is unselected.
Event severity when database setup fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Lync supplemental database is not created. The default is 15. It is possible that the supplemental database was not created because of one of the following reasons: ◆ The Discovery job was run with the *Set up supplemental database* parameter selected on a computer other than a front-end pool server ◆ The Discovery job was run on a computer with the *Set up supplemental database* parameter selected on which SQL Server is not installed ◆ The Discovery job was run on a computer with the *Set up supplemental database* parameter selected where Lync supplemental database was already created
Raise event if database setup succeeds?	Select **Yes** to raise an event if creation of the Lync supplemental database is successful. The default is unselected.

Description	How to Set It
Event severity when database setup succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Lync supplemental database is created successfully. The default is 25.
Start pruning job on supplemental database?	Select **Yes** to create a SQL job that deletes data from the supplemental database. The SQL job runs every night. The default is Yes. Data is deleted from the supplemental database based on the value you specify in the *Number of days to keep call detail records* parameter.
Number of days to keep call detail records	Specify the number of days' days' worth of call detail records to keep in the Lync supplemental database. Data older than what you specify is discarded. The default is 7 days. You can specify a maximum of 30 days.
SQL Server Information	
SQL Server \instance name	Specify the SQL Server name where you want to create the new Lync Server supplemental database along with the instance if any. If you specify both the SQL Server instance name for this parameter and the SQL Server database user name in the following parameter, these values must match the values you specified in "Configuring Security Manager Settings for the Supplemental Database" on page 22. If this field is left blank, then the script uses the default SQL server on the agent computer to create the supplemental database in the Lync agent where you run the discovery or the Lync_SetupSupplementalDB script. If the SQL database is not present on the Lync agent, then the script fails to create the database. If you do not specify the instance name, the script creates the database in the default instance.
SQL database user name	Specify the user name for the SQL Server where you want to create the new Lync Server supplemental database. Leave this parameter blank to use Windows authentication instead of SQL authentication.

SyntheticTransaction

Use this Knowledge Script to monitor the health of the Lync deployment. Each Lync synthetic transaction test is executed on the Lync Front End pool. Lync_SyntheticTransaction reports the test result and latency of the Lync synthetic transaction test, which helps in predicting the end user experience.

Before running this Knowledge Script, you need to set up and configure Lync Trusted Application Server. For more information about configuring a trusted application server, see "Setting Up Lync Trusted Application Server" on page 21.

To run this Knowledge Script, you should first discover the Lync trusted application server and every Lync FrontEnd pool within the server.

Resource Objects

Front End Pool

Default Schedule

The default interval for this script is 1 hour.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the SyntheticTransaction job fails. The default is 5.
Lync Test	
Test Instant Messaging	Select **Yes** to run the test for Instant Messaging against the Lync FrontEnd Pool.
Test failure event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Instant Messaging test fails. The default is 5.
Instant Messaging Latency	
Raise event when latency exceeds the threshold	Select **Yes** to raise an event when the latency of Instant Messaging exceeds the threshold. This option is selected by default.
Latency threshold	Specify the threshold in milliseconds for the latency of Instant Messaging. The default is 1000.
Event severity when latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the latency of Instant Messaging exceeds the threshold. The default is 10.
Collect data for latency	Select **Yes** to collect the data stream for Instant Messaging latency.
Test Group Instant Messaging	Select **Yes** to run the test for Group Instant Messaging against your Lync Pool.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the test for Group Instant Messaging fails. The default is 5.
Group Instant Messaging Latency	
Raise event if latency exceeds the threshold	Select **Yes** to raise an event when the latency of Group Instant Messaging exceeds the threshold. This option is selected by default.
Latency threshold	Specify the threshold in milliseconds for the latency of Group Instant Messaging test. The default is 1000.

Description	How to Set It
Event severity when latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Group Instant Messaging latency exceeds the threshold. The default is 10.
Collect data for latency	Select **Yes** to collect the data stream for the latency of Group Instant Messaging.
Test Peer-To-Peer Audio/ Video	Select **Yes** to run the test for Peer-To-Peer Audio/Video against your Lync Pool.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Peer-To-Peer Audio/Video test fails. The default is 5.
Peer-To-Peer Audio/Video Latency	
Raise event if latency exceeds the threshold	Select **Yes** to raise an event when the Peer-To-Peer Audio/Video latency exceeds the threshold. This option is selected by default.
Latency threshold	Specify the threshold in milliseconds for the latency of Peer-To-Peer Audio/ Video test. The default is 1000.
Event severity when latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Peer-To-Peer Audio/Video latency exceeds the threshold. The default is 10.
Collect data for latency	Select this option to collect the data stream for the latency of Peer-To-Peer Audio/Video.
Test Audio Video Conference	Select **Yes** to run the test for Audio/Video Conference against your Lync Pool.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Audio Video Conference test fails. The default is 5.
Audio/Video Conference Latency	
Raise event if latency exceeds the threshold	Select **Yes** to raise an event when the latency of audio/video conference call exceeds the threshold. This option is selected by default.
Latency threshold	Specify the threshold in milliseconds for the latency of the Audio/Video Conference test. The default is 1000.
Event severity when latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when latency of audio/video conference call exceeds the threshold.
Collect data for latency	Select **Yes** to collect the data stream for the latency of audio/video conference call.
Test Presence	Select **Yes** to run the test for Presence against your Lync Pool.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the test for Presence fails. The default is 5.
Presence Latency	
Raise event if latency exceeds the threshold	Select **Yes** to raise an event when the latency of Presence exceeds the threshold. This option is selected by default.

Description	How to Set It
Latency threshold	Specify threshold in milliseconds for the latency of Presence test. The default is 1000.
Event severity when latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Presence latency exceeds the threshold. The default is 10.
Collect data for latency	Select **Yes** to collect the data stream for the Presence latency.
Test Registration	Select **Yes** to run the test for Registration against your Lync Pool.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Registration test fails. The default is 5.
Registration Latency	
Raise event if latency exceeds the threshold	Select **Yes** to raise an event when the latency of Registration exceeds the threshold. This option is selected by default
Latency threshold	Specify the threshold in milliseconds for the latency of Registration test. The default is 1000.
Event severity when latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the latency of Registration exceeds the threshold. The default is 10.
Collect data for latency	Select **Yes** to collect the data stream for the Registration latency.
Test Address Book Service	Select **Yes** to run the test for the Address Book service against your Lync Pool.
Test failure event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the test for Address Book service fails. The default is 5.
Address Book Service Latency	
Raise event if latency exceeds the threshold	Select **Yes** to raise an event when the latency of Address Book service exceeds the threshold. This option is selected by default.
Latency threshold	Specify the threshold in milliseconds for the latency of the Address Book Service test. The default is 1000.
Event severity when latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the latency of Address Book service exceeds the threshold. The default is 10.
Collect data for latency	Select **Yes** to collect the data stream for the latency of the Address Book service.
Test Address Book Web Query	Select **Yes** to run the test for Address Book Web Query against your Lync Pool.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the Address Book Web Query test fails. The default is 5.
Address Book Web Query Latency	
Raise event if latency exceeds the threshold	Select **Yes** to raise an event when the latency of Address Book Web Query exceeds the threshold. This option is selected by default.

Description	How to Set It
Latency threshold	Specify threshold in milliseconds for the latency of Address Book Web Query test. The default is 1000.
Event severity when latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the latency of Address Book Web Query exceeds the threshold. The default is 10.
Collect data for latency	Select **Yes** to collect the data stream for the latency of Address Book Web Query.

SystemUptime

Use this Knowledge Script to monitor the length of time a server has been up and running since a reboot. This script generates a data stream for system uptime (hours) and raises an event if the Lync server is rebooted.

Resource Object

Lync Servers

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Raise event if system reboot detected?	Select **Yes** to raise an event if the system has rebooted. The default is Yes.
Event severity when system reboot detected	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the system has rebooted. The default is 10.
Monitor System Uptime	
Data Collection	
Collect data for system uptime?	Select **Yes** to collect data about system uptime, in hours. The default is Yes.

SystemUsage

Use this Knowledge Script to monitor the total CPU and memory usage of a Lync server, and to monitor the contributions of each Lync service to this usage. This script generates data streams for total CPU and memory usage for a Lync server (%) and for total CPU and memory usage by a service (%). It raises an event if a threshold set for these values is exceeded.

Resource Object

Services

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Service CPU Usage	
Event Notification	
Raise event if total CPU usage for a service exceeds threshold?	Select **Yes** to raise an event if the percentage of total CPU usage for the service exceeds the threshold. The default is Yes.
Threshold - Maximum service CPU usage	Specify the maximum percentage of the CPU that can be used by the service before an event is raised. The default is 65%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the maximum CPU usage for the service exceeds the threshold. The default is 15.
Data Collection	
Collect data for service CPU usage?	Select **Yes** to collect data about CPU usage for the service. The default is Yes.
Monitor Total CPU Usage	
Event Notification	
Raise event if total CPU usage exceeds threshold?	Select **Yes** to raise an event if the percentage of total CPU usage exceeds the threshold. The default is unchecked.
Threshold - Maximum total CPU usage	Specify the maximum percentage of the total CPU that can be used before an event is raised. The default is 80%.

Description	How to Set It
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the maximum CPU usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for total CPU usage?	Select **Yes** to collect data about total CPU usage. The default is unchecked.
Monitor Service Memory Usage	
Event Notification	
Raise event if total memory usage by a service exceeds threshold?	Select **Yes** to raise an event if the percentage of total memory usage by the service exceeds the threshold. The default is Yes.
Threshold - Maximum service memory usage	Specify the maximum percentage of memory used by the service that can be used before an event is raised. The default is 65%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the maximum memory used by a the service exceeds the threshold. The default is 15.
Data Collection	
Collect data for service memory usage?	Select **Yes** to collect data about total memory usage for the service. The default is Yes.
Monitor Total Memory Usage	
Event Notification	
Raise event if total memory usage exceeds threshold?	Select **Yes** to raise an event if the percentage of total memory usage exceeds the threshold. The default is Yes.
Threshold - Maximum total memory usage	Specify the maximum percentage of the total memory that can be used before an event is raised. The default is 80%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the maximum total memory usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for total memory usage?	Select **Yes** to collect data about total memory usage. The default is Yes.