Management Guide

NetIQ® AppManager® for Microsoft Exchange Server and Exchange Online

June 2019

Legal Notice

Contents

About this Book and the Library **5**
About NetIQ Corporation **7**

1 Introducing AppManager for Microsoft Exchange Server and Exchange Online **9**

1.1 Understanding Microsoft Exchange Server . . . 9
1.2 Understanding Microsoft Exchange Online . . . 10
1.3 How AppManager Can Help . . . 10

2 Installing and Configuring AppManager for Microsoft Exchange Server and Exchange Online **13**

2.1 System Requirements . . . 13
2.2 Installing the Module . . . 15
2.3 Deploying the Module with Control Center . . . 18
2.4 Silently Installing the Module . . . 18
2.5 Permissions for Discovering Exchange Server Resources . . . 19
2.6 Discovering Exchange Server Resources . . . 21
2.7 Configuring Security Manager to run Exchange Online Discovery . . . 22
2.8 Permissions for Discovering Exchange Online . . . 22
2.9 Discovering Exchange Online . . . 22
2.10 Configuring and Monitoring Database Availability Groups . . . 23
2.11 Configuring and Monitoring Clusters . . . 25
2.12 Upgrading Knowledge Script Jobs . . . 28
2.13 Configuring the PowerShell Execution Policy . . . 29
2.14 Changing Configuration Settings . . . 33
2.15 Troubleshooting PowerShell Errors . . . 34

3 Reporting with Analysis Center **37**

3.1 System Requirements for Analysis Center Reports . . . 37
3.2 Installing the Report Package . . . 37
3.3 Exchange Server 2007 or later Analysis Center Report Templates . . . 38

4 Exchange 2007 Knowledge Scripts **41**

4.1 All_BestPracticesAnalyzer . . . 43
4.2 All_ClockSynchronization . . . 46
4.3 All_EventLog . . . 47
4.4 All_ServiceStatus . . . 48
4.5 Availability . . . 50
4.6 BestPracticesAnalyzer . . . 53
4.7 CAS_Activity . . . 55
4.8 CAS_Connectivity . . . 63
4.9 CAS_OABAvailability . . . 67
4.10 CAS_PublicFolderAvailability . . . 68
4.11 DataCollection . . . 70
4.12 ETS_ExternalMail . . . 75

4.13 ETS_MessageHygiene . . . 78
4.14 Health . . . 80
4.15 HTS_Connectivity . . . 92
4.16 HTS_SafetyNet . . . 94
4.17 HTS_SendersAndRecipients . . . 95
4.18 HTS_TransportDumpster . . . 98
4.19 MBS_ClientActivity . . . 99
4.20 MBS_ClientConnectivity . . . 106
4.21 MBS_ClusterOwner . . . 109
4.22 MBS_DatabaseStateChange . . . 110
4.23 MBS_DatabaseStatus . . . 113
4.24 MBS_MailboxAccessibility . . . 117
4.25 MBS_MailboxUsage . . . 119
4.26 MBS_MailFlow . . . 121
4.27 MBS_MessagingRecordsMgmt . . . 122
4.28 MBS_PublicFolderUsage . . . 126
4.29 MBS_Replication . . . 128
4.30 Report_CopyQueueLength . . . 131
4.31 Report_DiskUsageStatus . . . 133
4.32 Report_DataLostInReplication . . . 135
4.33 Report_FileShareWitnessUsage . . . 137
4.34 Report_ReplayQueueLength . . . 140
4.35 Report_TransDumpUsage . . . 142
4.36 Transport_BackPressure . . . 144
4.37 Transport_ConnectorStatus . . . 145
4.38 Transport_QueueStatus . . . 147
4.39 UMS_CallActivity . . . 151
4.40 UMS_Connectivity . . . 154
4.41 UMS_Failures . . . 156
4.42 UMS_Performance . . . 159
4.43 Recommended Knowledge Script Group . . . 162

5 Exchange Online Knowledge Scripts 167

5.1 Specifying Inclusion or Exclusion Filters . . . 167
5.2 Using the Regular Expression Filters . . . 168
5.3 MailBoxQuota . . . 170
5.4 ServiceHealth . . . 174

6 Troubleshooting AppManager for Microsoft Exchange Server and Exchange Online 177

6.1 ExchangeOnline_MailboxQuota job throws an error after running for a longer duration . . . 177
6.2 MCPSHostServer.exe consuming too much CPU . . . 177

About this Book and the Library

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

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

Intended Audience

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

Other Information in the Library

The library provides the following information resources:

Installation Guide for AppManager

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

User Guide for AppManager Control Center

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

Administrator Guide for AppManager

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

Upgrade and Migration Guide for AppManager

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

Management guides

Provide information about installing and monitoring specific applications with AppManager.

Help

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

The AppManager library is available in Adobe Acrobat (PDF) format from the 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 http://community.netiq.com.

1 Introducing AppManager for Microsoft Exchange Server and Exchange Online

AppManager for Microsoft Exchange Server and Exchange Online lets you monitor the operation, performance, and availability of Microsoft Exchange Server and Exchange Online.

1.1 Understanding Microsoft Exchange Server

Previous versions of Microsoft Exchange employed traditional communication methods whereby email, voice mail, and fax traffic not only traveled different paths through communication networks (frequently requiring separate sites and servers), but were accessible only by different tools such as telephones, computers, and fax machines.

With Exchange Server, users receive e-mail, voice mail, fax messages, and calendar data directly into one inbox, and can access the inbox from a variety of applications, such as Microsoft Office Outlook, Outlook Web Access, mobile devices, or the telephone. This unified messaging system simplifies the user experience and reduces the number of servers required to provide e-mail, voice mail, and fax services.

Server roles provide flexibility in deploying Exchange Server. There are five server roles in Exchange Server:

- **Hub Transport** server role moves messages between the other server roles and applies compliance policies to messages while they are in transit.
- **Client Access** server role enables users to access their inbox from Outlook Web Access, POP3, IMAP 4, Outlook Anywhere, and Exchange Server ActiveSync.
- **Edge Transport** server role provides antivirus and anti-spam protection for your Exchange organization.
- **Mailbox** server role holds users' mailbox databases, which contain e-mail, calendar, contact, task, voice mail, and fax data.
- **Unified Messaging** server role lets users receive voice mail, e-mail, fax messages, and calendar data in their Exchange inboxes. It also enables voice access to the inbox from any telephone, and hosts any speech-enabled Automated Attendant that your organization may employ.

With the exception of the Edge Transport server role, which must be deployed on a server in the perimeter network, all other roles can run on one server or multiple servers, depending on the needs and size of your organization.

NOTE:

- Exchange Server 2007 and 2010 have five server roles as describe above: Hub Transport, Client Access, Edge Transport, Mailbox, and Unified Messaging.
- Exchange Server 2013 has only three server roles: Mailbox, Client Access, and Edge Transport. The Mailbox role includes Transport service, Mailbox databases, and Unified Messaging. The Client Access role provides authentication, limited redirection, and proxy services. The Edge Transport Server role provides improved anti-spam protection for your Exchange organization. It

also applies policies to messages in transport between the organization. AppManager for Microsoft Exchange Server and Exchange Online discovers the Hub Transport and Unified Messaging roles under Mailbox role for Exchange Server 2013.

- Exchange Server 2016 has two server roles: Mailbox and Edge Transport. The Mailbox role includes Transport service, Mailbox databases, Client Access service, and Unified Messaging. The Edge Transport role provides anti-spam and mail flow rules as mails enters and leaves your Exchange organization. AppManager for Microsoft Exchange Server and Exchange Online discovers the Mailbox databases and the Hub Transport, Client Access, and Unified Messaging services under Mailbox server for Exchange Server 2016.
- Exchange Server 2019 has two server roles: Mailbox and Edge Transport. The Mailbox role includes Transport service, Mailbox databases, and Client Access service. The Edge Transport role provides anti-spam and mail flow rules as mails enters and leaves your Exchange organization. AppManager for Microsoft Exchange Server and Exchange Online discovers the Mailbox databases, Hub Transport, and Client Access under Mailbox server for Exchange Server 2019.

1.2 Understanding Microsoft Exchange Online

Exchange Online is the hosted version of Microsoft ‘s messaging platform, Exchange Server. It includes access to emails, calenders, contacts, and tasks for any endpoint device. Because of its hosted nature; services are accessed across the wide area network (WAN) and there are no Exchange Server software packages to deploy and configure. Physical servers are not required for support.

1.3 How AppManager Can Help

AppManager for Microsoft Exchange Server and Exchange Online monitors Exchange Server resources installed in both *clustered* and *non-clustered* environments, DAG environments, and Exchange Online. The module supports the following environments:

- **Cluster continuous replication** (CCR) combines the replication and replay features in Exchange Server 2007 with the failover features of Microsoft Cluster services. CCR is a solution that can be deployed with no single point of failure in a single data center or between two data centers.
- **Single copy clusters** (SCC), known as shared storage clusters in previous versions of Exchange Server, are present in Exchange Server 2007. They are not present in versions later than Exchange Server 2007.
- **Local continuous replication** (LCR) is a single-server solution that uses creates and maintains a copy of a storage group on a second set of disks that are connected to the same server as the production storage group. LCR provides asynchronous log shipping, log replay, and a quick manual switch to a copy of the data.
- **Database availability group** (DAG) is a set of up to 16 Microsoft Exchange Server 2010, 2013, 2016, or 2019 Mailbox servers that provides automatic database-level recovery from a database, server, or network failure. DAG replaces CCR, SCC, and LCR on Exchange 2010, 2013, 2016, and 2019 servers. For more information, see Section 2.10, “Configuring and Monitoring Database Availability Groups,” on page 23.
- **Exchange Online** is the hosted version of Microsoft ‘s messaging platform, Exchange Server.

The Exchange2007 Knowledge Scripts raise events in the AppManager Operator Console or Control Center. The scripts collect information about server roles that you can use for trend analysis and reporting.

The Exchange Online Knowledge Scripts raise events in the AppManager Operator Console or Control Center. The scripts collect information about the mailbox quota and service health of Exchange Online domains (tenants).

With AppManager for Microsoft Exchange Server and Exchange Online, you can monitor the following:

- The Windows Event Log for warnings and errors whose source is either the Best Practices Analyzer or Exchange services
- Running status of all Exchange Server services
- Clock synchronization
- Response time for ActiveSync, Outlook Web Access, Outlook Web services, and the Autodiscovery service
- Number of messages in queue and change in queue size
- Status of send, receive, foreign, and delivery agent connectors
- Speed of mail flow to a specified e-mail address or Mailbox server
- Availability of offline address books and public folders
- Accessibility of mailbox database
- Communication between Hub Transport server and Mailbox server
- Synchronization between Hub Transport server and Edge Transport server
- Response to SMTP requests
- Replication health
- Mailbox database status
- Available disk space
- Cluster ownership
- Message management: deleting, journaling, moving
- Performance for the Unified Messaging server, including user response latency, operation response time, queued messages, queued OCS user notifications, and disconnected calls, and access to the Mailbox server, Hub Transport server, and Active Directory
- Exchange Online mailbox quota
- Office 365 service health

2 Installing and Configuring AppManager for Microsoft Exchange Server and Exchange Online

This chapter provides installation instructions and describes system requirements for AppManager for Microsoft Exchange Server and Exchange Online.

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

2.1 System Requirements

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

Software/Hardware	Version
NetIQ AppManager installed on the AppManager repository (QDB) computers, on the Exchange computers you want to monitor (agents), and on all console computers	8.0.3, 8.2, 9.1, 9.2, 9.5, 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, 9.2, 9.5, or later **NOTE:** ◆ Support for Windows Server 2008 on AppManager 7.x requires AppManager Windows Agent hotfix 71704 or later. ◆ Enhanced data collection on AppManager 7.x requires AppManager QDB hotfix 72040 or later. ◆ Enhanced Control Center performance and auto-deployment on AppManager 7.x requires AppManager Control Center hotfix 71647 or later. For more information about these hotfixes, see the AppManager Suite Hotfixes page.

Software/Hardware	Version
Microsoft Windows operating system on the agent computers	One of the following: ◆ Windows Server 2019 ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (64-bit) ◆ Windows Server 2003 R2 (64-bit)
Microsoft Exchange Server on the agent computers	One of the following: ◆ Exchange Server 2019 ◆ Exchange Server 2016 ◆ Exchange Server 2013 ◆ Exchange Server 2010 ◆ Exchange Server 2007
AppManager for Microsoft Windows module installed on the AppManager repository (QDB) computer, on the Exchange Server computers you want to monitor (agents), and on all console computers	Support for Windows Server 2008 R2 on AppManager 7.x requires the AppManager for Windows module, version 7.6.170.0 or later. For more information, see the AppManager Module Upgrades & Trials page.
Microsoft Exchange Server Role installed on the agent computers	At least one of the following Exchange Server roles installed: ◆ Client Access Role ◆ Edge Transport Role ◆ Hub Transport Role ◆ Mailbox Role ◆ Unified Messaging Role
Microsoft .NET Framework installed on the agent computers	3.0 and 3.5
Windows PowerShell Engine	2.0 for Exchange Server 2007 and 2010 3.0 or later for Exchange Server 2013 and 2016 **NOTE:** For Windows 2012 make sure that PowerShell 2.0 engine feature is installed. If this component is not installed the discovery process fails.
Microsoft SQL Server Native Client 11.0 **(for TLS 1.2 support)**	11.3.6538.0 or later **NOTE:** The SQL Server Native client can be installed from this Microsoft download link.

AppManager for Exchange Online has the following system requirements:

Item	Requirement
NetIQ AppManager installed on the AppManager repository (QDB) computers, on the Exchange computers you want to monitor (AppManager agents), and on all console computers	8.0.3, 8.2, 9.1, 9.2, 9.5, 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, 9.2, 9.5, or later
Microsoft Windows operating system installed on agent computers	One of the following: ◆ Windows Server 2019 ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012
AppManager for Microsoft Windows installed on the agent computers	8.0.104.0 or later
Windows Azure Active Directory Module for Windows Powershell (64-bit) installed on the agent computers	1.0.9031.1 or later
Microsoft .NET Framework installed on the agent computers	3.5 and 4.0 or later
Windows PowerShell Engine	3.0 or later
Microsoft SQL Server Native Client 11.0 **(for TLS 1.2 support)**	11.3.6538.0 or later **NOTE:** The SQL Server Native client can be installed from this Microsoft download link.

NOTE: If you want TLS 1.2 support and are running AppManager 9.1 or 9.2, then you are required to perform some additional steps. To know about the steps, see the article.

2.2 Installing the Module

Run the module installer on the Exchange servers 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-Exchange2007-7.x.x.0.msi` module installer from the `AM70-Exchange2007-7.x.x.0` self-extracting installation package on the AppManager Module Upgrades & Trials page.

If you are upgrading from the previous version of this module, version 7.5, you need to perform additional steps to install version 7.6 correctly. For more information, see Section 2.2.2, “Upgrading the Module,” on page 17.

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 `.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 `.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 and the Analysis Center reports 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.

2.2.1 Manually Installing the Module

You can install the module manually, or you can use Control Center to deploy the module on a remote computer where an agent is installed. For more information, see Section 2.3, “Deploying the Module with Control Center,” on page 18. 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 and to install the Analysis Center reports into the Analysis Center Configuration Database:
   - **4a** Select **Install Knowledge Scripts** to install the repository components.
   - **4b** Select **Install report package** to install the Analysis Center reports.
   - **4c** Specify the SQL Server name of the server hosting the QDB, as well as the case-sensitive QDB name.
   - **4d** Specify the SQL Server name of the server hosting the Analysis Center Configuration Database.
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, and 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 Exchange computers you want to monitor (agents) to install the agent components.

9 Configure the PowerShell Execution policy, and, if necessary, establish a trust relationship between NetIQ Corporation and the user accounts that will run the Exchange2007 category of Knowledge Scripts. For more information, see Section 2.13, “Configuring the PowerShell Execution Policy,” on page 29.

10 Ensure proper permissions and memberships are set before discovering Exchange Server resources. For more information, see Section 2.5, “Permissions for Discovering Exchange Server Resources,” on page 19.

11 (Conditional) If you have not discovered Exchange resources, run the Discovery_Exchange2007 Knowledge Script on all agent computers where you installed the module. For more information, see Section 2.6, “Discovering Exchange Server Resources,” on page 21.

12 To get the updates provided in this release, upgrade any running Knowledge Script jobs. For more information, see Section 2.12, “Upgrading Knowledge Script Jobs,” on page 28.

After the installation has completed, the `Exchange2007_Install.log` and `PowerShellHost_Install.log` files, located in the `\NetIQ\Temp\NetIQ_Debug\`<*ServerName*> folder, lists any problems that occurred.

2.2.2 Upgrading the Module

If you are upgrading from a previous release to this version, 7.6.0.1, install the version 7.6.0.1 on each Exchange Server agent, AppManager repository (QDB), and console.

AppManager for Microsoft Exchange Server and Exchange Online uses PowerShell scripts throughout the module, so you must set the PowerShell execution policy. For more information, see Section 2.13, “Configuring the PowerShell Execution Policy,” on page 29.

To upgrade from a previous version to version 7.6.0.1:

1 Stop the ad hoc jobs of the previous version and remove all Exchange Server and Exchange Online monitoring policies.

2 (Conditional) If you have Exchange Online objects discovered in TreeView, then delete all the Exchange Online objects from the TreeView.

3 Install version 7.6.0.1 of the module on all AppManager repositories (QDBs), consoles, and agents. For more information about running the installer, see Section 2.2, “Installing the Module,” on page 15.

4 The module installer automatically runs the Discovery Knowledge Script. If it does not, manually run Discovery_Exchange2007. For more information about the Discovery Knowledge Script, see Section 2.6, “Discovering Exchange Server Resources,” on page 21.

5 (Conditional) Run the Discovery_ExchangeOnline Knowledge Script to discover the Exchange Online objects. For more information about Discovery_ExchangeOnline Knowledge Script, see Section 2.9, “Discovering Exchange Online,” on page 22.

6 Recreate the ad hoc jobs and create new Exchange Server and Exchange Online monitoring policies.

2.3 Deploying the Module with Control Center

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

2.3.1 Deployment Overview

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

To deploy the module on an agent computer:

1. Verify the default deployment credentials.
2. Check in an installation package. For more information, see Section 2.3.2, “Checking In the Installation Package,” on page 18.
3. Configure an email address to receive notification of a deployment.
4. Create a deployment rule or modify an out-of-the-box deployment rule.
5. Approve the deployment task.
6. View the results.

2.3.2 Checking In the Installation Package

You must check in the installation package, `AM70-Exchange2007-7.x.x.0.xml`, before you can deploy the module on an agent computer.

To check in a module installation package:

1. Log on to Control Center 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-Exchange2007-7.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 Section 2.12, “Upgrading Knowledge Script Jobs,” on page 28.

2.4 Silently Installing the Module

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

```
msiexec.exe /i "AM70-Exchange2007-7.x.x.0.msi" /qn
```

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

To get the updates provided in this release, upgrade any running Knowledge Script jobs. For more information, see Section 2.12, “Upgrading Knowledge Script Jobs,” on page 28.

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

```
/L* "AM70-Exchange2007-7.x.x.0.msi.log"
```

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

NOTE: To perform a silent install on an AppManager agent running Windows 2008 R2, 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-Exchange2007-7.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-Exchange2007-7.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
```

2.5 Permissions for Discovering Exchange Server Resources

Before discovering and monitoring Exchange Server resources, ensure that the user account running the AppManager agent service (netiqmc) has the following memberships and permissions:

- Membership in the Exchange View-Only Administrators group (for Exchange Server 2007)
- Membership in View-Only Organization Management group (for Exchange Server 2010 or later)
- Membership in the Local Administrators group on the Exchange Server
- Permission to access the File Share Witness folder

In addition to the minimum permissions required for any role, following are the specific Exchange Server roles that require additional permissions:

Component	Required Permissions and Memberships for Exchange Server 2007	Required Permissions and Memberships for Exchange Server 2010 or later
Client Access Server role	◆ Membership in the Exchange Server Administrators group	◆ Membership in Server Management group ◆ Membership in the Organization Management group
Edge Transport Server role	◆ Membership in the Exchange Server Administrators group	◆ Membership in Server Management group

Component	Required Permissions and Memberships for Exchange Server 2007	Required Permissions and Memberships for Exchange Server 2010 or later
Hub Transport Server role	◆ Membership in the Exchange Organization Administrators group ◆ Membership in the `Builtin\Administrators` group on the Active Directory server	◆ Membership in the Organization Management Group ◆ Membership in the `Builtin\Administrators` group on the Active Directory server
Mailbox Server role	◆ Membership in the Exchange Server Administrators group ◆ Membership in the Exchange Recipient Administrators group	◆ Membership in Server Management group ◆ Membership in Recipient Management group ◆ Membership in the Organization Management group
Unified Messaging Server role	◆ Membership in the Exchange Server Administrators group, for support for the UMS_Connectivity Knowledge Script	◆ Membership in Server Management group, for support for the UMS_Connectivity Knowledge Script
Exchange Best Practices Analyzer tool (for all Exchange Server roles)	◆ Designation as the Domain Administrator, or membership in the `Builtin\Administrators` group on the Active Directory server, for enumerating the Active Directory information and calling the Microsoft Windows Management Instrumentation (WMI) providers on the domain controller and global catalog servers. ◆ Membership in the Local Administrators group on each Exchange server for calling the WMI providers and accessing the registry and the metabase ◆ Delegation for at least Exchange View-Only Permissions on the Exchange organization	◆ Designation as the Domain Administrator, *or* membership in the `Builtin\Administrators` group on the Active Directory server, for enumerating the Active Directory information and calling the Microsoft Windows Management Instrumentation (WMI) providers on the domain controller and global catalog servers ◆ Membership in the Local Administrators group on each Exchange server for calling the WMI providers and accessing the registry and the metabase ◆ Delegation for at least View-Only Organization Management Permissions on the Exchange organization
Directory Server	◆ Membership in the Local Administrators group on the local computer ◆ Delegation for at least Exchange View-Only Permissions	◆ Delegation for at least Exchange View-Only Permissions

2.6 Discovering Exchange Server Resources

Use the Discovery_Exchange2007 Knowledge Script to discover configuration and resources for Microsoft Exchange Server in both clustered and non-clustered environments.

Before using this Knowledge Script, set up the proper accounts and permissions. For more information, see Section 2.5, “Permissions for Discovering Exchange Server Resources,” on page 19.

NOTE: If you delete a resource object or add a resource object, such as a Mailbox or Public Folder database in your Exchange Server, you will need to run the Discovery_Exchange2007 Knowledge Script again to update the remaining objects. This behavior occurs on DAG and standalone Mailbox roles.

Run this script on an NT_MachineFolder object, or an NT_VIR_MachineFolder object. By default, this script runs once.

Set the Values tab parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Discovery_Exchange2007 job fails. The default is 5.
Discovery	
Event Notification	
Raise event if discovery succeeds?	Select **Yes** to raise an event if discovery succeeds. The default is No.
Event severity when discovery succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery succeeds. The default is 25.
Raise event if discovery fails?	Select **Yes** to raise an event if discovery fails. The default is Yes.
Event severity when discovery fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery fails. The default is 5.
Raise event if discovery partially succeeds?	Select **Yes** to raise an event if discovery returns some data but also generates warning messages. The default is Yes.
Event severity when discovery partially succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery returns some data but also generates warning messages. The default is 10.

2.7 Configuring Security Manager to run Exchange Online Discovery

Before you can run the Discovery_ExchangeOnline Knowledge Script to discover the Exchange Online resources, you need to configure Security Manager:

1. Open the Security Manager.
2. Select the Exchange server on which you want to run the Knowledge Script.
3. On the Custom tab, click **Add**.
4. In the **Label** field, type `ExchangeOnline`.
5. In the **Sub-Label** field, specify the Exchange Online domain name that you want to discover. For example, `abc.onmicrosoft.com`.
6. In the **Value 1** field, specify a username.
7. In the **Value 2** field, specify a password.
8. Leave the **Value 3** field blank.
9. Select the **Extended application support** option to encrypt the password when it is stored in the repository.
10. Click **OK** and then click **Apply** to save the settings.

IMPORTANT: The Exchange Online domain that is configured in the Security Manager can be only discovered and monitored using the Exchange Online Knowledge Scripts. If you want to monitor multiple Exchange Online domains in your environment, then you must configure the Security Manager for each of the Exchange Online domains separately. Follow the **Step 1** through the **Step 10** for each of the Exchange Online domains.

2.8 Permissions for Discovering Exchange Online

Before discovering and monitoring Exchange Online, ensure that the Exchange Online user account, which is configured in the Security Manager has the following permission and membership:

- Any one of the Customized administrator roles. The recommended role is Service administrator.
- Membership in the Exchange View-Only Organization Management.

To configure the Exchange Online user account in the Security Manager, see Configuring Security Manager to run Exchange Online Discovery.

For information on the Exchange Online permissions, see the Microsoft article.

2.9 Discovering Exchange Online

Use the Discovery_ExchangeOnline Knowledge Script to discover Mailbox quota and Service health of Microsoft Exchange Online.

Run this script on an NT_MachineFolder object. By default, this script runs once.

Set the Values tab parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Discovery_ExchangeOnline job fails. The default is 5.
Discovery	
Comma separated List of Exchange Online domains to be discovered	Specify the list of Exchange Online domain names that you have configured in the Security Manager and want to discover. Separate the domain names with a comma. **IMPORTANT:** The domain details must be configured in the Security Manager before specifying in this parameter. The domains that are not configured in the Security Manager cannot be discovered using the Knowledge Script. For example, if you want to specify the domain `abc.onmicrosoft.com` in this parameter, then it must be configured in the Security Manager. For more information, see Configuring Security Manager to run Exchange Online Discovery.
Event Notification	
Raise event if discovery succeeds?	Select **Yes** to raise an event if discovery succeeds. The default is No.
Event severity when discovery succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery succeeds. The default is 25.
Raise event if discovery fails?	Select **Yes** to raise an event if discovery fails. The default is Yes.
Event severity when discovery fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery fails. The default is 5.

2.10 Configuring and Monitoring Database Availability Groups

A **database availability group** (DAG) is a set of up to 16 Microsoft Exchange Server 2010, 2013, 2016, or 2019 Mailbox servers that provides automatic database-level recovery from a database, server, or network failure. Mailbox servers in a DAG monitor each other for failures. When you add a Mailbox server to a DAG, that Mailbox server works with the other servers in the DAG to provide automatic, database-level recovery from database, server, and network failures.

2.10.1 New Functionality in Exchange Server 2010, 2013, 2016, and 2019

In Microsoft Exchange Server 2010, 2013, 2016, and 2019, DAG functionality replaces the following clustering functionality used with Microsoft Exchange Server 2007: cluster continuous replication (CCR), single copy cluster (SCC), and Local Continuous Replication (LCR). Exchange Server 2010, 2013, 2016, and 2019 do not use storage groups.

2.10.2 Adding a DAG for Monitoring

Add the computers that represent the individual computers of a DAG to the Master Management Group of an AppManager repository in Control Center. When you have added all DAG computers, create a server group, for example, `EX2K_DAG_1`, and add each DAG computer to that group.

For more information about adding computers to the Master Management Group of a repository and creating server groups, see the *Control Center User Guide for AppManager*.

2.10.3 Discovering Resources on a DAG

Use the **Discovery_ExchangeDAG** Knowledge Script to discover configuration and resources for a Microsoft Exchange Server 2010, 2013, 2016, and 2019 Database Availability Group (DAG). Run Discovery_ExchangeDAG on an Exchange Server 2010, 2013, 2016, and 2019 server to discover the virtual object for DAG. After you discover the virtual object, you must run Discovery_Exchange2007 on the newly discovered object so you can discover the databases. For more information, see Section 2.6, “Discovering Exchange Server Resources,” on page 21.

Before using the Discovery_ExchangeDAG Knowledge Script, set up the proper accounts and permissions. For more information, see Section 2.5, “Permissions for Discovering Exchange Server Resources,” on page 19.

To discover resources in an Exchange Server 2010, 2013, 2016, and 2019 DAG, run the following Discovery Knowledge Scripts in the order listed:

Knowledge Script	Resources Discovered
Discovery_NT	Run this script on each physical server that is a member of the DAG to discover Windows configuration and resources.
Discovery_Exchange2007	Run this script on each physical server that is a member of the DAG to discover Exchange Server 2010, 2013, 2016, and 2019 databases.
Discovery_ExchangeDAG	Run this script on any one of the physical servers that is a member of the DAG to discover Exchange Server 2010, 2013, 2016, and 2019 DAG virtual objects. Running this script creates a new top-level object that represents the DAG in the TreeView of the Operator Center console.
Discovery_Exchange2007	Run this script on the new top-level DAG node discovered in the previous step to discover the mailbox database resources in the DAG (which is the set of all mailbox databases managed by all servers in the DAG).

Set the Values tab parameters as needed:

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

Parameter	How to Set It
Raise event if DAG discovery succeeds?	Select **Yes** to raise an event if DAG discovery succeeds. The default is No.
Event severity when DAG discovery succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which DAG discovery succeeds. The default is 25.
Raise event if DAG discovery fails?	Select **Yes** to raise an event if discovery fails. The default is Yes.
Event severity when DAG discovery fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery fails. The default is 5.

NOTE: If you previously ran the Discovery_Cluster Knowledge Script on nodes that now belong to a DAG, the Discovery_Cluster script discovered the Windows Cluster resource object, NT_CLU_MachineFolder. If you later run Discovery_ExchangeDAG on any node that belongs to the DAG, the script will not discover any new objects, because an object with same name was added using Discovery_Cluster KS. As a result, you will not be able to use Discovery_Exchange2007 KS to discover the databases on the DAG object, because Discovery_Exchange2007 does not work with the NT_CLU_MachineFolder resource object.

To address this situation, remove the Windows Cluster object that was discovered with the Discovery_Cluster Knowledge Script and use the Discovery_ExchangeDAG to discover the DAG object.

2.10.4 Monitoring Resources on a DAG

The following Mailbox server Knowledge Scripts can monitor DAGs in Exchange Server 2010, 2013, 2016, and 2019:

- MBS_DatabaseStateChange
- MBS_DatabaseStatus
- MBS_MailboxUsage
- MBS_PublicFolderUsage (only for Exchange Server 2013, 2016, and 2019)

2.11 Configuring and Monitoring Clusters

Cluster groups are features of Windows Server 2003 and Windows Server 2008. You can install Exchange Server 2007 on the nodes of a cluster group and have the advantages of clustering available to your messaging environment. Exchange 2010, 2013, 2016, and 2019 do not support cluster groups.

Cluster continuous replication (CCR) configurations support active/passive mode.

AppManager for Microsoft Exchange Server and Exchange Online supports up to eight physical nodes for single copy cluster (SCC) configurations. For more information, see Section 2.11.3, “Monitoring Resources on Cluster Nodes,” on page 26.

NOTE: If you have clusters set up on Exchange Server 2007 and you upgrade to Exchange Server 2010, 2013, 2016, and 2019, you must manually delete the Exchange2007 objects from the Navigation pane or TreeView in AppManager and run discovery again after you upgrade to Exchange Server 2010, 2013, 2016, and 2019.

2.11.1 Adding an Exchange Server Cluster to the Master View

Add the computers that represent the individual nodes of a cluster to the master view of an AppManager repository in Control Center. Then group the nodes by cluster.

For example, if EX2KSVR_1 and EX2KSVR_2 are the two nodes of an Exchange Server 2007 cluster, add each computer to the master view.

When you have added all node computers, create a server group, for example, EX2K_CLUSTER_1, and add each node computer to that group.

For more information about adding computers to the master view of a repository and creating server groups, see the *Control Center User Guide for AppManager*.

2.11.2 Discovering Resources on Cluster Nodes

To discover resources in an Exchange Server 2007 cluster, run the following Discovery Knowledge Scripts in the order listed:

Knowledge Script	Resources Discovered
Discovery_NT	Windows configuration and resources, such as memory, physical and logical disks, and CPU.
Discovery_MSCS	Microsoft Cluster Service configuration and resources, such as cluster services and nodes in a cluster. **NOTE:** The MSCS module is not mandatory to monitor the Exchange server cluster. It is only used if you want to monitor additional services for Microsoft Cluster configuration and resources, such as cluster services and nodes in a cluster.
Discovery_Cluster	Clustered Mailbox Server (CMS) objects.
Discovery_Exchange2007	Exchange Server configuration and resources, such as services, server view, and protocols. When you discover Exchange resources, AppManager for Microsoft Exchange Server and Exchange Online lists each CMS that a computer can own as a child object of that computer, regardless of whether the CMS is active at the time of discovery.

2.11.3 Monitoring Resources on Cluster Nodes

Use cluster-aware Knowledge Scripts on both physical and virtual server to monitor resources on *each node* in a cluster and on each CMS as it moves from node to node as a result of failover. The All_* Knowledge Scripts and the Knowledge Scripts that run on a Mailbox server can monitor Windows cluster resources. Microsoft supports clustering only on the Mailbox server role.

- All_BestPracticesAnalyzer
- All_ClockSynchronization
- All_EventLog
- All_ServiceStatus
- MBS_DatabaseStateChange
- MBS_DatabaseStatus

- MBS_MailboxAccessibility
- MBS_MailboxUsage
- MBS_MailFlow
- MBS_MessagingRecordsMgmt
- MBS_PublicFolderUsage
- MBS_Replication

You can run the MBS_* Knowledge Scripts on physical and virtual nodes.

2.11.4 Collecting Data for Clustered Mailbox Servers

When you monitor a CMS, AppManager for Microsoft Exchange Server and Exchange Online associates the collected data with the physical node.

- A Knowledge Script job running on a CMS collects data for that CMS and for the associated physical node.
- A Knowledge Script job running on a physical node collects data for any CMS associated with that physical node.

Example 1: SCC cluster with Active/Active configuration

If `CMS1` is active on `EX2KSVR_1` and `CMS2` is active on `EX2KSVR_2`, the job creates two datastreams when you run the job on `CMS1`:

- Datastream for `CMS1`
- Datastream for `EX2KSVR_1`

When you run a job on `EX2KSVR_1`, the job collects data for `CMS1`. If `CMS2` fails over to `EX2KSVR_1` and you run a job on `EX2KSVR_1`, the job creates two datastreams:

- Datastream for `CMS1`
- Datastream for `CMS2`

Example 2: CCR cluster with Active/Passive configuration

If `CMS1` is active on `EX2KSVR_1`, the job creates two datastreams when you run the job on `CMS1`:

- Datastream for `CMS1`
- Datastream for `EX2KSVR_1`

If `CMS1` fails over to `EX2KSVR_2`, and you run a job on `EX2KSVR_2` the job creates two datastreams:

- Data stream for `CMS1`
- Datastream for `EX2KSVR_2`

2.12 Upgrading Knowledge Script Jobs

If you are using AppManager 8.x or later, the module upgrade process now *retains* any changes you may 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 may 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.

This release of AppManager for Microsoft Exchange Server and Exchange Online might contain updated Knowledge Scripts. You can push the changes for updated scripts to running Knowledge Script jobs in one of the following ways:

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

2.12.1 Running AMAdmin_UpgradeJobs

The AMAdmin_UpgradeJobs Knowledge Script can push changes to running Knowledge Script jobs. Your AppManager repository (QDB) must be at version 7.0 or later. Upgrading jobs to use the most recent script version allows the jobs to take advantage of the latest script logic while maintaining existing parameter values for the job.

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

2.12.2 Propagating Knowledge Script Changes

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

Before propagating script changes, verify that the script parameters are set to your specifications. New parameters may need to be set appropriately for your environment or application.

If you are not using AppManager 8.x or later, customized script parameters may 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 both properties and the script.

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

2.12.3 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.

2.13 Configuring the PowerShell Execution Policy

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

2.13.1 Understanding PowerShell Cmdlets

Microsoft Exchange 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**. In addition to the base cmdlets provided by PowerShell, installation of the Exchange Management Console adds approximately 300 Exchange Server cmdlets.

When running the Exchange2007 category of Knowledge Scripts, AppManager makes a series of calls to PowerShell and the Exchange Server cmdlets. The combination of cmdlets depends on the version of Exchange Server. AppManager executes the cmdlets to manipulate Exchange Server objects such as Outlook Web Access, virtual directories, mailboxes, distribution groups, and storage groups (2007 only).

For more information about using Powershell, see your Microsoft PowerShell documentation.

2.13.2 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 Exchange2007 Knowledge Scripts. Although the scripts that ship with AppManager for Microsoft Exchange Server and Exchange Online is written in VBScript and installed as `<scriptname>.qml`, the logic for the scripts is 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 Exchange2007 Knowledge Scripts, but with a `.ps1` extension.

NOTE: The digital signature encoded in an Exchange2007 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 an Exchange2007 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 Section 2.13.3, “Trusting Exchange PowerShell Scripts,” on page 30.
- **RemoteSigned**, which allows local scripts to run regardless of signature, and requires trusted digital signatures only for remote scripts. Exchange2007 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 Exchange 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.
3. Repeat Steps **1** and **2** on all agent computers, including Server role computers.

2.13.3 Trusting Exchange PowerShell 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 Exchange PowerShell 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 *each* Exchange Server in your environment.

You can import the digital certificate by running one of the Exchange2007 PowerShell scripts from the command line.

To import the digital certificate:

1. Open the Exchange Command Shell on the agent computer.
2. Change to the `AppManager\bin\PowerShell\Scripts` directory.
3. Type `.\Exchange2007_All_EventLog.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 Exchange PowerShell scripts.

To extend trust to all other user accounts, see Section 2.13.4, “Extending Trust to All User Accounts,” on page 31.

To establish trust between all users accounts and the Microsoft digital certificate, see Section 2.13.5, “Establishing Trust for the Microsoft Certificate,” on page 32.

2.13.4 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.

2.13.5 Establishing Trust for the Microsoft Certificate

The Exchange2007 Knowledge Scripts access a file called `Exchange.Format.ps1xml`, which Microsoft ships with Exchange Server. For the Exchange2007 Knowledge Scripts to run properly, the Microsoft digital signature certificate must have a trust relationship with the Microsoft digital signature certificate.

To create this trust relationship, perform the steps outlined in Section 2.13.4, “Extending Trust to All User Accounts,” on page 31, with the following exceptions:

- In Step 9 on page 31, right-click the **Microsoft** certificate instead of the **NetIQ** certificate.
- In Step 12 on page 31, type `Microsoft` instead of `NetIQ`.
- In Step 9 on page 32, select **Microsoft.cer** instead of **NetIQ.cer**.

2.14 Changing Configuration Settings

AppManager for Microsoft Exchange Server and Exchange Online includes the following components:

- A client object, `MCPSHostClient.dll`, which runs within the AppManager agent. This client object starts the server program and asks it to run jobs.
- A server program, `MCPSHostServer.exe`, which provides the PowerShell environment in which the Exchange2007 scripts are executed.

Both components have associated configuration files that define certain operational parameters. You can modify these settings to fine-tune performance or to specify resource usage limits.

The configuration files are in XML format. After making changes, ensure that the files retain their well-formed XML format. Also do not remove or change settings other than those documented here. NetIQ Corporation strongly recommends that you create backup copies of these files before modifying them.

NOTE: This topic does not discuss all configuration settings. As a rule, if a configuration setting is not discussed in this topic, you should not change the value of that setting.

2.14.1 Client Configuration Settings

The client configuration file, `MCPSHostClient.dll.config`, resides in the `AppManager\bin\PowerShell` directory. You can change the following settings.

In the `<appSettings>` section:

- **maxActiveServers** Use this setting to specify the maximum number of servers that can be active at any time. Use this setting in conjunction with `maxMemoryUsage` to specify a lower memory threshold with an increased number of servers that can be used. This combination is beneficial for situations in which a server exceeds the memory limitation and has to shut down. If only one server can be active at a time, job requests are blocked until the server restarts. If you allow more than one server to be active, job requests can be executed in other server processes or on new servers if the current number of active servers is less than `maxActiveServers`.
- **serverStartupTimeout** If `MCPSHostServer.exe` is not already running when a job is scheduled for execution, the client starts the server automatically. After starting the server, the client attempts to contact it. Use this configuration setting to specify the number of seconds that the client should attempt to contact the server. An error event is raised if the client cannot contact the server within the specified period.

In the `<log4net>` section:

- **file** Use this setting to specify the pathname of the log file. If the pathname is a relative path, it is considered to be relative to the `\AppManager\bin\PowerShell` directory.
- **appendToFile** Use this setting to indicate whether the client overwrites the existing log file or appends to it, at the time the client is loaded into the AppManager agent.
- **maxSizeRollBackups** Use this setting to specify the number of old log files you want to retain.
- **maximumFileSize** Use this setting to specify the maximum size of a log file. After a log file reaches this size, it is deleted, or renamed if the `maxSizeRollBackups` value is greater than 0.

2.14.2 Server Configuration Settings

The server configuration file, `MCPSHostServer.exe.config`, resides in the `AppManager\bin\PowerShell` directory. You can change the following settings.

In the `<appSettings>` section:

- **serverShutdownTimeout** Use this setting to specify the number of seconds that the server will remain running when no jobs are executing. If no jobs are submitted to the server during this period, the server shuts down and will restart the next time a client needs to run a job.
- **upperMaxRunspaceHosts** The PowerShell runspace pool allocates runspaces as needed. Each execution of a job requires one runspace. Runspaces return to the pool after use and are then available for other jobs. Use this setting to set the absolute limit on the number of runspaces allocated for a pool. If a client requests a runspace when none is available and the pool has reached this limit, the client is blocked from running until a runspace becomes available.

  If you do not specify the runspace setting, the pool always allocates a new runspace, even if all others are in use, thereby ensuring that clients never have to wait for a runspace to be available.
- **maxMemoryUsage** Use this setting to specify the maximum amount of memory, in megabytes, that the server process should consume. If memory usage exceeds the maximum size, the server blocks additional requests from clients and restarts automatically after the last client has finished job execution. Because Exchange2007 Knowledge Script jobs use Exchange cmdlets, which require a large amount of memory, server memory usage can grow excessively.

In the `<log4net>` section:

- **file** Use this setting to specify the pathname of the log file. If the pathname is a relative path, it is considered to be relative to the `\AppManager\bin\PowerShell` directory.
- **appendToFile** Use this setting to indicate whether the client overwrites the existing log file or appends to it, at the time the client is loaded into the AppManager agent.
- **maxSizeRollBackups** Use this setting to specify the number of old log files you want to retain.
- **maximumFileSize** Use this setting to specify the maximum size of a log file. After a log file reaches this size, it is deleted, or renamed if the `maxSizeRollBackups` value is greater than 0.

2.15 Troubleshooting PowerShell Errors

Knowledge Scripts in the Exchange2007 category may raise such events as `"PowerShell script failed to run to completion”` or `"Error executing PowerShell script."` These errors can occur when Knowledge Scripts take a long time to run, or when there is contention for access to the server that executes the PowerShell scripts, `MCPSHostServer.exe`. The following are some recommendations for resolving these issues:

- **Increase the amount of memory that can be used by MCPSHostServer.exe**. Increasing the memory limit reduces the frequency with which the server restarts due to excessive memory usage. Increasing the memory limit also reduces the number of PowerShell errors; each time the server recognizes that it is exceeding its memory usage threshold, the server prevents new jobs from executing until all existing jobs have completed and the server restarts. If existing jobs take a significant amount of time to complete, the waiting jobs may time out and return errors. To increase the amount of memory `MCPSHostServer.exe` can use, modify the value of the `maxMemoryUsage` setting. For more information, see Section 2.14, “Changing Configuration Settings,” on page 33.

- **Increase the number of PowerShell execution environments, or runspaces that MCPSHostServer.exe can host**. The default number of runspaces is eight, which means no more than eight Knowledge Script jobs can be running simultaneously in the server. If you attempt to run additional jobs, the jobs are held back until runspaces become available as existing jobs complete their iterations. Being held back in this manner increases the chance that jobs will time out before running, or before completing their iteration. To increase the number of available runspaces, modify the `upperMaxRunspaceHosts` setting. For more information, see Section 2.14, “Changing Configuration Settings,” on page 33.

  Increasing this value will be beneficial if you are running more than eight Exchange2007 Knowledge Script jobs, but even then the benefit may not be significant.

NOTE: The client’s maxActiveServers configuration option specifies the maximum number of servers that can be active at any time (the default is five). The maxActiveServers configuration value and the UpperMaxRunspaceHosts server configuration value determine the total number of jobs that can be serviced at any one time. You can have more than this number of jobs in the “Running” state in AppManager, but only if some of the jobs are between iterations, and not actually running at the same time.

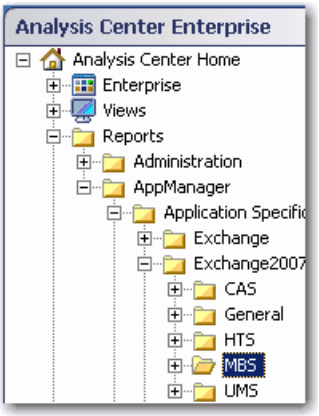
---

3 Reporting with Analysis Center

NetIQ Analysis Center is designed to import raw data from multiple AppManager repositories, transform that data into useful information about the computing infrastructure that supports your business, and publish that information in the form of reports.

AppManager for Microsoft Exchange Server and Exchange Online or later ships with a package of Analysis Center report templates designed specifically for Exchange Server 2007 or later data. With these reports, you can capture and distribute vital information such as average daily and hourly response time for mail flow.

You can find the reports in the Analysis Center Navigation pane sorted by server role within the **Reports > AppManager > Application Specific > Exchange2007** folder.



3.1 System Requirements for Analysis Center Reports

Exchange Reports for Analysis Center have the following system requirements:

- Analysis Center version 2.7 or later
- AppManager for Microsoft Exchange version 7.3 or later

3.2 Installing the Report Package

You can install the Analysis Center reports for this module to either local or remote databases. You need to install the reports only once per database.

To install the report package:

1. Launch the module installer, `AM70-Exchange2007-7.x.x.0.msi`.
2. From the Knowledge Script and Report Package Installation Options page of the installation wizard, select **Install report package**.
3. In the **SQL Server name\instance** field, specify the SQL Server name of the server hosting the Analysis Center Configuration Database.

4 In the **Analysis Center configuration database name** field, type the name of the configuration database and click **Next**.

5 Select either Windows or SQL Server authentication and click **Next**.

6 When the installer finishes, launch the Analysis Center console.

3.3 Exchange Server 2007 or later Analysis Center Report Templates

The Analysis Center report package for AppManager for Microsoft Exchange Server and Exchange Online or later contains the following templates.

Template	Description
Client Access Server Report Templates	
Average OWA login failures	Two reports based on the datastreams generated by the CAS_Activity Knowledge Script. The daily report and the hour report present the average number of Outlook Web Access login failures for the period you specify.
Average number of current OWA users	A daily report and an hourly report that present the average number of users logged on to Outlook Web Access for the period you specify.
Average number of OWA user sessions	Two reports based on the datastreams generated by the CAS_Activity Knowledge Script. The daily report and the hourly report present the average Outlook Web Access login rate for user sessions for the period you specify.
General Exchange Report Templates	
NOTE: Unlike the other report templates in the Exchange2007 report package, the General templates allow you to report on any datastream generated by any Knowledge Script in the Exchange2007 category.	
Exchange Server 2007 performance data filtered by data source	Examines performance data for Exchange Server 2007 or later based on data source for the period you specify.
Exchange Server 2007 performance data filtered by Knowledge Script	Examines performance data for Exchange Server 2007 or later, based on the Knowledge Scripts that generated the datastreams, for the period you specify.
Hub Transport Server Report Templates	
Average use of Transport Dumpster queue	Two reports based on the datastreams generated by the HTS_TransportDumpster Knowledge Script. The daily report and the hourly report present average use of the Transport Dumpster queue for the period you specify: number of items in the queue, size of items in the queue, insertion rate, deletion rate, and number of re-deliveries.
Mailbox Server Report Templates	
Average length of the copy queue	Two reports based on the datastreams generated by the MBS_Replication Knowledge Script. The hourly report and the daily report present the average number of logs in the copy queue for the period you specify.

Template	Description
Average disk usage	Two reports based on the datastreams generated by the MBS_DatabaseStatus Knowledge Script. The daily report and the hourly report present average disk usage for the period you specify, including disk access time, disk read time, disk write time, and queued requests.
Average use of File Share Witness	Two reports based on the datastreams generated by the MBS_Replication Knowledge Script. The daily report and the hourly report present average use of File Share Witness by server for the period you specify.
Average number of mailboxes in a storage group	Examines the average number of mailboxes in a storage group (Exchange 2007 only) for the period you specify. This report uses the datastreams generated by the MBS_MailboxUsage Knowledge Script.
Average size of largest mailboxes	Examines the average size of the top *n* mailboxes for the period you specify. This report uses the datastreams generated by the MBS_MailboxUsage Knowledge Script.
Average mail flow response time	Two reports based on the datastreams generated by the MBS_MailFlow Knowledge Script. The daily report and the hourly report present average mail flow response time for the period you specify.
Average number of messages in top n mailboxes	Examines the average number of messages in the top *n* mailboxes for the period you specify. This report uses the datastreams generated by the MBS_MailboxUsage Knowledge Script.
Average number of logs in the replay queue	Two reports based on the datastreams generated by the MBS_Replication Knowledge Script. The daily report and the hourly report present the average number of logs in the replay queue for the period you specify.
Unified Messaging Server Report Templates	
Average call activity per UMS call type	Two reports based on the datastreams generated by the UMS_CallActivity Knowledge Script. The daily report and the hourly report present average call activity for each UMS call type.
Average number of UMS-related failures	Two reports based on the datastreams generated by the UMS_Failures Knowledge Script. The daily report and the hourly report present the average number of UMS-related failures: calls disconnected due to internal or external errors, redirection failures, and failures for accessing the Mailbox server, the Hub Transport server, and Active Directory.
Average number of Unified Messaging operations	Two reports based on the datastreams generated by the UMS_Performance Knowledge Script. The daily report and the hourly report present the average number of Unified Messaging operations based on response time.

4 Exchange 2007 Knowledge Scripts

AppManager for Microsoft Exchange Server and Exchange Online provides Knowledge Scripts for monitoring Microsoft Exchange Server.

The **Exchange Server 2007** Knowledge Scripts supports Microsoft Exchange Server 2007 resources installed in *non-clustered* environments and the following *clustered* environments:

- *Cluster continuous replication* (CCR) combines the log shipping and replay functionality in Exchange Server 2007 with the failover functionality in the Microsoft cluster service. CCR is a solution that can be deployed with no single point of failure in a single datacenter or between two datacenters.
- *Single copy clusters* (SCC), known as shared storage clusters in previous versions of Exchange Server, are present in Exchange Server 2007.

In a clustered environment, AppManager raises error events if failover occurs while jobs are running. These error events are expected results of the failover process and can be safely ignored.

A subset of the Knowledge Scripts support Microsoft Exchange Server 2010, 2013, 2016, and 2019 resources installed in a database availability group (DAG). A DAG is a set of up to 16 Microsoft Exchange Server 2010, 2013, 2016, or 2019 Mailbox servers that provides automatic database-level recovery from a database, server, or network failure. Exchange Server 2010, 2013, 2016, and 2019 do not use storage groups.

NOTE: You should review the permissions required for different roles in the Section 2.5, “Permissions for Discovering Exchange Server Resources,” on page 19 before you run the Knowledge Scripts.

You should review the permissions required for different roles in the Section 2.5, “Permissions for Discovering Exchange Server Resources,” in the *AppManager for Exchange Management guide* before you run the Knowledge Scripts.

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**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press F1.

Knowledge Script	What It Does
All_BestPracticesAnalyzer	Monitors the Windows event log for errors and warnings raised by the Exchange Best Practices Analyzer.
All_ClockSynchronization	Monitors the synchronization of clocks for one or more Domain Controllers.
All_EventLog	Monitors the Windows Application event log for errors and warning events related to Exchange Server.
All_ServiceStatus	Monitors the status of Exchange Server services.
CAS_Activity	Monitors Client Access server services and functions.
CAS_Connectivity	Monitors connectivity for Client Access server services on Exchange Server 2007 and 2010: ActiveSync, Outlook Web Access, Outlook Web services, and the Autodiscover service.

Knowledge Script	What It Does
CAS_OABAvailability	Monitors whether offline address books can be downloaded.
CAS_PublicFolderAvailability	Monitors the accessibility of public folders on the Client Access server.
ETS_ExternalMail	Monitors e-mail sent to and from your Exchange environment.
ETS_MessageHygiene	Monitors message hygiene functions for the Edge Transport server.
HTS_Connectivity	Monitors the connectivity with a Mailbox server, and monitors the time of the last synchronization with the Edge Transport server.
HTS_SafetyNet	Monitors the Safety Net availability in Exchange Server 2013, 2016, and 2019. It replaces the Transport Dumpster Knowledge script available for Exchange Server 2007 and 2010.
HTS_SendersAndRecipients	Measures number of messages in a mailbox and total message size for senders and recipients.
HTS_TransportDumpster	Monitors Transport Dumpster activity, availability, and the number of items in the Transport Dumpster.
MBS_ClientActivity	Monitors Exchange Server 2013, 2016 and 2019 Mailbox server services and functions.
MBS_ClientConnectivity	Monitors connectivity for Mailbox server services on Exchange Server 2013, 2016, and 2019: ActiveSync, Outlook Web services, and the Autodiscover service.
MBS_ClusterOwner	Determines whether an Exchange Server is the owner of the node and whether the CMS is down. This script only runs on servers with Exchange Server 2007.
MBS_DatabaseStateChange	Monitors changes in the state of mailbox databases on an Exchange Server. States include active, passive, suspended, removed, or unmounted.
MBS_DatabaseStatus	Monitors Exchange Server mailbox databases for size of online maintenance window, defragmentation time, free log space, free file space, and number of mailboxes.
MBS_MailboxAccessibility	Monitors the ability of the Mailbox server to access individual mailboxes.
MBS_MailboxUsage	Measures the size of mailboxes by the number of messages in the mailbox or by total message size in MB.
MBS_MailFlow	Sends test e-mail to local or remote Mailbox servers.
MBS_MessagingRecordsMgmt	Monitors message management tasks such as deleting, journaling, moving, and retention.
MBS_PublicFolderUsage	Measures the size of public folders by the number of messages in the folders or by total message size in MB.
MBS_Replication	Monitors replication status and performance for a Mailbox server.
Transport_BackPressure	Monitors the status of back pressure for the Hub Transport server.
Transport_ConnectorStatus	Monitors the status of send, receive, foreign, and delivery agent connectors on Exchange Servers.

Knowledge Script	What It Does
Transport_QueueStatus	Monitors the status of queues on the Hub Transport server: submission queue, mailbox delivery queue, remote delivery queue, poison message queue, and unreachable destination queue.
UMS_CallActivity	Monitors call activity on the Unified Messaging server: voice, fax, play on phone, auto attendant, subscriber access, prompt editing.
UMS_Connectivity	Monitors connectivity to Hub Transport servers, Mailbox servers, Active Directory, and Unified Messaging-enabled mailboxes.
UMS_Failures	Monitors failures related to redirected calls, disconnected calls, and access to Active Directory, the Hub Transport server, and the Mailbox server.
UMS_Performance	Monitors the performance of the Unified Messaging server: user response latency, operation response time, queued messages for call answering, queued OCS user notifications, and calls disconnected while playing audio hourglass tones.
Recommended Knowledge Script Group	Performs essential monitoring of your Exchange Server environment.

4.1 All_BestPracticesAnalyzer

Use this Knowledge Script to monitor the Windows event log for errors and warnings whose source is BPA (Exchange Best Practices Analyzer). This script raises an event if the Knowledge Script job fails or the event log contains error and warning messages.

If you are not running the BPA, you can use this script to execute the BPA each time the script runs. If you set the *Execute Best Practices Analyzer during job?* parameter to **Yes**, AppManager runs the BPA at each iteration of the Knowledge Script job. AppManager then stops the BPA and analyzes the event log for errors and warnings raised by the BPA.

NOTE

- This script may raise duplicate events on computers where multiple Exchange Server 2007 and 2010 roles are installed. These duplicate events are raised because the BPA populates the event log with errors and warnings for *each role* when the error or warning is applicable for the entire Exchange Server 2007 or 2010 organization.
- This script is not applicable for Exchange Server 2013, 2016, and 2019.
- Most BPA events do not indicate which role they are associated with. Therefore, this script raises events that are not associated with a role. However, the AppManager event messages include the text of the BPA event, which should help you determine which role is affected.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see Section 4.43, “Recommended Knowledge Script Group,” on page 162.

4.1.1 Running the ExBPAcmd.exe Tool Manually

The BPA must be running so that it can submit any errors or warnings to the event log. This script will not work if you are not running the BPA and do not enable the *Execute Best Practices Analyzer during job?* parameter.

If you do not enable this script to launch the BPA, then run the `ExBPAcmd.exe` tool manually to monitor the Windows Event Log for errors and warnings.

To run the ExBPAcmd.exe tool manually:

1. Open the Exchange Management Shell.
2. Run the following command:

   ```
   $exBPAoutput = . "C:\Program Files\Microsoft\Exchange Server\Bin\ExBPAcmd.exe"
   -p Events:Enable -r "5,$role,$scan_type,Server=<ExchangeServerName>"
   ```

   where `$role` is one of the following values enclosed in quotation marks (“ ”): `Mailbox`, `Gateway`, `Bridgehead`, `ClientAccess`, `ClusterMailbox`

   where `$scan_type` is one of the following values enclosed in quotation marks (“ ”): `Health`, `ConnectivityTask`, `Ex2007Readiness`, `Perf`, `Permissions`

   where `<ExchangeServerName>` is the name of the Exchange server where you want to run the `ExBPAcmd.exe` tool.
3. Run the following command to display the output of the `ExBPAcmd.exe` tool:

   ```
   Write-Host $exBPAoutput
   ```

   These commands enable the event log register.

4.1.2 Prerequisites

Before running this script, ensure that the following permissions and memberships exist.

Component	Required Permissions and Memberships
Account running the AppManager agent service (netiqmc)	◆ Membership in the Builtin\Administrators group on the Active Directory server ◆ Membership in the local Administrators group on the local computer ◆ Delegation for at least Exchange View-Only permissions
Exchange Best Practice Analyzer tool (for all Exchange Server roles)	◆ Designation as the Domain Administrator, or membership in the Builtin\Administrators group on the Active Directory server, for enumerating the Active Directory information and calling the Microsoft Windows Management Instrumentation (WMI) providers on the domain controller and global catalog servers ◆ Membership in the Local Administrators group on each Exchange server for calling the WMI providers and accessing the registry and the metabase ◆ Delegation for at least Exchange View-Only Permissions on the Exchange organization

4.1.3 Resource Object

Exchange_Server

4.1.4 Default Schedule

By default, this script runs every one hour.

4.1.5 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the All_BestPracticesAnalyzer job fails. The default is 5.
Analyze Exchange Server 2007/2010 Best Practices	
Execute Best Practices Analyzer during job?	Select **Yes** to allow AppManager to launch the BPA using a command-line execution of `ExBPACmd.exe` at each iteration of this script. If you are already running the BPA, then clear this option. The BPA *must* be running so that it can submit any errors or warnings to the event log. The default is Yes.
Type of scan to execute	Select the type of scan the BPA should perform: ◆ **Connectivity Test**. To scan network connections and permissions for the selected Exchange server. ◆ **Exchange 2007 Readiness Check**. To assess your organization's readiness for Exchange Server 2007. ◆ **Health Check**. To perform a full scan, checking for errors, warnings, and configuration information. This option is selected by default. ◆ **Permission Check**. To ensure that your Exchange Server 2007 deployment has the proper credentials as defined by your organization.
Event Notification	
Comma-separated list of event IDs to ignore	Provide a list of error and warning ID numbers that this script should ignore when scanning the event log. Separate the numbers with a comma.
Raise event for errors found in Windows Event Log?	Select **Yes** to raise an event when the event log contains error messages raised by the BPA. The default is Yes.
Event severity when errors found in the Windows Event Log	Set the severity level, from 1 to 40, to indicate the importance of an event in which the event log contains error messages. The default is 5.
Raise event for warnings found in Windows Event Log?	Select **Yes** to raise an event when the event log contains warning messages raised by the BPA. The default is Yes.
Event severity for warnings found in the Windows Event Log	Set the severity level, from 1 to 40, to indicate the importance of an event in which the event log contains warning messages raised by the BPA. The default is 15.

4.2 All_ClockSynchronization

Use this Knowledge Script to monitor the synchronization of clocks for one or more Domain Controllers. This script raises an event if the number of seconds of difference between clocks exceeds the threshold you set.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see Section 4.43, “Recommended Knowledge Script Group,” on page 162.

4.2.1 Resource Object

Exchange_Server

4.2.2 Default Schedule

By default, this script runs every 15 minutes.

4.2.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the All_ClockSynchronization job fails. The default is 5.
Monitor Clock Synchronization with Domain Controller	
Comma-separated list of Domain Controllers to test	Use this parameter to limit the number of Domain Controller (DC) clocks that are tested for synchronization with the clock on the server running the ClockSynchronization Knowledge Script. Provide a list of fully qualified hostnames, separating multiple names by commas. Leave this parameter blank to test all DC clocks in your organization.
Event Notification	
Raise event if clocks are not synchronized?	Select **Yes** to raise an event if the clock on the server running the ClockSynchronization Knowledge Script is not synchronized with the clock on the DC. The default is Yes.
Threshold - Maximum clock difference	Set the maximum number of seconds that the server clock can be out of sync with the DC. For example, setting the threshold to 2 indicates that it is acceptable for the clock to be two seconds faster or slower than the clock on the DC. The default is 10 seconds. If you want the server clock to be in sync with the DC clock, set this parameter to 0.
Event severity when clock difference exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the clock synchronization offset exceeds the threshold you set. The default is 25.

4.3 All_EventLog

Use this Knowledge Script to monitor the Windows Application event log for errors and warnings that contain the word **exchange**. This script raises an event if event log entries match your search criteria. You can filter your search by event ID, event category, and event source.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see Section 4.43, “Recommended Knowledge Script Group,” on page 162.

4.3.1 Resource Object

Exchange_Server

4.3.2 Default Schedule

By default, this script runs every 15 minutes.

4.3.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the All_EventLog job fails. The default is 5.
Monitor Windows Event Log	
Event Notification	
Comma-separated list of event sources to ignore	Provide a list of event sources that this script should ignore when scanning the Application event log. Separate the source names with a comma. Event sources are computers whose names are displayed in the Source column of the event log.
Comma-separated list of event categories to ignore	Provide a list of event categories that this script should ignore when scanning the Application event log. Separate the category names with a comma.
Comma-separated list of event IDs to ignore	Provide a list of error and warning ID numbers that this script should ignore when scanning the Application event log. Separate the numbers with a comma.
Raise event if Exchange error events are found?	Select **Yes** to raise an event if the Application event log contains error events that match your search criteria. The default is Yes.
Event severity when Exchange error events are found	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Application event log contains error events. The default is 10.
Raise event if Exchange warning events are found?	Select **Yes** to raise an event if the Application event log contains warning events that match your search criteria. The default is Yes.
Event severity when Exchange warning events are found	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Application event log contains warning events. The default is 20.

4.4 All_ServiceStatus

Use this Knowledge Script to monitor the status of Exchange Server services. This script raises an event when services are not running, and when stopped services fail to start. Also, you can collect data for all the exchange server services through this script.

This script monitors and restarts the following Exchange Server services:

Mailbox Server Role Services		
Monitoring	Active Directory Topology	Information Store
Mailbox Assistants	Mail Submission	Replication Service
System Attendant	Search Indexer	Service Host
Transport Log Search	Search (Exchange)	Server Extension for Windows Server Backup
Client Access Server Role Services		
Service Host	Active Directory Topology	File Distribution
Hub Transport Server Role Services		
Active Directory Topology	EdgeSync	Transport
Transport Log Search		
Edge Transport Server Role Services		
ADAM	Credential Service	Transport
Anti-SPAM Update	Monitoring	Transport Log Search
Unified Messaging Server Role Services		
Active Directory Topology	File Distribution	Monitoring
Unified Messaging	Speech Engine	

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see Section 4.43, “Recommended Knowledge Script Group,” on page 162.

4.4.1 Resource Objects

- Exchange2007_Services
- Exchange2007_Service
- Exchange2010_Services
- Exchange2010_Service
- Exchange2013_Services
- Exchange2013_Service
- Exchange2016_Services
- Exchange2016_Service
- Exchange2019_Services
- Exchange2019_Service

4.4.2 Default Schedule

By default, this script runs every 15 minutes.

4.4.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the All_ServiceStatus job fails. The default is 5.
Monitor Status of Exchange Services	
Services to be Monitored	
Monitor services configured to start automatically?	Select **Yes** to monitor Exchange Server services that are configured to start automatically. The default is Yes. When you enable this parameter, the All_ServiceStatus job does not raise events for services that are configured to start manually, nor does it start manual services that are not running.
Monitor services configured to start manually?	Select **Yes** to monitor Exchange Server services that are configured to start manually. The default is No. When enabled, the All_ServiceStatus job does not raise events for services that are configured to start automatically.
Event Notification	
Raise event if Exchange services are not running?	Select **Yes** to raise an event if at least one Exchange Server service is not running. The default is Yes. When you enable this parameter, the All_ServiceStatus job raises events only for those services you selected in the **Services to be Monitored** parameters.
Event severity when services are not running	Set the severity level, from 1 to 40, to indicate the importance of an event in which at least one Exchange Server service is not running. The default is 10.
Start services not currently running?	Select **Yes** to start Exchange Server services that are not running. The default is Yes. When you enable this parameter, the All_ServiceStatus job starts only those services you selected in the **Services to be Monitored** parameters.
Threshold - Timeout for service startup	Set the number of seconds that AppManager should wait for Exchange Server services to restart before raising an event. The default is 60 seconds.
Raise event if stopped services fail to start?	Select **Yes** to raise an event if AppManager cannot start Exchange Server services that are not running. The default is Yes.
Event severity when stopped services fail to start	Set the severity level, from 1 to 40, to indicate the importance of an event in which Exchange Server services fail to start after the specified timeout period. The default is 5.
Data Collection	

Parameter	How to Set It
Collect Data?	Select **Yes** to collect data for all exchange server services. The default is No.

4.5 Availability

This Knowledge Script is obsolete, although you can still use it. Its functionality is distributed among the following Knowledge Scripts introduced with AppManager for Exchange Server 2007 version 7.3:

- HTS_TransportDumpster
- MBS_DatabaseStateChange
- MBS_MailboxAccessibility
- MBS_MailboxUsage
- MBS_Replication

****

Use this Knowledge Script to monitor the availability of the Exchange Server Mailbox Role and Hub Transport Role.

For the Mailbox Role, this script monitors the following activities:

- Mailbox database availability
- Replication latency
- Number of pending replication transactions
- Replication rate
- Status of replication agent
- Availability of the File Share Witness, a requirement for using the CCR functionality in Exchange Server 2007

For the Hub Transport Role, this script monitors the availability of the Transport Dumpster, a container for e-mail that has already been sent and is waiting for deletion.

4.5.1 Prerequisites

Before running this script, ensure that the following permissions and memberships exist.

Component	Required Permissions and Memberships
Account running the AppManager agent service (netiqmc)	◆ Membership in the Builtin\Administrators group on the Active Directory server ◆ Membership in the local Administrators group on the local computer ◆ Delegation for at least Exchange View-Only permissions
Mailbox server role	◆ Membership in the Exchange Server Administrators and Exchange Recipient Administrators group ◆ Membership in the local Administrators group

4.5.2 Resource Objects

- Exchange_HubTransportServer
- Exchange_MailboxServer

To monitor individual storage groups and mailbox databases, use the Objects tab to select the specific objects to monitor.

4.5.3 Default Schedule

By default, this script runs every 30 minutes.

4.5.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Availability job fails. The default is 5.
Raise event indicating active/ passive cluster state?	Select **Yes** to raise an informational event indicating the current status of the cluster: active or passive. The default is No.
Monitor Exchange 2007 Server Availability	
Mailbox Server Role	
Mailbox Database Availability	
Raise event if mailbox databases are unmounted?	Select **Yes** to raise an event if mailbox databases are unmounted. The default is Yes. When a database is unmounted, the Exchange Server cannot store information in it or read information from it.
Event severity when mailbox databases are unmounted	Set the severity level, from 1 to 40, to indicate the importance of an event in which mailbox databases are unmounted. The default is 15.
Replication Latency	

Raise event if replication latency exceeds threshold?	Select **Yes** to raise an event if replication latency exceeds the threshold you set. The default is Yes.
	
	When this parameter is set to **Yes**, the Extended ESE performance counters in the registry are enabled. The following updates are made automatically in the registry values:
	
	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ESE\ Performance`
	
	`Value Name: Show Advanced Counters`
	
	`Data Type: REG_DWORD`
	
	`Value: 1`

Parameter	How to Set It
Event severity when replication latency threshold exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which replication latency exceeds the threshold you set. The default is 5.
Threshold -- Maximum replication latency	Set the maximum number of milliseconds for which replication latency is allowed before an event is raised. The default is 20000 milliseconds.
Pending Replication Transactions	
Raise event if pending replication transactions exceed threshold?	Select **Yes** to raise an event if the number of pending replication transactions exceeds the threshold you set. The default is Yes.
Event severity when pending replication transactions exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of pending replication transactions exceeds the threshold you set. The default is 5.
Threshold -- Maximum number of pending replication transactions	Set the maximum number of pending replication transactions allowed before an event is raised. The default is 500.
Replication Rate	
Raise event if replication rate exceeds threshold?	Select **Yes** to raise an event if the replication rate exceeds the threshold you set. The default is Yes.
Event severity when replication rate threshold exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the replication rate exceeds the threshold you set. The default is 5.
Threshold -- Maximum replication rate	Enter the maximum number of replications allowed per minute before an event is raised. The default is 500.
Replication Agent	
Raise event if replication agent is not running?	Select **Yes** to raise an event if the replication agent is not running. The default is Yes.
Event severity when replication agent is not running	Set the severity level, from 1 to 40, to indicate the importance of an event in which the replication agent is not running. The default is 5.
File Share Witness	
Raise event if file share witness is unavailable?	Select **Yes** to raise an event if the File Share Witness is unavailable. The default is Yes.
Event severity when file share witness is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which the File Share Witness is unavailable. The default is 15.
Hub Transport Server Role	
Transport Dumpster Availability	
Raise event if transport dumpster is unavailable?	Select **Yes** to raise an event if the Transport Dumpster is unavailable. The default is Yes.
Event severity when transport dumpster is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Transport Dumpster is unavailable. The default is 15.

4.6 BestPracticesAnalyzer

This Knowledge Script is obsolete, although you can continue to use it. Its functionality is provided by the All_BestPracticesAnalyzer Knowledge Script introduced with AppManager for Exchange Server 2007 version 7.3.

****

Use this Knowledge Script to monitor the Windows Event Log for errors and warnings whose source is BPA (Exchange Best Practices Analyzer). This script raises an event if the Knowledge Script job fails or the Windows Event Log contains error and warning messages.

If you are not running the BPA, you can use this script to execute the BPA each time the script runs. If you set the *Execute Best Practices Analyzer during job?* parameter to **Yes**, AppManager runs the BPA at each iteration of the Knowledge Script job. It then stops the BPA and analyzes the Windows Event Log for errors and warnings raised by the BPA.

NOTE: This script may raise duplicate events on computers where multiple Exchange Server 2007 or 2010 roles are installed. These duplicate events are raised because the BPA populates the Windows Event Log with errors and warnings for each role when the error or warning is applicable for the entire Exchange Server 2007 or 2010 organization.

4.6.1 Running the ExBPAcmd.exe Tool Manually

The BPA must be running, launched by you or this script, so that it can submit any errors or warnings to the Windows Event Log. If you are not running the BPA and you clear the *Execute Best Practices Analyzer during job?* parameter, then this Knowledge Script job will not work.

If you do not enable this script to launch the BPA, then run the `ExBPAcmd.exe` tool manually to monitor the Windows Event Log for errors and warnings.

To run the ExBPAcmd.exe tool manually:

1. Open the Exchange Management Shell.
2. Run the following command:

   ```
   $exBPAoutput = . "C:\Program Files\Microsoft\Exchange Server\Bin\ExBPAcmd.exe"
   -p Events:Enable -r "5,$role,$scan_type,Server=<ExchangeServerName>"
   ```

   where `$role` must be replaced by any one of the following values enclosed in quotation marks (“ ”): `Mailbox`, `Gateway`, `Bridgehead`, `ClientAccess`, `ClusterMailbox`

   `$scan_type` must be replaced by any one of the following values enclosed in quotation marks (“ ”): `Health`, `ConnectivityTask`, `Ex2007Readiness`, `Perf`, `Permissions`

   and `<ExchangeServerName>` must be replaced with the name of your Exchange server where you want to run the `ExBPAcmd.exe` tool.
3. Run the following command to display the output of the `ExBPAcmd.exe` tool:

   ```
   Write-Host $exBPAoutput
   ```

   These commands enable the event log register.

4.6.2 Prerequisites

Before running this script, ensure that the following permissions and memberships exist.

Component	Required Permissions and Memberships
Account running the AppManager agent service (netiqmc)	◆ Membership in the Builtin\Administrators group on the Active Directory server ◆ Membership in the local Administrators group on the local computer ◆ Delegation for at least Exchange View-Only permissions
Exchange Best Practice Analyzer tool (for all Exchange Server roles)	◆ Designation as the Domain Administrator, *or* membership in the Builtin\Administrators group on the Active Directory server, for enumerating the Active Directory information and calling the Microsoft Windows Management Instrumentation (WMI) providers on the domain controller and global catalog servers ◆ Membership in the Local Administrators group on each Exchange server for calling the WMI providers and accessing the registry and the metabase ◆ Delegation for at least Exchange View-Only Permissions on the Exchange organization

4.6.3 Resource Objects

- Exchange_ClientAccessServer
- Exchange_EdgeTransportServer
- Exchange_HubTransportServer
- Exchange_MailboxServer

4.6.4 Default Schedule

By default, this script runs every one hour.

4.6.5 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the BestPracticesAnalyzer job fails. The default is 5.
Raise event indicating active/passive cluster state?	Select **Yes** to raise an informational event indicating the current status of the cluster: active or passive. The default is No.
Analyze Exchange Server 2007 Best Practices	

Parameter	How to Set It
Execute Best Practices Analyzer during job?	Select **Yes** to allow AppManager to launch the BPA using a command-line execution of `ExBPACmd.exe` at each iteration of this script. If you are already running the BPA, then clear this option. However, the BPA *must* be running, launched by you or this script, so that it can submit any errors or warnings to the Windows Event Log. The default is Yes.
Type of scan to execute	Select the type of scan the BPA should perform: ◆ **Connectivity Test**. To scan network connections and permissions for the selected Exchange server. ◆ **Exchange 2007 Readiness**. To assess your organization's readiness for Exchange Server 2007. ◆ **Health Check**. To perform a full scan, checking for errors, warnings, and configuration information. This option is selected by default. ◆ **Permission Check**. To ensure that your Exchange Server 2007 deployment has the proper credentials as defined by your organization.
Event for errors raised in Windows Event Log	
Event severity for Windows Event Log errors	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Windows Event Log contains error messages. The default is 10.
Raise event for warnings raised in Windows Event Log?	Select **Yes** to raise an event when the Windows Event Log contains warning messages raised by the BPA. The default is Yes.
Event severity for Windows Event Log warnings	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Windows Event Log contains warning messages raised by the BPA. The default is 20.

4.7 CAS_Activity

Use this Knowledge Script to monitor Client Access server (CAS) services and functions:

- Availability Service activity
- ActiveSync response time and request rate
- Outlook Web Access response time, search time, login rate, and login failures
- Outlook Web Services request rate and current connections
- IMAP4 (Internet Message Access protocol) processing time, current connections, and active SSL connections
- POP3 (Post Office Protocol) processing time, login rate, current connections, and active SSL connections

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see Section 4.43, “Recommended Knowledge Script Group,” on page 162.

NOTE: This Knowledge Script is available only for Exchange Server 2007 and 2010. For Exchange Server 2013, 2016, and 2019, see Section 4.19, “MBS_ClientActivity,” on page 99.

4.7.1 Resource Objects

- Exchange2007_ClientAccessServer
- Exchange2010_ClientAccessServer

4.7.2 Default Schedule

By default, this script runs every 15 minutes.

4.7.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to set it
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CAS_Activity job fails. The default is 5.
Comma separated list of servers for which events should not be raised if CAS services are disabled	Specify a comma separated list of server names for which the event messages should not be raised if the client services are in the disabled state.
Monitor Availability Service Activity	
Event Notification	
Raise event if response time for free/busy requests exceeds threshold?	Select **Yes** to raise an event if the response time for free or busy requests to Microsoft Outlook exceeds the threshold you set. The default is Yes.
Threshold - Maximum free/busy request response time	Set the maximum length of time that Microsoft Outlook can take to respond to free/busy requests before an event is raised. The default is 5000 milliseconds.
Event severity when response time for free/busy requests exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the response time for free/busy requests exceeds the threshold. The default is 15.
Data Collection	
Collect data for free/busy request response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the length of response time during the monitoring interval. The default is No.
Monitor ActiveSync Activity	
Monitor ActiveSync Response Time	
Event Notification	
Raise event if ActiveSync response time exceeds threshold?	Select **Yes** to raise an event if the response time for ActiveSync exceeds the threshold you set. The default is Yes.

Parameter	How to set it
Threshold - Maximum response time	Set the maximum length of time that ActiveSync can take to respond to requests before an event is raised. The default is 100 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which ActiveSync response time exceeds the threshold. The default is 15.
Data Collection	
Collect data for response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the length of response time during the monitoring interval. The default is No.
Monitor ActiveSync Request Rate	
Event Notification	
Raise event if ActiveSync request rate exceeds threshold?	Select **Yes** to raise an event if the rate of synchronization requests to ActiveSync exceeds the threshold you set. The default is Yes.
Threshold - Maximum request rate	Set the maximum number of requests that can occur per second before an event is raised. The default is 10 synchronization requests per second.
Event severity when request rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ActiveSync request rate exceeds the threshold. The default is 15.
Data Collection	
Collect data for request rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the rate of synchronization requests during the monitoring interval. The default is No.
Monitor Outlook Web Access Activity	
Monitor Outlook Web Access Response Time	
Event Notification	
Raise event if Outlook Web Access response time exceeds threshold?	Select **Yes** to raise an event if the response time for Outlook Web Access (OWA) exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time	Set the maximum amount of time that it can take for OWA to respond to requests before an event is raised. The default is 100 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which OWA response time exceeds the threshold. The default is 15.
Data Collection	
Collect data for response time?	Select **Yes** to collect .data for charts and reports. When enabled, data collection returns the length of response time during the monitoring interval. The default is No.

Parameter	How to set it
Monitor Outlook Web Access Search Time	
Event Notification	
Raise event if Outlook Web Access search time exceeds threshold?	Select **Yes** to raise an event if Outlook Web Access (OWA) search time exceeds the threshold. The default is Yes. The OWA search feature allows users to find items in a mailbox.
Threshold - Maximum search time	Set the maximum length of time that OWA can spend performing a search before an event is raised. The default is 100 milliseconds.
Event severity when search time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which OWA search time exceeds the threshold. The default is 15.
Data Collection	
Collect data for search time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the length of search time during the monitoring interval. The default is No.
Monitor Outlook Web Access Login Rate	
Event Notification	
Raise event if login rate exceeds threshold?	Select **Yes** to raise an event if the rate at which users log in to Outlook Web Access (OWA) exceeds the threshold. The default is Yes.
Threshold - Maximum login rate	Set the maximum rate at which users can log in to OWA before an event is raised. The default is 10 logins per second.
Event severity when login rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the rate at which users log in to OWA exceeds the threshold. The default is 15.
Data Collection	
Collect data for login rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the OWA log in rate for the monitoring interval. The default is No.
Monitor Outlook Web Access Login Failures	
Event Notification	
Raise event if login failures exceed threshold?	Select **Yes** to raise an event if the failures for logging in to Outlook Web Access (OWA), expressed as a percentage of all login attempts, exceed the threshold. The default is Yes.
Threshold - Maximum percentage of login failures	Set the maximum percentage of OWA login failures that can occur before an event is raised. The default is 10%.

Parameter	How to set it
Event severity when login failures exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which percentage of OWA login failures exceeds the threshold. The default is 15.
Data Collection	
Collect data for login failures?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of OWA login failures for the monitoring interval. The default is No.
Monitor Outlook Web Services Activity	
Monitor Outlook Web Services Request Rate	
Event Notification	
Raise event if Outlook Web Services request rate exceeds threshold?	Select **Yes** to raise an event if the rate of requests to Outlook Web Services exceeds the threshold you set. The default is Yes.
Threshold - Maximum request rate	Set the maximum number of requests that can occur per second before an event is raised. The default is 10 requests per second.
Event severity when request rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the rate of requests to Outlook Web Services exceeds the threshold. The default is 15.
Data Collection	
Collect data for request rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the rate of requests during the monitoring interval. The default is No.
Monitor Outlook Web Services Current Connections	
Event Notification	
Raise event if number of current connections exceeds threshold?	Select **Yes** to raise an event if the number of connections established with Outlook Web Services exceeds the threshold you set. The default is Yes. By knowing the number of current connections, you can determine user load for Outlook Web Services
Threshold - Maximum number of current connections	Set the maximum number of connections to Outlook Web Services that can be established before an event is raised. The default is 25 connections.
Event severity when number of current connections exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of connections established with Outlook Web Services exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of current connections?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of connections established during the monitoring interval. The default is No.

Parameter	How to set it
Monitor IMAP4 Activity	
Monitor IMAP4 Command Processing Time	
Event Notification	
Raise event if command processing time exceeds threshold?	Select **Yes** to raise an event if the amount of processing time for IMAP4 commands exceeds the threshold you set. The default is Yes.
Threshold - Maximum command processing time	Set the maximum amount of time that can be spent processing IMAP4 commands before an event is raised. The default is 100 milliseconds.
Event severity when command processing time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the amount of processing time for IMAP4 commands exceeds the threshold. The default is 15.
Data Collection	
Collect data for command processing time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the amount of processing time spent during the monitoring interval. The default is No.
Monitor IMAP4 Connections Rate	
Event Notification	
Raise event if connections rate exceeds threshold?	Select **Yes** to raise an event if the number of IMAP4 connections to your Exchange server exceeds the threshold you set. The default is Yes.
Threshold - Maximum connections rate	Set the maximum number of IMAP4 connection requests that can occur per second before an event is raised. The default is 10 connections per second.
Event severity when connections rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of IMAP4 connection requests exceeds the threshold. The default is 15.
Data Collection	
Collect data for connections rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of IMAP4 connection requests for the monitoring intervals. The default is No.
Monitor IMAP4 Current Connections	
Event Notification	
Raise event if number of current connections exceeds threshold?	Select **Yes** to raise an event if the number of current IMAP4 connections to your Exchange server exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of current connections	Set the maximum number of IMAP4 connections that can be established before an event is raised. The default is 10 connections.

Parameter	How to set it
Event severity when number of current connections exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of IMAP4 connections exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of current connections?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of IMAP4 connections established during the monitoring interval. The default is No.
Monitor IMAP4 Active SSL Connections	
Event Notification	
Raise event if number of active SSL connections exceeds threshold?	Select **Yes** to raise an event if the number of current IMAP4 connections to your Exchange server over SSL (Secure Sockets Layer) exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of active SSL connections	Set the maximum number of IMAP4 connections that can be established over SSL before an event is raised. The default is 50 connections.
Event severity when number of active SSL connections exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of IMAP4 SSL connections exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of active SSL connections?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of IMAP4 SSL connections established during the monitoring interval. The default is No.
Monitor POP3 Activity	
Monitor POP3 Command Processing Time	
Event Notification	
Raise event if command processing time exceeds threshold?	Select **Yes** to raise an event if the amount of processing time for POP3 commands exceeds the threshold you set. The default is Yes.
Threshold - Maximum command processing time	Set the maximum amount of time that can be spent processing POP3 commands before an event is raised. The default is 10 milliseconds.
Event severity when command processing time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the amount of processing time for POP3 commands exceeds the threshold. The default is 15.
Data Collection	
Collect data for command processing time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the amount of processing time spent during the monitoring interval. The default is No.

Parameter	How to set it
Monitor POP3 Connections Rate	
Event Notification	
Raise event if connections rate exceeds threshold?	Select **Yes** to raise an event if the number of POP3 connections to your Exchange server exceeds the threshold you set. The default is Yes.
Threshold - Maximum connections rate	Set the maximum number of POP3 connection requests that can occur per second before an event is raised. The default is 10 connections per second.
Event severity when connections rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of POP3 connection requests exceeds the threshold. The default is 15.
Data Collection	
Collect data for connections rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of POP3 connection requests for the monitoring intervals. The default is No.
Monitor Current POP3 Current Connections	
Event Notification	
Raise event if number of current connections exceeds threshold?	Select **Yes** to raise an event if the number of current POP3 connections to your Exchange server exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of current connections	Set the maximum number of POP3 connections that can be established before an event is raised. The default is 10 connections.
Event severity when number of current connections exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of POP3 connections that are currently established exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of current connections?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of POP3 connections established during the monitoring interval. The default is No.
Monitor POP3 Active SSL Connections	
Event Notification	
Raise event if number of active SSL connections exceeds threshold?	Select **Yes** to raise an event if the number of current POP3 connections to your Exchange server over SSL (Secure Sockets Layer) exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of active SSL connections	Set the maximum number of POP3 connections that can be established over SSL before an event is raised. The default is 25 connections.

Parameter	How to set it
Event severity when number of active SSL connections exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of POP3 SSL connections exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of active SSL connections	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of POP3 SSL connections established during the monitoring interval. The default is No.

4.8 CAS_Connectivity

Use this Knowledge Script to monitor the connectivity of Client Access server (CAS) services on Exchange Server 2007 and 2010: ActiveSync, Outlook Web Access, Outlook Web services, and the Autodiscover service. This script raises an event when a connectivity test fails and when response time exceeds the threshold you set.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see Section 4.43, “Recommended Knowledge Script Group,” on page 162.

NOTE: This Knowledge Script is available only for Exchange Server 2007 and 2010. For Exchange Server 2013, 2016, and 2019, see Section 4.20, “MBS_ClientConnectivity,” on page 106.

4.8.1 Configuring Security Manager to Test Outlook Web Access Connectivity

Before you can run the CAS_Connectivity Knowledge Script to test Outlook Web Access connectivity using a custom URL, you need to configure Security Manager for the Client Access server where the job will run. You do not need to configure Security Manager if you are using an internal or external URL.

To configure AppManager Security Manager to test connectivity:

1. On the Extensions menu in the Operator Console, click **Security Manager**.
2. Select the Client Access server you want to test.
3. On the Custom tab, click **Add**.
4. In the Label field, type **Exchange2007**.
5. In the Sub-label field, type **MailboxCredentials**
6. In the Value 1 field, specify the mailbox name, which is also referred to as the user account, to be used in the test.
7. In the Value 2 field, specify the password for the mailbox.
8. Leave the Value 3 field blank.
9. Select **Extended application support** to encrypt the password when it is stored in the repository.
10. Click **OK**.
11. Click **Apply** to save the Security Manager settings.

4.8.2 Running CAS_Connectivity on a Client Access Server

When you run the CAS_Connectivity Knowledge Script on a Client Access server, the script automatically creates a CAS test user mailbox on each Mailbox server in the Exchange deployment if those mailboxes do not already exist. In an Exchange deployment containing Exchange 2007 and Exchange 2010 servers, if you run the CAS_Connectivity script on an Exchange 2010 Client Access Server, the script will not be able to create the mailboxes on Exchange 2007 Mailbox Servers, and AppManager raises an error event about the problem. This is due to the issue that Microsoft does not support creating mailboxes across different version types. To resolve, you must manually create the CAS test user mailboxes on the Exchange 2007 Mailbox Servers.

To create CAS test user mailboxes on an Exchange 2007 Mailbox Server:

1. Log in to one of the Exchange 2007 Mailbox Servers and open the Exchange Management Shell.
2. Change directories to the `Scripts` directory under the Microsoft Exchange installation directory.
3. Run the following command:
   `Get-MailboxServer | .\New-TestCasConnectivityUser.ps1`.
4. Follow the on-screen instructions to create the CAS test user mailbox on each Mailbox server.

4.8.3 Resource Objects

- Exchange2007_ClientAccessServer
- Exchange2010_ClientAccessServer

4.8.4 Default Schedule

By default, this script runs every 30 minutes.

4.8.5 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Communicate only with Exchange Servers in the local domain?	Select **Yes** to test only Exchange Servers in the same domain as the server on which you run the CAS_Connectivity job. When this option is unselected, certain tests for the Client Access server attempt to contact *all* Mailbox servers in your organization. These tests will fail if the Exchange accounts in one domain do not have access to other domains. Leave this option unselected if you specify a Mailbox server in the *Mailbox server to be used for connectivity tests* parameter.
Ignore these Mailbox servers when testing CAS to MBS communications	Provide a comma-separated list of the hostnames of the Mailbox servers that you want to exclude from connectivity testing between the Client Access server and the Mailbox server. Leave this option blank if you specify a Mailbox server in the *Mailbox server to be used for connectivity tests* parameter.

Parameter	How to Set It
Mailbox server to be used for connectivity tests	By default, the CAS_Connectivity job tests connectivity to all Mailbox servers. Use this parameter to enable testing to one Mailbox server. Enter the hostname of the computer that hosts the Mailbox server with which you want to check connectivity. The hostname need not be fully qualified unless DNS lookup does not resolve the simple name. If you monitor Outlook web access connectivity and specify a custom URL, that custom URL will be used to test Outlook web access connectivity instead of this mailbox server.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CAS_Connectivity job fails. The default is 5.
Connectivity Test User Configuration	
Use alternate test mailbox configured in Security Manager?	Select **Yes** to use the test mailbox that you have specified in the Security Manager. The default is No.
Create default test mailbox automatically?	Select **Yes** to create a default test mailbox automatically. The default is Yes.
Create non-existent test mailboxes every N job iterations (specify N)	Specify the number of job iterations for which the non-existent test mailboxes will be created on the Mailbox server. The default is 1.
Monitor ActiveSync Connectivity	
Event Notification	
Raise event if ActiveSync connectivity test fails?	Select **Yes** to raise an event if AppManager cannot check connectivity to ActiveSync. The default is Yes.
Event severity when ActiveSync connectivity test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot check connectivity to ActiveSync. The default is 5.
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes to connect to ActiveSync exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time for connectivity test	Set how long AppManager should wait for connectivity with ActiveSync before raising an event. The default is 10000 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time it takes to connect to ActiveSync exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for ActiveSync response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average response time for connecting to ActiveSync. The default is No.
Monitor Outlook Web Access Connectivity	
Allow unsecure (http) communication?	Select **Yes** if you want to allow unsecure communication using `http` instead of `https` when testing the Web access connectivity. The default is No.

Parameter	How to Set It
URL type to be used for connectivity test	Select whether you want to use an internal URL, an external URL, or a custom URL for the connectivity test. If you select a custom URL, configure the credentials in Security Manager before you run a job. The default type is Internal.
Custom URL to be used for connectivity test	Specify the URL you want to use for the connectivity test. The default is blank.
Event Notification	
Raise event if Outlook Web Access connectivity test fails?	Select **Yes** to raise an event if AppManager cannot check connectivity to Outlook Web Access (OWA). The default is Yes.
Event severity when Outlook Web Access connectivity test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot check connectivity to OWA. The default is 5.
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes to connect to Outlook Web Access exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time for connectivity test	Set how long AppManager should wait to confirm connectivity with OWA before raising an event. The default is 10000 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time it takes to connect to OWA exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for Outlook Web Access response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average response time for connecting to OWA. The default is No.
Monitor Outlook Web Services Connectivity	
Use SSL (HTTPS) for connectivity test?	Select **Yes** to use Secure Socket Layer (SSL) to test connectivity to Outlook Web services. The default is No. If you select **Yes**, AppManager will use only SSL to test connectivity. If you clear the option, AppManager will first use SSL to test connectivity. If that attempt fails, AppManager will then try to test connectivity without using SSL.
Event Notification	
Raise event if Outlook Web services connectivity test fails?	Select **Yes** to raise an event if AppManager cannot check connectivity to Outlook Web services. The default is Yes.
Event severity when Outlook Web services connectivity test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot check connectivity to Outlook Web services. The default is 5.
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes to connect to Outlook Web services exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time for connectivity test	Set how long AppManager should wait to confirm connectivity with Outlook Web services before raising an event. The default is 10000 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time taken for testing connectivity to Outlook Web services exceeds the threshold that you set. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for Outlook Web services response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average response time for connecting to Outlook Web services. The default is No.
Monitor Autodiscover Service Connectivity	
Event Notification	
Raise event if Autodiscover service connectivity test fails?	Select **Yes** to raise an event if AppManager cannot check connectivity to the Autodiscover service. The default is Yes. The Autodiscover service allows Outlook 2007 clients and mobile devices to be recognized when they connect to the Client Access server.
Event severity when Autodiscover service connectivity test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot check connectivity to the Autodiscover service. The default is 5.
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes to connect to the Autodiscover service exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time for connectivity test	Set how long AppManager should wait to confirm connectivity with the Autodiscover service before raising an event. The default is 10000 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time taken for testing connectivity to the Autodiscover service exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for Autodiscover service response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average response time for connecting to the Autodiscover service. The default is No.

4.9 CAS_OABAvailability

Use this Knowledge Script to monitor the availability of offline address books (OABs) for a Client Access server. This script raises an event if OABs cannot be downloaded.

This Knowledge Script monitors the offline address books only if they are hosted in a virtual directory. If they are in a public folder, this Knowledge Script does not monitor those.

NOTE: This script is currently not supported for use with Exchange Server 2013, 2016, and 2019.

4.9.1 Resource Objects

- Exchang2007_ClientAccessServer
- Exchange2010_ClientAccessServer

4.9.2 Default Schedule

By default, this script runs every 15 minutes.

4.9.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Communicate only with Exchange Servers in the local domain?	Select **Yes** to test only Exchange Servers in the same domain as the server on which you run the CAS_OABAvailability job. When this option is unselected, certain tests for the Client Access server attempt to contact *all* Mailbox servers in your organization. These tests will fail if the Exchange accounts in one domain do not have access to other domains. Leave this option unselected if you specify a Mailbox server in the *Mailbox server hosting offline address books to be accessed* parameter.
Ignore these Mailbox servers when testing CAS to MBS communications	Provide a comma-separated list of the host names of the Mailbox servers that you want to exclude from availability testing between the Client Access server and the Mailbox server. Leave this option blank if you specify a Mailbox server in the *Mailbox server hosting offline address books to be accessed* parameter.
Mailbox server hosting offline address books to be accessed	By default, the OABAvailability job tests connectivity to all Mailbox servers. Use this parameter to enable testing to one Mailbox server. Enter the hostname of the Mailbox server computer that hosts the OABs you want to monitor. The hostname need not be fully qualified unless DNS lookup does not resolve the simple name.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OABAvailability job fails. The default is 5.
Monitor Offline Address Book Availability	
Event Notification	
Raise event if offline address books cannot be downloaded?	Select **Yes** to raise an event if the Client Access server's offline address books cannot be downloaded. The default is Yes.
Event severity when offline address books cannot be downloaded	Set the severity level, from 1 to 40, to indicate the importance of an event in which offline address books cannot be downloaded. The default is 5.

4.10 CAS_PublicFolderAvailability

Use this Knowledge Script to monitor the accessibility of public folders on a Client Access server. This script raises an event when public folders are inaccessible.

4.10.1 Resource Objects

- Exchange2007_ClientAccessServer
- Exchange2010_ClientAccessServer

- Exchange2013_ClientAccessServer
- Exchange2016_ClientAccessServer
- Exchange2019_ClientAccessServer

4.10.2 Default Schedule

By default, this script runs every 15 minutes.

4.10.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Communicate only with Exchange Servers in the local domain?	Select **Yes** to test only Exchange Servers in the same domain as the server on which you run the CAS_PublicFolderAvailability job. When this option is unselected, certain tests for the Client Access server attempt to contact *all* Mailbox servers in your organization. These tests will fail if the Exchange accounts in one domain do not have access to other domains. Leave this option unselected if you specify a Mailbox server in the *Mailbox server hosting public folders to be accessed* parameter.
Ignore these Mailbox servers when testing CAS to MBS communications	Provide a comma-separated list of the hostnames of the Mailbox servers that you want to exclude from availability testing between the Client Access server and the Mailbox server. Leave this option blank if you specify a Mailbox server in the *Mailbox server hosting public folders to be accessed* parameter.
Mailbox server hosting public folders to be accessed	By default, the CAS_PublicFolderAvailability job tests connectivity to all Mailbox servers. Use this parameter to enable testing to one Mailbox server. Enter the hostname of the Mailbox server computer that hosts the public folders you want to monitor. The hostname need not be fully qualified unless DNS lookup does not resolve the simple name.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CAS_PublicFolderAvailability job fails. The default is 5.
Monitor Public Folder Availability	
Event Notification	
Raise event if public folders are inaccessible?	Select **Yes** to raise an event if the public folders on the Client Access server are inaccessible. The default is Yes.
Event severity when public folders are inaccessible	Set the severity level, from 1 to 40, to indicate the importance of an event in which public folders on the Client Access server are inaccessible. The default is 5.

4.11 DataCollection

This Knowledge Script is obsolete, although you can continue to use it. Its functionality is distributed among the following Knowledge Scripts introduced with AppManager for Exchange Server 2007 version 7.3.

- CAS_Activity
- ETS_ExternalMail
- HTS_SendersAndRecipients
- HTS_TransportDumpster
- MBS_MailboxUsage
- MBS_MailboxAccessibility

****

Use this Knowledge Script to collect Exchange Server 2007 performance data for reporting and trend analysis. This script raises an event if the DataCollection job fails.

4.11.1 Prerequisites

Before running this script, ensure that the AppManager agent service (`netiqmc`) is a member of the following security groups on the specified Exchange Server 2007 role:

Exchange Server 2007 Role	Membership Group
Client Access server role	The local Administrators group on the Client Access server
Mailbox server role	◆ Exchange Server Administrators group ◆ Exchange Recipient Administrators group ◆ Local Administrators group
Hub Transport server role	◆ Exchange Server Administrators group ◆ Local Administrators group
Edge Transport server role	◆ Exchange Server Administrators group ◆ Local Administrators group

4.11.2 Resource Objects

- Exchange_ServerIcon
- Exchange_ClientAccessServer
- Exchange_EdgeTransportServer
- Exchange_HubTransportServer
- Exchange_MailboxServer

To monitor individual storage groups and mailbox databases, use the Objects tab to select the specific objects to monitor.

4.11.3 Default Schedule

The default schedule is **Every 30 minutes**.

4.11.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DataCollection job fails. The default is 5.
Raise event indicating active/passive cluster state?	Select **Yes** to raise an informational event indicating the current status of the cluster: active or passive. The default is No.
Collect Exchange Server 2007 Data	
Client Access Server Role	
Collect data for Outlook Web Access activity?	Select **Yes** to collect data related to Outlook Web Access (OWA) activity. When enabled, data collection returns the following data streams: ◆ Logons per second ◆ Store logon failure (%) ◆ Current users ◆ Requests per second ◆ Failed requests per second ◆ Average response time (ms) The data in these data streams is collected from the `MSExchange OWA` performance counter category.
Collect data for IMAP4 activity?	Select **Yes** to collect data related to IMAP4 activity. When enabled, data collection returns the following data streams: ◆ Logins per second ◆ Current connections ◆ Active SSL connections ◆ Average command processing time (ms) These data streams are not available if the IMAP4 service is not running. The data in these data streams is collected from the `MSExchangeImap4` performance counter category.

Parameter	How to Set It
Collect data for POP3 activity?	Select **Yes** to collect data related to POP3 activity. When enabled, data collection returns the following data streams: ◆ Current connections ◆ Active SSL connections ◆ Average command processing time (ms) These data streams are not available if the POP3 service is not running. The data in these data streams is collected from the `MSExchangePop3` performance counter category.
Edge Transport Server Role	
Collect data for recipients and domains of outgoing mail?	Select **Yes** to collect data related to outgoing e-mail domains and recipients. When enabled, data collection returns the following data streams: ◆ Average number of messages sent to top *n* recipient domains ◆ Average size (bytes) of total messages sent to top *n* recipient domains Use the *Number of top recipients and domains used in data* parameter to determine the value of n. AppManager uses the `Get-MessageTrackingLog` cmdlet to determine the top recipient domains, based on message count and total message size.
Number of top recipients and domains used in data	Set the number of recipients and domains you want to include in the data streams generated by the *Collect data for recipients and domains of outgoing mail?* parameter. The default is 10.
Collect data for domains sending incoming mail?	Select **Yes** to collect data related to external domains that send incoming e-mail. When enabled, data collection returns the following data streams: ◆ Average number of messages sent by top *n* external domains ◆ Average size (bytes) of messages sent by top *n* external domains Use the *Number of top domains used in data* parameter to determine the value of *n*. AppManager uses the `Get-MessageTrackingLog` cmdlet to determine the top sending domains, based on message count and total message size.
Number of top domains used in data	Set the number of domains you want to include in the data streams generated by the *Collect data for domains sending incoming mail?* parameter. The default is 10.
Collect data for senders of outgoing mail?	Select **Yes** to collect data related to senders of e-mail to external addresses. When enabled, data collection returns the following data streams: ◆ Average number of external messages sent by top *n* senders ◆ Average size (bytes) of total external messages sent by top *n* senders Use the *Number of top senders used in data* parameter to determine the value of *n*. AppManager uses the `Get-MessageTrackingLog` cmdlet to determine the top senders of e-mail, based on message count and total message size.

Parameter	How to Set It
Number of top senders used in data	Set the number of senders you want to include in the data streams generated by the *Collect data for senders of outgoing mail?* parameter. The default is 10.
Collect data for recipients of incoming mail?	Select **Yes** to collect data related to recipients of e-mail from external addresses. When enabled, data collection returns the following data streams: ◆ Average number of external messages received by top *n* recipients ◆ Average size (bytes) of total external messages received by top *n* recipients Use the *Number of top recipients used in data* parameter to determine the value of *n*. AppManager uses the `Get-MessageTrackingLog` cmdlet to determine the top recipients of e-mail, based on message count and total message size.
Number of top recipients used in data	Set the number of recipients you want to include in the data streams generated by the *Collect data for recipients of incoming mail?* parameter. The default is 10.
Hub Transport Server Role	
Collect data for SMTP send and receive activity?	Select **Yes** to collect data related to SMTP activity. When enabled, data collection returns the following data streams: ◆ Messages sent per second ◆ Messages received per second ◆ Message bytes sent per second ◆ Message bytes received per second ◆ Current outbound connections ◆ Current inbound connections ◆ Average messages sent per connection ◆ Average messages received per connection The data in these data streams is collected from the `MSExchangeTransportSmtpReceived` and `MSExchangeTransportSmtpSend` performance counter categories.
Collect data for transport dumpster queue usage?	Select **Yes** to collect data for transport dumpster queue activity. When enabled, data collection returns the number of e-mail in the dumpster at a given instance and also the space allocated for the transport dumpster.
Collect data for items queued for delivery?	Select **Yes** to collect data for MTA queue activity. When enabled, data collection returns the number of messages queued for delivery
Collect data for recipients of internal mail?	Select **Yes** to collect data related to recipients of internal e-mail. When enabled, data collection returns the following data streams: ◆ Average number of messages for top *n* recipients ◆ Average size (bytes) of messages for top *n* recipients Use the *Number of top recipients used in data* parameter to determine the value of *n*. AppManager uses the `Get-MessageTrackingLog` cmdlet to determine the top recipients of internal e-mail, based on message count and total message size.

Parameter	How to Set It
Number of top recipients used in data	Set the number of internal e-mail recipients you want to include in the data streams generated by the *Collect data for recipients of internal mail?* parameter. The default is 10.
Collect data for senders of internal mail?	Select **Yes** to collect data related to senders of internal mails. When enabled, data collection returns the following data streams: ◆ Average number of messages for top *n* senders ◆ Average size (bytes) of messages for top *n* senders Use the *Number of top senders used in data* parameter to determine the value of *n*. AppManager uses the `Get-MessageTrackingLog` cmdlet to determine the top senders of internal e-mail, based on message count and total message size.
Number of top senders used in data	Set the number of internal e-mail senders you want to include in the data streams generated by the *Collect data for senders of internal mail?* parameter. The default is 10.
Mailbox Server Role	
Collect data for mailbox size and message count?	Select **Yes** to collect data related to mailbox size and message counts. When enabled, data collection returns the following data streams: ◆ Average number of mailboxes in the *n* largest mailbox databases ◆ Average number of messages in *n* largest mailboxes ◆ Average size (KB) of the *n* largest mailboxes ◆ Average size (MB) of the *n* largest mailbox databases Use the *Number of top mailboxes and mailbox databases used in data* parameter to determine the value of *n*. AppManager uses Exchange cmdlets to determine the largest mailboxes and mailbox databases, based on number and size of mailboxes and messages.
Number of top mailboxes and mailbox databases used in data	Set the number of mailboxes and mailbox databases you want to include in the data streams generated by the *Collect data for mailbox size and message count?* parameter. The default is 10.
Collect data for RPC activity of information store?	Select **Yes** to collect data related to RPC (Remote Procedure Call) activity for the information store. When enabled, data collection returns the following data streams: ◆ RPC packets per second ◆ RPC slow packets ◆ RPC average latency (ms) ◆ RPC operations per second ◆ RPC requests The data in these data streams is collected from the `MSExchangeIS` performance counter category.

Parameter	How to Set It
Collect data for message transmission activity?	Select **Yes** to collect data related to message transmissions. When enabled, data collection returns the following data streams: ◆ Messages in the database receive queue ◆ Average message delivery time (ms) ◆ Messages delivered per second ◆ Messages sent per second The data in these data streams is collected from the `MSExchangeIS` Mailbox performance counter category.
Collect data for disk activity?	Select **Yes** to collect data related to logical disk activity. When enabled, data collection returns the following data streams: ◆ Disk time (percentage of time that the logical disk is being accessed) ◆ Disk read time (percentage of time that the logical disk is being read) ◆ Disk write time (percentage of time that the logical disk is being written to) ◆ Average disk queue length (average number of requests in queue) The data in these data streams is collected from the `LogicalDisk` performance counter category.
Collect data for copy and replay queue length?	Select **Yes** to collect data for copy and replay queue length. When enabled, data collection returns the following data streams: ◆ Copy queue length ◆ Replay queue length The data in these data streams is collected per storage group. The storage group has to be enabled with Local Continuous Replication (LCR) or Cluster Continuous Replication (CCR) or both.
Collect data for file share witness usage on two node CCR setup?	Select **Yes** to collect data for file share witness usage on a two node CCR setup. When enabled, data collection returns data for the following data streams: ◆ MNSFileShareCheckInterval ◆ MNSFileShareDelay ◆ MNSFileShareRatio

4.12 ETS_ExternalMail

Use this Knowledge Script to monitor e-mail sent to and from your Exchange environment. This script raises an event when average mail volume for recipients, recipient domains, senders, and sending domains exceeds the threshold you set. You select whether mail volume is measured by number of messages or total size of messages in MB.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see Section 4.43, “Recommended Knowledge Script Group,” on page 162.

4.12.1 Resource Objects

- Exchange2007_EdgeTransportServer
- Exchange2010_EdgeTransportServer

4.12.2 Default Schedule

By default, this script runs daily.

4.12.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Measure mail volume by message count or total message size	Select how this script measures the volume of mail sent to and from your Exchange environment. Choose from **Message count** or **Total message size**. Total message size is measured in MB.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ETS_ExternalMail job fails. The default is 5.
Monitor Recipient Domains of Outgoing Mail	
Number of top recipient domains of outgoing mail	Set the top *n* recipient domains to be monitored for average mail volume. The default is 10 domains, the minimum is 0, and the maximum is 2147483647. To monitor all recipient domains for average mail volume, enter 0.
Event Notification	
Raise event if average mail volume for top recipient domains exceeds threshold?	Select **Yes** to raise an event if the average mail volume for the top *n* recipient domains exceeds the threshold you set. The default is Yes.
Threshold - Maximum average mail volume for top recipient domains	Set the maximum value that average mail volume can attain before an event is raised. The default is 1000.
Event severity when average mail volume for top recipient domains exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average mail volume for the top *n* recipient domains exceeds the threshold. The default is 15.
Data Collection	
Collect data for average mail volume for top recipient domains?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average mail volume for the top *n* recipient domains during the monitoring interval. The default is Yes.
Monitor Sending Domains of Incoming Mail	
Number of top sending domains of incoming mail	Set the top *n* sending domains to be monitored for average mail volume. The default is 10 domains, the minimum is 0, and the maximum is 2147483647. To monitor all domains for average mail volume, enter 0.

Parameter	How to Set It
Event Notification	
Raise event if average mail volume for top sending domains exceeds threshold?	Select **Yes** to raise an event if the average mail volume for the top *n* sending domains exceeds the threshold you set. The default is Yes.
Threshold - Maximum average mail volume for top sending domains	Set the maximum value that average mail volume can attain before an event is raised. The default is 1000.
Event severity when average mail volume for top sending domains exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average mail volume for the top *n* sending domains exceeds the threshold. The default is 15.
Data Collection	
Collect data for average mail volume for top sending domains?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average mail volume for the top *n* sending domains during the monitoring interval. The default is Yes.
Monitor Senders of Outgoing Mail	
Number of top senders of outgoing mail	Set the top *n* senders of mail to be monitored for average mail volume. The default is 10 senders, the minimum is 0, and the maximum is 2147483647. To monitor all senders for average mail volume, enter 0.
Event Notification	
Raise event if average mail volume for top senders of outgoing mail exceeds threshold?	Select **Yes** to raise an event if the average mail volume for the top *n* senders of mail exceeds the threshold you set. The default is Yes.
Threshold - Maximum average mail volume for top senders of outgoing mail	Set the maximum value that average mail volume can attain before an event is raised. The default is 1000.
Event severity when average mail volume for top senders of outgoing mail exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average mail volume for the top *n* senders of mail exceeds the threshold. The default is 15.
Data Collection	
Collect data for average mail volume for top senders of outgoing mail?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average mail volume for the top *n* senders of mail during the monitoring interval. The default is Yes.
Monitor Recipients of Incoming Mail	
Number of top recipients of incoming mail	Set the top *n* recipients of mail to be monitored for average mail volume. The default is 10 recipients, the minimum is 0, and the maximum is 2147483647. To monitor all recipients for average mail volume, enter 0.
Event Notification	
Raise event if average mail volume for top recipients of incoming mail exceeds threshold?	Select **Yes** to raise an event if the average mail volume for the top *n* recipients of mail exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum average mail volume for top recipients of incoming mail	Set the maximum value that average mail volume can attain before an event is raised. The default is 1000.
Event severity when average mail volume for top recipients of incoming mail exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average mail volume for the top *n* recipients of mail exceeds the threshold. The default is 15.
Data Collection	
Collect data for average mail volume for top recipients of incoming mail?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average mail volume for the top *n* recipients of mail during the monitoring interval. The default is Yes.

4.13 ETS_MessageHygiene

Use this Knowledge Script to monitor Edge Transport server message hygiene functions: whether the anti-spam update service is running, the total number of messages that have been filtered as spam, and the number of messages that have been filtered as spam from any one user. You determine which content filter to monitor.

4.13.1 Resource Objects

- Exchange2007_EdgeTransportServer
- Exchange2010_EdgeTransportServer

4.13.2 Default Schedule

By default, this script runs every hour.

4.13.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ETS_MessageHygiene job fails. The default is 5.
Monitor Anti-Spam Update Service	
Event Notification	
Raise event if anti-spam update service is not running?	Select **Yes** to raise an event if the anti-spam update service is not running. The default is Yes. The anti-spam update service provides daily updates to your content filter.

Parameter	How to Set It
Event severity when anti-spam update service is not running	Set the severity level, from 1 to 40, to indicate the importance of an event in which the anti-spam update service is not running. The default is 15.
Start anti-spam update service if not running?	Select **Yes** to start the anti-spam update service if it is not running.The default is Yes.
Threshold - Timeout for anti-spam update service to start	Set the number of seconds that AppManager should wait for the anti-spam update service to start before raising an event. The default is 60 seconds.
Raise event if anti-spam update service fails to start?	Select **Yes** to raise an event if AppManager cannot start the anti-spam update service. The default is Yes.
Event severity when anti-spam update service fail to start	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot start the anti-spam service. The default is 5.
Monitor Total Messages Filtered	
Include only those messages filtered for these reasons	Provide a comma-separated list of the names of the content filters whose activity you want to monitor. The names do not need to be case-sensitive. One of the many fields in a message is a field titled “Reason.” The content of the Reason field is the filter name you provide in this parameter. Possible filter names are `SCLAtORAboveDeleteThreshold`, `ACLAtOrAboveRejectThreshold`, `BlockListProvide`, and `LocalBlockList`. To monitor all messages, leave this parameter blank. **NOTE:** Quotation marks (“) are not supported in this field. This script returns an error if you enter quotation marks as part of a content filter name.
Event Notification	
Raise event if number of filtered messages exceeds threshold?	Select **Yes** to raise an event if the number of filtered messages from all users exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of filtered messages	Set the maximum number of messages that can be filtered for the reason you specified in *Include only those messages filtered for these reasons*. AppManager raises an event if the number of messages exceeds the threshold. The default is 1000.
Event severity when number of filtered messages exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of filtered messages exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of filtered messages?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages filtered for the reason you specified in *Include only those messages filtered for these reasons*. The default is No.
Monitor Worst Offenders	

Parameter	How to Set It
Include only those messages filtered for these reasons	Provide a comma-separated list of the names of the content filters whose activity you want to monitor. The names in the list do not need to be case-sensitive. One of the many fields in a message is a field titled “Reason.” The content of the Reason field is the filter name you provide in this parameter. To monitor all messages, leave this parameter blank. **NOTE:** Quotation marks (“) are not supported in this field. This script returns an error if you enter quotation marks as part of a content filter name.
Maximum number of worst offenders to display	Set the maximum number of worst-offending users to include in an event. These offenders will have sent e-mail that has been filtered as spam for the reasons you indicated in *Include only those messages filtered for these reasons*. The default is 10.
Event Notification	
Raise event if number of filtered messages received from a user exceeds threshold?	Select **Yes** to raise an event if the number of filtered messages from any one user exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of filtered messages received from a user	Set the maximum number of messages that can be filtered for the reason you specified in *Include only those messages filtered for this reason*. AppManager raises an event if the number of messages from one user exceeds the threshold. The default is 100.
Event severity when number of filtered messages received from a user exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of filtered messages from any one user exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of filtered messages received from worst offenders?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of filtered messages that fit the following criteria: ◆ The messages were filtered for the reasons you specified in *Include only those messages filtered for these reasons*. ◆ The messages were sent from the top *n* worst offending senders. You determine the value of *n* in *Maximum number of worst offenders to display.* The default is No.

4.14 Health

This Knowledge Script is obsolete, although you can continue to use it. Its functionality is distributed among the following Knowledge Scripts introduced with AppManager for Exchange Server 2007 version 7.3:

◆ All_ClockSynchronization	◆ MBS_DatabaseStateChange
◆ All_EventLog	◆ MBS_MailboxAccessibility

◆ All_ServiceStatus	◆ MBS_MailboxUsage
◆ CAS_Activity	◆ MBS_MailFlow
◆ CAS_Connectivity	◆ MBS_MessagingRecordsMgmt
◆ CAS_OABAvailability	◆ MBS_PublicFolderUsage
◆ CAS_PublicFolderAvailability	◆ MBS_Replication
◆ ETS_ExternalMail	◆ Transport_BackPressure
◆ ETS_MessageHygiene	◆ Transport_QueueStatus
◆ HTS_Connectivity	◆ UMS_CallActivity
◆ HTS_SendersAndRecipients	◆ UMS_Connectivity
◆ HTS_TransportDumpster	◆ UMS_Performance
◆ MBS_ClusterOwner	

****

Use this Knowledge Script to monitor the health of Exchange Server 2007 Server roles. This script monitors the following services and activities:

- The Windows Event Log for errors and warnings that arise from any service name that contains the word **exchange**
- Running status of all Exchange Server 2007 services
- Clock synchronization with the Domain Controller
- Response time to ActiveSync, Outlook Web Access, Outlook Web services, and the Autodiscovery service
- Number of messages in queue and change in queue size
- Status of send, receive, and foreign connectors
- Speed of e-mail flow to a specified e-mail address or Mailbox server
- Availability of offline address books and public folders
- Accessibility of mailbox
- Communication between Hub Transport server and Mailbox server
- Synchronization between Hub Transport server and Edge Transport server
- Response to SMTP requests
- Replication health
- Status of mounted and unmounted database
- Available disk space

This script monitors and restarts the following Exchange Server 2007 services:

Mailbox Server Role Services		
IIS Admin Service	Exchange Active Directory Topology	Exchange Information Store
Exchange Mailbox Assistance	Exchange Mail Submission	Exchange Replication Service

Exchange System Attendant	Exchange Search Indexer	Exchange Service Host
Exchange Transport Log Search	Search (Exchange)	World Wide Web Publishing Service
Client Access Server Role Services		
IIS Admin Service	Exchange Active Directory Topology	Exchange File Distribution
Exchange Service Host	World Wide Web Publishing Service	
Hub Transport Server Role Services		
Exchange Active Directory Topology	Exchange EdgeSync	Exchange Transport
Exchange Transport Log Search		
Edge Transport Server Role Services		
Exchange ADAM	Exchange Credential Service	Exchange Transport

This script raises an event and displays information for the following Exchange Server 2007 parameters:

Parameter	What is Displayed
SummaryCopyStatus	Displays the current overall status of the Local Continuous Replication (LCR), Cluster Continuous Replication (CCR) and Single Copy Cluster (SCC) copies. The possible values for the SummaryCopyStatus parameter are: ◆ **Not Supported**: The current configuration does not support continuous replication. ◆ **Disabled**: The storage group and its database object have HasLocalCopy set to 0. ◆ **Failed**: Database or logs are incompatible with each other, or the storage group is improperly configured for LCR. ◆ **Seeding**: Database seeding is in progress. ◆ **Suspended**: Transaction log copying and replay are stopped. ◆ **Healthy**: Status is healthy and normal.
LastInspectedLogTime	Displays the time stamp on the target storage group of the last successful inspection of a transaction log file. The time stamp is displayed if the database is down, or the CopyQueueLength and ReplayQueueLength parameters exceed the recommended thresholds.

NOTE: In the case of LCR copy, this script checks and displays the SummaryCopyStatus and LastInspectedLogTime parameter values only if Exchange Server 2007 is installed in a non-clustered environment.

This script also raises an event for the following conditions:

- The Knowledge Script job fails
- Stopped services fail to start
- The Windows Event Log contains errors and warnings

- Thresholds are exceeded
- Connectors are disabled

4.14.1 Prerequisites

If the AppManager agent service, `netiqmc`, is not running under the Local System account, then ensure that the user account running the service is a member of the following groups for the indicated server roles.

Server Roles	Membership Group
Client Access server role	The Health Knowledge Script monitors the health of vital Client Access server components such as ActiveSync, Outlook Web Services, and Outlook Web Access. This monitoring requires the creation of a test user and an associated mailbox. If a test user and a mailbox do not exist, AppManager creates them automatically when the Health Knowledge Script runs. However, in order for AppManager to successfully create a test user and mailbox, the account under which the AppManager netiqmc service runs must be a member of certain groups and be endowed with the following permissions: ◆ Exchange Organization Administrators group ◆ Local Administrators group After you run the Health Knowledge Script once with proper permissions and memberships in place and the test user and mailbox are created, a user with lesser privileges can run the Health Knowledge Script. You can also create the test user and mailbox manually. For more information about creating the test user and mailbox, see your Microsoft Exchange Server 2007 documentation.
Edge Transport server role	Local Administrators group
Hub Transport server role	◆ Exchange Organization Administrators group ◆ Local Administrators group If the AppManager agent service is running under the Local System account, all health monitoring will succeed except the monitoring of message queues.
Mailbox server role	◆ Exchange Server Administrators group ◆ Local Administrators group

4.14.2 Resource Objects

- Exchange_ServerIcon
- Exchange_ClientAccessServer
- Exchange_EdgeTransportServer
- Exchange_HubTransportServer
- Exchange_MailboxServer

To monitor individual storage groups, mailbox databases, transport queues, and services, use the Objects tab to select the specific objects to monitor.

4.14.3 Default Schedule

By default, this script runs every 30 minutes.

4.14.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Communicate only with Exchange Servers in the local domain?	Select **Yes** to allow the Health job to test only Exchange Servers in the same domain as the server on which you run the Health job. When this option is unselected, certain health tests for the Client Access server and the Hub Transport server attempt to contact all Mailbox servers in your organization. These tests will fail if the Exchange accounts in one domain do not have access to other domains.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Health job fails. The default is 5.
Raise event indicating active/passive cluster state?	Select **Yes** to raise an informational event indicating the current status of the cluster: active or passive. The default is No.
Monitor Exchange 2007 Server Health	
All Server Roles	
Status of Exchange 2007 services	
Raise event if Exchange 2007 services are not running?	Select **Yes** to raise an event if at least one Exchange Server 2007 service is not running. The default is Yes.
Event severity when services are not running	Set the severity level, from 1 to 40, to indicate the importance of an event in which at least one Exchange Server 2007 service is not running. The default is 15.
Start services not currently running?	Select **Yes** to start Exchange Server 2007 services that are not running. The default is Yes.
Raise event if stopped services fail to restart?	Select **Yes** to raise an event if AppManager cannot restart Exchange Server 2007 services that are not running. The default is Yes.
Threshold - Timeout for service restart	Set the number of seconds that AppManager should wait for Exchange Server 2007 services to restart before raising an event. The default is 15 seconds.
Event severity when stopped services fail to start	Set the severity level, from 1 to 40, to indicate the importance of an event in which Exchange Server 2007 services fail to restart after the specified timeout period. The default is 5.
Windows Event Log	

Parameter	How to Set It
Raise event if errors are found?	Select **Yes** to raise an event if the Windows Event Log contains errors that arise from any service name that contains the word **exchange**. The default is Yes.
Event severity when errors are found	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Windows Event Log contains error messages. The default is 10.
Raise event if warnings are found?	Select **Yes** to raise an event if the Windows Event Log contains warnings that arise from any service name that contains the word **exchange**. The default is Yes.
Event severity when warnings are found	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Windows Event Log contains warning messages. The default is 20.
Clock Synchronization with Domain Controller	
Comma-separated list of Domain Controllers to test	Use this parameter to limit the number of Domain Controller (DC) clocks that are tested for synchronization with the clock on the server running the Health Knowledge Script. Leave this parameter blank to test all DC clocks in your organization. The list can contain fully qualified hostnames, separated by commas. It can also contain patterns that use the following wildcards. Separate the patters with commas. ◆ An asterisk (*) matches zero or more characters. ◆ A question mark (?) matches a single character. ◆ The braces ([]) match any single character included between the braces. Use a dash (-) to specify a range between the braces. For example, [a-z] matches any alphabetic character; [0-9] matches any number, and [aeiou] matches any vowel. If a pattern contains wildcards, all fully qualified DC names that match the pattern are included in the synchronization test. All matching is case-sensitive.
Raise event if clocks are not synchronized?	Select **Yes** to raise an event if the clock on the server running the Health Knowledge Script is not synchronized with the clock on the DC. The default is Yes.
Threshold - Maximum amount of clock offset	Set the maximum number of seconds that the server clock can be out of sync with the DC. For example, setting the threshold to 2 indicates that it is acceptable for the clock to be two seconds faster or slower than the clock on the DC. The default is 10 seconds. If you want the server clock to be in sync with the DC clock, set this parameter to 0.
Event severity when clock offset exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the clock synchronization offset exceeds the threshold you set. The default is 25.
Client Access Server Role	
ActiveSync Connectivity	
Raise event if ActiveSync connectivity test fails?	Select **Yes** to raise an event if AppManager cannot check connectivity to ActiveSync. The default is Yes.
Event severity when ActiveSync connectivity test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot check connectivity to ActiveSync. The default is 15.

Parameter	How to Set It
Raise event if response time is excessive?	Select **Yes** to raise an event if the amount of time it takes to connect to ActiveSync exceeds the threshold you set. The default is Yes.
Threshold - Response time for connectivity test	Set the number of milliseconds that AppManager should wait for connectivity with ActiveSync before raising an event. The default is 1000 ms. The minimum is 1 ms.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time taken for testing connectivity to ActiveSync exceeds the threshold that you set. The default is 25.
Outlook Web Access Connectivity	
Raise event if Outlook Web Access connectivity test fails?	Select **Yes** to raise an event if AppManager cannot check connectivity to Outlook Web Access. The default is Yes.
Event severity when Outlook Web Access connectivity test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot check connectivity to Outlook Web Access. The default is 15.
Raise event if response time is excessive?	Select **Yes** to raise an event if the amount of time it takes to connect to Outlook Web Access exceeds the threshold you set. The default is Yes.
Threshold - Response time for connectivity test	Set the number of milliseconds that AppManager should wait to confirm connectivity with Outlook Web Access before raising an event. The default is 1000 ms. The minimum is 1 ms.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time taken for testing connectivity to Outlook Web Access exceeds the threshold that you set. The default is 25.
Outlook Web Services Connectivity	
Use SSL (HTTPS) for connectivity test?	Select **Yes** to use Secure Socket Layer (SSL) to test connectivity to Outlook Web services. The default is Yes. If you select **Yes**, AppManager will use only SSL to test connectivity. If you clear the option, AppManager will first use SSL to test connectivity. If that attempt fails, AppManager will then try to test connectivity without using SSL.
Raise event if Outlook Web services connectivity test fails?	Select **Yes** to raise an event if AppManager cannot check connectivity to Outlook Web services. The default is Yes.
Event severity when Outlook Web services connectivity test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot check connectivity to Outlook Web services. The default is 15.
Raise event if response time is excessive?	Select **Yes** to raise an event if the amount of time it takes to connect to Outlook Web services exceeds the threshold you set. The default is Yes.
Threshold - Response time for connectivity test	Set the number of milliseconds that AppManager should wait to confirm connectivity with Outlook Web Services before raising an event. The default is 1000 ms. The minimum is 1 ms.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time taken for testing connectivity to Outlook Web services exceeds the threshold that you set. The default is 25.
Autodiscovery Service Connectivity	

Parameter	How to Set It
Event Notification	
Raise event if Autodiscovery service connectivity test fails?	Select **Yes** to raise an event if AppManager cannot check connectivity to the Autodiscovery service. The default is Yes. The Autodiscovery service allows Outlook 2007 clients and mobile devices to be recognized when they connect to the Client Access server.
Event severity when Autodiscovery service connectivity test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot check connectivity to the Autodiscovery service. The default is 15.
Offline Address Book Availability	
Raise event if offline address books cannot be downloaded?	Select **Yes** to raise an event if the Client Access server's offline address books cannot be downloaded. The default is Yes.
Event severity when offline address books cannot be downloaded	Set the severity level, from 1 to 40, to indicate the importance of an event in which offline address books cannot be downloaded. The default is 15.
Public Folder Availability	
Raise event if public folders are inaccessible?	Select **Yes** to raise an event if the Client Access server's public folders are inaccessible. The default is Yes. A public folder can be inaccessible for one of the following reasons: ◆ The public folder database is unmounted ◆ The Mailbox server is not running ◆ The user does not have proper access permissions
Event severity when public folders are inaccessible	Set the severity level, from 1 to 40, to indicate the importance of an event in which public folders are inaccessible. The default is 15.
Edge Transport Server Role	
Message Hygiene	
Raise event if percentage of content-filtered messages exceeds threshold?	Select **Yes** to raise an event if the percentage of increase in content-filtered messages exceeds the threshold you set. The default is Yes. Content-filtered messages are those that the Edge Transport server filters for security breaches such as, spam, viruses, or blocked e-mail addresses.
Threshold - Maximum percentage of messages filtered because of content	Set the maximum percentage that is acceptable for the increase in filtered messages between Knowledge Script job iterations. AppManager raises an event if the percentage exceeds the threshold. The default is 40%.
Event severity when percentage of filtered messages exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of filtered messages exceeds the threshold you set. The default is 15.
Raise event if size of poison message queue exceeds threshold?	Select **Yes** to raise event if the number of messages in the poison message queue exceeds the threshold you set. The default is Yes. The poison message queue is a quarantine destination for those messages that the Edge Transport server identifies as potentially fatal to the Exchange server 2007 server.

Parameter	How to Set It
Threshold - Maximum number of messages in poison message queue	Set the maximum number of messages that can be quarantined in the poison message queue before an event is raised. The default is 5 messages.
Event severity when number of messages in poison message queue exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of messages in the poison message queue exceeds the threshold you set. The default is 15.
Message Queues	
Raise event for number of messages in queue?	Select **Yes** to raise an event if the number of messages in queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of messages in queue	Set the maximum number of messages that can be in queue before an event is raised. The default is 1000 messages.
Event severity when queue size exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of messages in queue exceeds the threshold you set. The default is 15.
Raise event if increase in queue size is excessive?	Select **Yes** to raise an event if the percentage of increase in queue size since the last job iteration exceeds the threshold you set. The default is Yes.
Threshold - Percentage increase in queue size since last job iteration	Set the maximum acceptable percentage of increase in queue size since the last job iteration. AppManager raises an event if the percentage of increase exceeds this value. The default is 50%.
Event severity when increase in queue size exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in queue size exceeds the threshold you set. The default is 15.
Send and Receive Connectors	
Raise event if any send or receive connectors are disabled?	Select **Yes** to raise an event if a send or receive connector is disabled. The default is Yes. The connector sends and receives e-mail from a Hub Transport server. The e-mail may be sent and received within the organization through the intranet or outside the organization through the Internet.
Event severity when any connectors are disabled	Set the severity level, from 1 to 40, to indicate the importance of an event in which a send or receive connector is disabled. The default is 15.
Raise event if receive connectors cannot respond to SMTP requests?	Select **Yes** to raise an event if a receive connector is unable to respond to SMTP (Simple Mail Transfer Protocol) requests. The default is Yes.
Event severity when receive connectors cannot respond to SMTP requests	Set the severity level, from 1 to 40, to indicate the importance of an event in which a receive connector is unable to respond to SMTP requests. The default is 15.
Raise event if send connectors cannot send mail to internal recipients?	Select **Yes** to raise an event if a send connector is unable to send e-mail from the Internet to your intranet. The default is Yes.
Event severity when send connectors cannot send mail to internal recipients	Set the severity level, from 1 to 40, to indicate the importance of an event in which a send connector is unable to send e-mail from the Internet to your intranet. The default is 15.

Parameter	How to Set It
Hub Transport Server Role	
Server Communication	
Raise event if time of last Edge synchronization exceeds threshold?	Select **Yes** to raise an event if synchronization between the Edge Transport server and the Hub Transport server has not occurred within the last *n* minutes. The default is Yes. Use the *Threshold - Maximum number of minutes since last Edge synchronization* parameter to determine the value of *n.*
Threshold - Maximum number of minutes since last Edge synchronization	Set the maximum number of minutes that should elapse since the last synchronization before an event is raised. The default is 30 minutes.
Event severity when time of last Edge synchronization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of minutes since the last synchronization exceeds the threshold you set. The default is 15.
Raise event if unable to communicate with any Mailbox servers?	Select **Yes** to raise an event when the Hub Transport server cannot communicate with the Mailbox databases on the Mailbox server. The default is Yes. The Hub Transport server transports e-mail to and from the Mailbox server. Therefore, ensuring uninterrupted communication is vital to the health of your Exchange Server 2007 environment.
Event severity when unable to communicate with any Mailbox servers	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Hub Transport server cannot communicate with the Mailbox databases on the Mailbox server. The default is 15.
Message Queues	
Raise event for number of messages in queue?	Select **Yes** to raise an event if the number of messages in queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of messages in queue	Set the maximum number of messages that can be in queue before an event is raised. The default is 1000 messages.
Event severity when queue size exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of messages in queue exceeds the threshold you set. The default is 15.
Raise event if increase in queue size is excessive?	Select **Yes** to raise an event if the percentage of increase in queue size since the last job iteration exceeds the threshold you set. The default is No.
Threshold - Percentage of increase in queue size since last job iteration	Set the maximum acceptable percentage of increase in queue size since the last job iteration. If the percentage of increase exceeds this value, an event is raised. The default is 50%.
Event severity when increase in queue size exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in queue size exceeds the threshold you set. The default is 15.
Send, Receive, and Foreign Connectors	

Parameter	How to Set It
Raise event if any send, receive, or foreign connectors are disabled?	Select **Yes** to raise an event if a send, receive, or foreign connector is disabled. The default is Yes. The receive connectors receive e-mail from an Edge Transport server, a Mailbox server, or from the Internet when an Edge role is not set up in the Exchange environment. The send connectors send e-mail to the mailbox of the intended recipient or to the Edge Transport server for delivery to another domain. The foreign connectors move e-mail to a server within the organization that does not communicate using SMTP.
Event severity when any connectors are disabled	Set the severity level, from 1 to 40, to indicate the importance of an event in which a send, receive, or foreign connector is disabled. The default is 15.
Raise event if receive connectors cannot respond to SMTP requests?	Select **Yes** to raise an event if a send, receive, or foreign connector is unable to respond to SMTP requests. The default is Yes.
Event severity when receive connectors cannot respond to SMTP requests	Set the severity level, from 1 to 40, to indicate the importance of an event in which a receive connector is unable to respond to SMTP requests. The default is 15.
Mailbox Server Role	
Mail Flow	
Target Mailbox server	Enter the hostname of the computer that hosts the Mailbox server with which you want to check connectivity. The hostname need not be fully qualified unless DNS lookup does not resolve the simple name. This is an optional parameter. **Important** Both the Mailbox server and the computer on which you run this Knowledge Script must be in the *same* Active Directory forest. To test e-mail flow to a Mailbox server that is not in the same Active Directory forest, use the *E-mail address for recipient of test message* parameter. The connectivity test verifies that the local Mailbox server can send e-mail to the specified Mailbox server.
Email address for recipient of test message	Provide the e-mail address with which you want to check connectivity. The connectivity test will verify that the local Mailbox server can send e-mail to the specified e-mail address. **Important** Use this parameter to test e-mail flow to a Mailbox server that is *not* in the same Active Directory forest as the local Mailbox server. To test e-mail flow to a Mailbox server that is in the same Active Directory forest, use the *Target Mailbox server* parameter.
Raise event if mail flow test fails?	Select **Yes** to raise an event if AppManager cannot check connectivity to the e-mail address you specified. The default is Yes.

Parameter	How to Set It
Event severity when mail flow test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot check connectivity to the e-mail address you specified. The default is 15.
Raise event if response time is excessive?	Select **Yes** to raise an event if the amount of time it takes to connect to the e-mail address exceeds the threshold you set. The default is Yes.
Threshold - Response time for mail flow test	Set the number of milliseconds that AppManager should wait to confirm connectivity with the e-mail address before raising an event. The default is 1000 ms. The minimum is 1 ms.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time taken for testing connectivity to the e-mail address exceeds the threshold that you set. The default is 25.
Mailbox Accessibility	
Raise event if system mailbox cannot be accessed?	Select **Yes** to raise an event if the Mailbox server cannot access the system mailbox. The default is Yes. The system mailbox is inaccessible when it does not exist.
Event severity when system mailbox cannot be accessed	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Mailbox server cannot access the system mailbox. The default is 15.
Raise event if response time is excessive?	Select **Yes** to raise an event if the amount of time it takes to connect to the system mailbox exceeds the threshold you set. The default is Yes.
Threshold - Response time for mailbox accessibility test	Set the number of milliseconds that AppManager should wait to confirm connectivity with the system mailbox before raising an event. The default is 1000 ms. The minimum is 1 ms.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time taken for testing connectivity to the system mailbox exceeds the threshold that you set. The default is 25.
Storage Group Replication	
Raise event if replication is unhealthy?	Select **Yes** to raise an event if storage group replication is unhealthy. The default is Yes. AppManager considers replication to be unhealthy if at least one of the following conditions exists: ◆ The length of the copy queue for a storage group is greater than 3. ◆ The length of the replay queue for a storage group is greater than 20. ◆ The Exchange Server indicates that replication is unhealthy.
Event severity when replication is unhealthy	Set the severity level, from 1 to 40, to indicate the importance of an event in which storage group replication is unhealthy. The default is 15.
Database Status	
Raise event if databases are unmounted?	Select **Yes** to raise an event if databases are unmounted. The default is Yes. When a database is unmounted, the Exchange Server cannot store information in it or read information from it.
Event severity when databases are unmounted	Set the severity level, from 1 to 40, to indicate the importance of an event in which databases are unmounted. The default is 5.

Parameter	How to Set It
Disk Space	
Raise event if free space for database files is low?	Select **Yes** to raise an event if the amount of free space for database files falls below the threshold you set. The default is Yes.
Threshold - Minimum free disk space	Set the minimum amount of disk space that must be available to prevent an event from being raised. The default is 1024 MB.
Event severity when free disk space falls below threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the amount of free disk space falls below the threshold. The default is 25.
Raise event if free space for log files is low?	Select **Yes** to raise an event if the amount of free space for log files falls below the threshold you set. The default is Yes.
Threshold - Minimum free disk space	Set the minimum amount of disk space that must be available to prevent an event from being raised. The default is 1024 MB.
Event severity when free disk space falls below threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the amount of free disk space falls below the threshold. The default is 25.

4.15 HTS_Connectivity

Use this Knowledge Script to monitor the connectivity with a Mailbox server and to monitor the time of the last synchronization with the Edge Transport server. This script raises an event if a threshold is exceeded.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see Section 4.43, “Recommended Knowledge Script Group,” on page 162.

4.15.1 Resource Objects

- Exchange2007_HubTransportServer
- Exchange2010_HubTransportServer
- Exchange2013_HubTransportServer
- Exchange2016_HubTransportServer
- Exchange2019_HubTransportServer

4.15.2 Default Schedule

By default, this script runs every 15 minutes.

4.15.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	

Parameter	How to Set It
Communicate only with Exchange Servers in the local domain?	Select **Yes** to test only Exchange Servers in the same domain as the server on which you run the HTS_Connectivity job. When this option is unselected, the tests attempt to contact *all* Mailbox servers in your organization. These tests will fail if the Exchange accounts in one domain do not have access to other domains.
Ignore these Mailbox servers when testing HTS to MBS communications	Provide a comma-separated list of the hostnames of the Mailbox servers that you want to exclude from availability testing between the Hub Transport server and the Mailbox server.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the HTS_Connectivity job fails. The default is 5.
Monitor Mailbox Server Communication	
Event Notification	
Raise event if unable to communicate with a Mailbox server?	Select **Yes** to raise an event when the Hub Transport server cannot communicate with a Mailbox database on the Mailbox server. The default is Yes. The Hub Transport server transports e-mail to and from the Mailbox server. Therefore, ensuring uninterrupted communication is vital to the health of your Exchange Server environment.
Threshold - Maximum number of seconds to wait before timing out	Set the maximum length of time the Hub Transport server should attempt to contact the Mailbox server before timing out and raising an event. The default is 15 seconds.
Event severity when unable to communicate with a Mailbox server	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Hub Transport server cannot communicate with a Mailbox database on the Mailbox server. The default is 5.
Monitor Edge Synchronization	
Event Notification	
Raise event if this Hub Transport server is not subscribed to any Edge Transport servers?	Select **Yes** to raise an event if the Hub Transport server you are monitoring is not subscribed to an Edge Transport server. AppManager cannot monitor synchronization if the Hub Transport server is not subscribed to the Edge Transport server. Disable this parameter if you will not monitor synchronization with the Edge Transport server. Subscription to the Edge Transport server is not required for AppManager to monitor Mailbox server communication or connector availability. The default is Yes.
Event severity when this Hub Transport server is not subscribed to any Edge Transport servers	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Hub Transport server is not subscribed to an Edge Transport server. The default is 15.

Parameter	How to Set It
Raise event if time of last Edge synchronization exceeds threshold?	Select **Yes** to raise an event if synchronization between the Edge Transport server and the Hub Transport server has not occurred within the last *n* minutes. The default is Yes. Use the *Threshold - Maximum number of minutes since last Edge synchronization* parameter to determine the value of *n*.
Threshold - Maximum number of minutes since last Edge synchronization	Set the maximum number of minutes that can elapse since the last synchronization before an event is raised. The default is 30 minutes.
Event severity when time of last Edge synchronization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of minutes since the last synchronization exceeds the threshold you set. The default is 15.

4.16 HTS_SafetyNet

Use this Knowledge Script to monitor the Safety Net availability in Exchange Server 2013, 2016, and 2019. It replaces the HTS_TransportDumpster Knowledge script available for Exchange Server 2007 and 2010. You can use this Knowledge Script to monitor Safety Net activities like, average safety net resubmit request time span, resubmit latency average time, resubmit request count, safety net resubmission count, safety net resubmission request count, shadow safety net resubmission count, and shadow safety net resubmission request count.

4.16.1 Resource Objects

- Exchange2013_HubTransportServer
- Exchange2016_HubTransportServer
- Exchange2019_HubTransportServer

4.16.2 Default Schedule

By default, this script runs every 15 minutes.

4.16.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the HTS_SafetyNet job fails. The default is 5.
Monitor Safety Net Availability	
Event Notification	

Parameter	How to Set It
Raise event if Safety Net is unavailable?	Select **Yes** to raise an event if the Safety Net cannot be accessed. The default is Yes.
Event severity when Safety Net is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Safety Net cannot be accessed. The default is 5.
Monitor Safety Net Activity	
Data Collection	
Collect data for average Safety Net resubmit request time span?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average time span of resubmit request of all e-mail messages in Safety Net during the monitoring interval. The default is No.
Collect data for resubmit latency average time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average response time of resubmit requests of e-mail messages in the Safety Net during the monitoring period. The default is No.
Collect data for resubmit request count?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the resubmit request count of e-mail messages in the Safety Net during the monitoring interval. The default is No.
Collect data for Safety Net resubmission count?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the total resubmission count of e-mail messages in the Safety Net during the monitoring interval. The default is No.
Collect data for Safety Net resubmission request count?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the total resubmission request count of e-mail messages in the Safety Net during the monitoring interval. The default is No
Collect data for Shadow Safety Net resubmission count?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the total resubmission count of e-mail messages in the shadow Safety Net during the monitoring interval. The default is No
Collect data for Shadow Safety Net resubmission request count?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the total resubmission request count of e-mail messages in the shadow Safety Net during the monitoring interval. The default is No

4.17 HTS_SendersAndRecipients

Use this Knowledge Script to measure average and individual e-mail volume for senders and recipients. This script raises an event if the number of messages or the total size in MB of all messages exceeds the threshold you set.

4.17.1 Resource Objects

- Exchange2007_HubTransportServer
- Exchange2010_HubTransportServer
- Exchange2013_HubTransportServer
- Exchange2016_HubTransportServer
- Exchange2019_HubTransportServer

4.17.2 Default Schedule

By default, this script runs every one hour.

4.17.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Measure mail volume by message count or total message size	Select how this script measures the volume of mail sent to and from your Exchange environment. Choose from **Message count** or **Total message size**. Total message size is measured in MB. The default is Message count.
Comma-separated list of senders and recipients to ignore	Provide a list of e-mail addresses that this script should ignore when measuring e-mail volume. Separate multiple addresses with a comma.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the HTS_SendersAndRecipients job fails. The default is 5.
Monitor Recipients of Internal Mail	
Monitor Average Mail Volume for Recipients of Internal Mail	
Number of top recipients to monitor for average volume	Set the top *n* e-mail recipients whose average internal mail volume you want to monitor. The default is 10 recipients, the minimum is 0, and the maximum is 2147483647. To monitor all recipients for average volume, enter 0.
Event Notification	
Raise event if average volume for top recipients of internal mail exceeds threshold?	Select **Yes** to raise an event if the average mail volume for the top *n* recipients exceeds the threshold you set. The default is Yes.
Threshold - Maximum average volume for top recipients of internal mail	Set the maximum value that average mail volume can attain before an event is raised. The default is 250. Use the *Measure mail volume by message count or total message size* parameter to indicate whether the threshold is in number of messages or Megabytes of message.
Event severity when average volume for top recipients of internal mail exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which average mail volume for the top *n* recipients exceeds the threshold. The default is 15.
Data Collection	
Collect data for average volume of top recipients of internal mail?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average mail volume for the top *n* recipients during the monitoring interval. The default is Yes.
Monitor Individual Mail Volume for Recipients of Internal Mail	

Parameter	How to Set It
Number of top recipients to monitor for individual volume	Set the top *n* e-mail recipients whose individual internal mail volume you want to monitor. The default is 10 recipients, the minimum is 0, and the maximum is 2147483647. To monitor all recipients for individual volume, enter 0.
Event Notification	
Raise event if mail volume for top individual recipients exceeds threshold?	Select **Yes** to raise an event if the individual mail volume for the top *n* recipients exceeds the threshold you set. The default is Yes.
Threshold - Maximum mail volume for individual recipients	Set the maximum value that individual mail volume can attain before an event is raised. The default is 250. Use the *Measure mail volume by message count or total message size* parameter to indicate whether the threshold is in number of messages or Megabytes of message.
Event severity when mail volume for individual recipients exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which individual mail volume for the top *n* recipients exceeds the threshold. The default is 15.
Data Collection	
Collect data for mail volume for individual recipients?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the individual mail volume for the top *n* recipients during the monitoring interval. The default is No.
Monitor Senders of Internal Mail	
Monitor Average Mail Volume for Senders of Internal Mail	
Number of top senders to monitor for average volume	Set the top *n* e-mail senders whose average internal mail volume you want to monitor. The default is 10 senders, the minimum is 0, and the maximum is 2147483647. To monitor all senders for average volume, enter 0.
Event Notification	
Raise event if average volume for top senders of internal mail exceeds threshold?	Select **Yes** to raise an event if the average mail volume for the top *n* senders exceeds the threshold you set. The default is Yes.
Threshold - Maximum average volume for top senders of internal mail	Set the maximum value that average mail volume can attain before an event is raised. The default is 50. Use the *Measure mail volume by message count or total message size* parameter to indicate whether the threshold is in number of messages or Megabytes of message.
Event severity when average volume for top senders of internal mail exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which average mail volume for the top *n* senders exceeds the threshold. The default is 15.
Data Collection	
Collect data for average volume of top senders of internal mail?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average mail volume for the top *n* senders during the monitoring interval. The default is Yes.
Monitor Individual Mail Volume for Senders of Internal Mail	

Parameter	How to Set It
Number of top senders to monitor for individual volume	Set the top *n* e-mail senders whose individual internal mail volume you want to monitor. The default is 10 senders, the minimum is 0, and the maximum is 2147483647. To monitor all senders for individual volume, enter 0.
Event Notification	
Raise event if mail volume for top individual senders exceeds threshold?	Select **Yes** to raise an event if the individual mail volume for the top *n* senders exceeds the threshold you set. The default is Yes.
Threshold - Maximum mail volume for individual senders	Set the maximum value that individual mail volume can attain before an event is raised. The default is 50. Use the *Measure mail volume by message count or total message size* parameter to indicate whether the threshold is in number of messages or Megabytes of message.
Event severity when mail volume for individual senders exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which individual mail volume for the top *n* senders exceeds the threshold. The default is 15.
Data Collection	
Collect data for mail volume for individual senders?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the individual mail volume for the top *n* senders during the monitoring interval. The default is No.

4.18 HTS_TransportDumpster

Use this Knowledge Script to monitor Transport Dumpster availability, the number and size of items in the Transport Dumpster, and activity:

- Rate at which items are inserted into the Transport Dumpster
- Rate at which items are deleted from the Transport Dumpster
- Number of items redelivered by the Transport Dumpster

The Transport Dumpster is a container in which recently delivered e-mail is stored. It allows the Hub Transport server to defer the deletion of e-mail so that it can redeliver e-mail after an unscheduled outage.

NOTE: This Knowledge Script is available only for Exchange Server 2007 and 2010. For Exchange Server 2013, 2016, and 2019, see Section 4.16, “HTS_SafetyNet,” on page 94.

4.18.1 Resource Objects

- Exchange2007_HubTransportServer
- Exchange2010_HubTransportServer

4.18.2 Default Schedule

By default, this script runs every 15 minutes.

4.18.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the HTS_TransportDumpster job fails. The default is 5.
Monitor Transport Dumpster Availability	
Event Notification	
Raise event if Transport Dumpster is unavailable?	Select **Yes** to raise an event if the Transport Dumpster cannot be accessed. The default is Yes.
Event severity when Transport Dumpster is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Transport Dumpster cannot be accessed. The default is 5.
Monitor Size of Transport Dumpster	
Data Collection	
Collect data for number of items in Transport Dumpster?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of e-mail messages in the Transport Dumpster during the monitoring interval. The default is No.
Collect data for total size of items currently in Transport Dumpster?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the size of all e-mail messages in MB in the Transport Dumpster during the monitoring interval. The default is No.
Monitor Transport Dumpster Activity	
Data Collection	
Collect data for item insertion rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the rate at which e-mail messages were inserted in the Transport Dumpster during the monitoring interval. The default is No.
Collect data for item deletion rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the rate at which e-mail messages were deleted from the Transport Dumpster during the monitoring interval. The default is No.
Collect data for item redelivery count?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the rate at which e-mail messages were redelivered from the Transport Dumpster during the monitoring interval. The default is No.

4.19 MBS_ClientActivity

In Exchange Server 2013, 2016, and 2019, the performance counters for Client Access Server (CAS) activity is available only from Mailbox Server. Use this Knowledge Script to monitor Exchange Server 2013 Mailbox server services and functions:

- Availability Service activity
- ActiveSync response time and request rate
- Outlook Web Access response time, search time, login rate, and login failures

- Outlook Web Services request rate and current connections
- IMAP4 (Internet Message Access protocol) processing time, current connections, and active SSL connections
- POP3 (Post Office Protocol) processing time, login rate, current connections, and active SSL connections

NOTE: This Knowledge script only runs on servers with Exchange Server 2013, 2016, and 2019. This script replaces the CAS_Activity Knowledge script available for Exchange Server 2007 and 2010.

4.19.1 Resource Objects

- Exchange2013_MailboxServer
- Exchange2016_MailboxServer
- Exchange2019_MailboxServer

4.19.2 Default Schedule

By default, this script runs every 15 minutes.

4.19.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_ClientActivity job fails. The default is 5.
Comma separated list of servers for which events should not be raised if CAS services are disabled	Specify a comma separated list of server names for which the event messages should not be raised if the client services are in the disabled state.
Monitor Availability Service Activity	
Event Notification	
Raise event if response time for free/busy requests exceeds threshold?	Select **Yes** to raise an event if the response time for free and busy requests to Microsoft Outlook exceeds the threshold you set. The default is Yes. The Availability Service monitors free/busy requests.
Threshold - Maximum free/busy request response time	Set the maximum length of time that Microsoft Outlook can take to respond to free/busy requests before an event is raised. The default is 5000 milliseconds.
Event severity when response time for free/busy requests exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the response time for free/busy requests exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for free/busy request response time?	Select **Yes** to collect data for charts and reports on the response time for free/busy requests. When enabled, data collection returns the length of response time during the monitoring interval. The default is No.
Monitor ActiveSync Activity	
Monitor ActiveSync Response Time	
Event Notification	
Raise event if ActiveSync response time exceeds threshold?	Select **Yes** to raise an event if the response time for ActiveSync exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time	Set the maximum length of time that ActiveSync can take to respond to requests before an event is raised. The default is 100 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which ActiveSync response time exceeds the threshold. The default is 15.
Data Collection	
Collect data for response time?	Select **Yes** to collect data for charts and reports on ActiveSync response time. When enabled, data collection returns the length of response time during the monitoring interval. The default is No.
Monitor ActiveSync Request Rate	
Event Notification	
Raise event if ActiveSync request rate exceeds threshold?	Select **Yes** to raise an event if the rate of synchronization requests to ActiveSync exceeds the threshold you set. The default is Yes.
Threshold - Maximum request rate	Set the maximum number of requests that can occur per second before an event is raised. The default is 10 synchronization requests per second.
Event severity when request rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ActiveSync request rate exceeds the threshold. The default is 15.
Data Collection	
Collect data for request rate?	Select **Yes** to collect data for charts and reports on ActiveSync request time. When enabled, data collection returns the rate of synchronization requests during the monitoring interval. The default is No.
Monitor Outlook Web Access Activity	
Monitor Outlook Web Access Response Time	
Event Notification	
Raise event if Outlook Web Access response time exceeds threshold?	Select **Yes** to raise an event if the response time for Outlook Web Access (OWA) exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time	Set the maximum amount of time that it can take for OWA to respond to requests before an event is raised. The default is 100 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which OWA response time exceeds the threshold. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for response time?	Select **Yes** to collect data for charts and reports on the response time of OWA. When enabled, data collection returns the length of response time during the monitoring interval. The default is No.
Monitor Outlook Web Access Search Time	
Event Notification	
Raise event if Outlook Web Access search time exceeds threshold?	Select **Yes** to raise an event if Outlook Web Access (OWA) search time exceeds the threshold. The default is Yes. The OWA search feature allows users to find items in a mailbox.
Threshold - Maximum search time	Set the maximum length of time that OWA can spend performing a search before an event is raised. The default is 100 milliseconds.
Event severity when search time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which OWA search time exceeds the threshold. The default is 15.
Data Collection	
Collect data for search time?	Select **Yes** to collect data for charts and reports on Outlook Web Access (OWA) search time. When enabled, data collection returns the length of search time during the monitoring interval. The default is No.
Monitor Outlook Web Access Login Rate	
Event Notification	
Raise event if login rate exceeds threshold?	Select **Yes** to raise an event if the rate at which users log in to Outlook Web Access (OWA) exceeds the threshold. The default is Yes.
Threshold - Maximum login rate	Set the maximum rate at which users can log in to OWA before an event is raised. The default is 10 logins per second.
Event severity when login rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the rate at which users log in to OWA exceeds the threshold. The default is 15.
Data Collection	
Collect data for login rate?	Select **Yes** to collect data for charts and reports on the rate at which users log in to OWA. When enabled, data collection returns the OWA log in rate for the monitoring interval. The default is No.
Monitor Outlook Web Access Login Failures	
Event Notification	
Raise event if login failures exceed threshold?	Select **Yes** to raise an event if the failures for logging in to Outlook Web Access (OWA), expressed as a percentage of all login attempts, exceed the threshold. The default is Yes.
Threshold - Maximum percentage of login failures	Set the maximum percentage of OWA login failures that can occur before an event is raised. The default is 10%.
Event severity when login failures exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which percentage of OWA login failures exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for login failures?	Select **Yes** to collect data for charts and reports on the percentage of OWA login failures. When enabled, data collection returns the percentage of OWA login failures for the monitoring interval. The default is No.
Monitor Outlook Web Services Activity	
Monitor Outlook Web Services Request Rate	
Event Notification	
Raise event if Outlook Web Services request rate exceeds threshold?	Select **Yes** to raise an event if the rate of requests to Outlook Web Services exceeds the threshold you set. The default is Yes.
Threshold - Maximum request rate	Set the maximum number of requests that can occur per second before an event is raised. The default is 10 requests per second.
Event severity when request rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the rate of requests to Outlook Web Services exceeds the threshold. The default is 15.
Data Collection	
Collect data for request rate?	Select **Yes** to collect data for charts and reports on the rate of requests to Outlook Web Services. When enabled, data collection returns the rate of requests during the monitoring interval. The default is No.
Monitor Outlook Web Services Current Connections	
Event Notification	
Raise event if number of current connections exceeds threshold?	Select **Yes** to raise an event if the number of connections established with Outlook Web Services exceeds the threshold you set. The default is Yes. By knowing the number of current connections, you can determine user load for Outlook Web Services.
Threshold - Maximum number of current connections	Set the maximum number of connections to Outlook Web Services that can be established before an event is raised. The default is 25 connections.
Event severity when number of current connections exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of connections established with Outlook Web Services exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of current connections?	Select **Yes** to collect data for charts and reports on the number of connections established with Outlook Web Services. When enabled, data collection returns the number of connections established during the monitoring interval. The default is No.
Monitor IMAP4 Activity	
Monitor IMAP4 Command Processing Time	
Event Notification	
Raise event if command processing time exceeds threshold?	Select **Yes** to raise an event if the amount of processing time for IMAP4 commands exceeds the threshold you set. The default is Yes.
Threshold - Maximum command processing time	Set the maximum amount of time that can be spent processing IMAP4 commands before an event is raised. The default is 100 milliseconds.

Parameter	How to Set It
Event severity when command processing time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the amount of processing time for IMAP4 commands exceeds the threshold. The default is 15.
Data Collection	
Collect data for command processing time?	Select **Yes** to collect data for charts and reports on the amount of processing time for IMAP4 commands. When enabled, data collection returns the amount of processing time spent during the monitoring interval. The default is No.
Monitor IMAP4 Connections Rate	
Event Notification	
Raise event if connections rate exceeds threshold?	Select **Yes** to raise an event if the number of IMAP4 connections to your Exchange server exceeds the threshold you set. The default is Yes.
Threshold - Maximum connections rate	Set the maximum number of IMAP4 connection requests that can occur per second before an event is raised. The default is 10 connections per second.
Event severity when connections rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of IMAP4 connection requests exceeds the threshold. The default is 15.
Data Collection	
Collect data for connections rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of IMAP4 connection requests for the monitoring intervals. The default is No.
Monitor IMAP4 Current Connections	
Event Notification	
Raise event if number of current connections exceeds threshold?	Select **Yes** to raise an event if the number of current IMAP4 connections to your Exchange server exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of current connections	Set the maximum number of IMAP4 connections that can be established before an event is raised. The default is 10 connections.
Event severity when number of current connections exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of IMAP4 connections exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of current connections?	Select **Yes** to collect data for charts and reports on number of IMAP4 connections established. When enabled, data collection returns the number of IMAP4 connections established during the monitoring interval. The default is No.
Monitor IMAP4 Active SSL Connections	
Event Notification	
Raise event if number of active SSL connections exceeds threshold?	Select **Yes** to raise an event if the number of current IMAP4 connections to your Exchange server over SSL (Secure Sockets Layer) exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum number of active SSL connections	Set the maximum number of IMAP4 connections that can be established over SSL before an event is raised. The default is 50 connections.
Event severity when number of active SSL connections exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of IMAP4 SSL connections exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of active SSL connections?	Select **Yes** to collect data for charts and reports on the IMAP4 connections that can be established over SSL. When enabled, data collection returns the number of IMAP4 SSL connections established during the monitoring interval. The default is No.
Monitor POP3 Activity	
Monitor POP3 Command Processing Time	
Event Notification	
Raise event if command processing time exceeds threshold?	Select **Yes** to raise an event if the amount of processing time for POP3 commands exceeds the threshold you set. The default is Yes.
Threshold - Maximum command processing time	Set the maximum amount of time that can be spent processing POP3 commands before an event is raised. The default is 10 milliseconds.
Event severity when command processing time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the amount of processing time for POP3 commands exceeds the threshold. The default is 15.
Data Collection	
Collect data for command processing time?	Select **Yes** to collect data for charts and reports on the processing time for POP3 commands. When enabled, data collection returns the amount of processing time spent during the monitoring interval. The default is No.
Monitor POP3 Connections Rate	
Event Notification	
Raise event if connections rate exceeds threshold?	Select **Yes** to raise an event if the number of POP3 connections to your Exchange server exceeds the threshold you set. The default is Yes.
Threshold - Maximum connections rate	Set the maximum number of POP3 connection requests that can occur per second before an event is raised. The default is 10 connections per second.
Event severity when connections rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of POP3 connection requests exceeds the threshold. The default is 15.
Data Collection	
Collect data for connections rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of POP3 connection requests for the monitoring intervals. The default is No.
Monitor Current POP3 Current Connections	
Event Notification	

Parameter	How to Set It
Raise event if number of current connections exceeds threshold?	Select **Yes** to raise an event if the number of current POP3 connections to your Exchange server exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of current connections	Set the maximum number of POP3 connections that can be established before an event is raised. The default is 10 connections.
Event severity when number of current connections exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of POP3 connections that are currently established exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of current connections?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of POP3 connections established during the monitoring interval. The default is No.
Monitor POP3 Active SSL Connections	
Event Notification	
Raise event if number of active SSL connections exceeds threshold?	Select **Yes** to raise an event if the number of current POP3 connections to your Exchange server over SSL (Secure Sockets Layer) exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of active SSL connections	Set the maximum number of POP3 connections that can be established over SSL before an event is raised. The default is 25 connections.
Event severity when number of active SSL connections exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of POP3 SSL connections exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of active SSL connections?	Select **Yes** to collect data for charts and reports on POP3 SSL connections. When enabled, data collection returns the number of POP3 SSL connections established during the monitoring interval. The default is No.

4.20 MBS_ClientConnectivity

Use this Knowledge Script to monitor the connectivity of Mailbox server (MBS) services on Exchange Server 2013, 2016, and 2019: ActiveSync, Outlook Web services, and the Autodiscover service. This script raises an event when a connectivity test fails and when response time exceeds the threshold you set.

4.20.1 Running MBS_ClientConnectivity on a Mailbox Server

When you run the MBS_ClientConnectivity Knowledge Script on a Mailbox server, the script automatically creates a test user mailbox on each Mailbox server in the Exchange deployment if those mailboxes do not already exist.

You can also manually create the test user mailboxes on the Exchange 2013, 2016, and 2019 Mailbox Servers.

To create test user mailboxes on an Exchange 2013, 2016, or 2019 Mailbox Server:

1. Login to one of the Exchange 2013, 2016, and 2019 Mailbox Servers and open the Exchange Management Shell.
2. Change directories to the `Scripts` directory under the Microsoft Exchange installation directory.
3. Run the following command:
   `Get-MailboxServer | .\New-TestCasConnectivityUser.ps1`.
4. Follow the on-screen instructions to create the test user mailbox on each Mailbox server.

4.20.2 Resource Objects

- Exchange2013_MailboxServer
- Exchange2016_MailboxServer
- Exchange2019_MailboxServer

4.20.3 Default Schedule

By default, this script runs every 30 minutes.

4.20.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_ClientConnectivity job fails. The default is 5.
Connectivity Test User Configuration	
Use alternate test mailbox configured in Security Manager?	Select **Yes** to use the test mailbox that you have specified in the Security Manager. The defaut is No.
Create default test mailbox on Mailbox servers automatically?	Select **Yes** to create a default test mailbox automatically. The default is Yes.
Create non-existent test mailboxes every N job iterations (specify N)	Specify the number of job iterations for which the non-existent test mailboxes will be created on the Mailbox server. The default is 1.
Monitor ActiveSync Connectivity	
ActiveSync URL to be used in connectivity test	Specify the URL for the ActiveSync that is used to monitor the connectivity in the following format: `https://localhost:<port>/Microsoft-Server-ActiveSync`.
Event Notification	
Raise event if ActiveSync connectivity test fails?	Select **Yes** to raise an event if AppManager cannot check connectivity to ActiveSync. The default is Yes.

Parameter	How to Set It
Event severity when ActiveSync connectivity test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot check connectivity to ActiveSync. The default is 5.
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes to connect to ActiveSync exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time for connectivity test	Set how long AppManager should wait for connectivity with ActiveSync before raising an event. The default is 10000 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time it takes to connect to ActiveSync exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for ActiveSync response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average response time for connecting to ActiveSync. The default is No.
Monitor Outlook Web Services Connectivity	
Event Notification	
Raise event if Outlook Web services connectivity test fails?	Select **Yes** to raise an event if AppManager cannot check connectivity to Outlook Web services. The default is Yes.
Event severity when Outlook Web services connectivity test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot check connectivity to Outlook Web services. The default is 5.
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes to connect to Outlook Web services exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time for connectivity test	Set how long AppManager should wait to confirm connectivity with Outlook Web services before raising an event. The default is 10000 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time taken for testing connectivity to Outlook Web services exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for Outlook Web services response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average response time for connecting to Outlook Web services. The default is No.
Monitor Autodiscover Service Connectivity	
Event Notification	
Raise event if Autodiscover service connectivity test fails?	Select **Yes** to raise an event if AppManager cannot check connectivity to the Autodiscover service. The default is Yes. The Autodiscover service allows Outlook clients and mobile devices to be recognized when they connect to the Mailbox server.
Event severity when Autodiscover service connectivity test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot check connectivity to the Autodiscover service. The default is 5.

Parameter	How to Set It
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes to connect to the Autodiscover service exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time for connectivity test	Set how long AppManager should wait to confirm connectivity with the Autodiscover service before raising an event. The default is 10000 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time taken for testing connectivity to the Autodiscover service exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for Autodiscover service response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average response time for connecting to the Autodiscover service. The default is No.

4.21 MBS_ClusterOwner

Use this Knowledge Script to determine whether an Exchange Server is the owner of a node. This script raises an event if the selected server is not the node owner and if the selected Clustered Mailbox Server (CMS) is down.

NOTE: This script only runs on servers with Exchange Server 2007.

4.21.1 Resource Object

Exchange2007_MailboxServer

4.21.2 Default Schedule

By default, this script runs every five minutes.

4.21.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_ClusterOwner job fails. The default is 5.
Monitor Node Ownership	
Raise event if not node owner?	Select **Yes** to raise an event if the selected Exchange Server is not the owner of its node. The default is No.

Parameter	How to Set It
Event severity when not node owner	Set the severity level, from 1 to 40, to indicate the importance of an event in which the selected Exchange Server is not the owner of the node. The default is 20.
Data Collection	
Collect data for ownership status?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns “0” when the server is not the node owner and “100” if the server is the node owner. The default is Yes.
Monitor Node State	
Event Notification	
Raise event when node is down?	Select **Yes** to raise an event if the node in which the Exchange Server resides is down. The default is Yes.
Event severity when node is down	Set the severity level, from 1 to 40, to indicate the importance of an event in which the node in which the Exchange Server resides is down. The default is 5.
Raise event if CMS is down?	Select **Yes** to raise an event if the Clustered Mailbox Server (CMS) on which the Exchange Server resides is down. The default is Yes.
Event severity when CMS is down	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CMS on which the Exchange Server resides is down. The default is 5.

4.22 MBS_DatabaseStateChange

Use this Knowledge Script to monitor changes in the database state, such as active, passive, or suspended, of the mailbox databases on an Exchange Server in a database availability group (DAG) or an Exchange Virtual Server (EVS). This script raises an event if a database is in a specified state, or moves into a specified state.

A job executed on a database in an Exchange Server 2010, 2013, 2016, and 2019 DAG causes the job to run on all servers in the DAG. However, only the server that currently owns the database monitors that database.

NOTE

- Exchange Server 2010, 2013, 2016, and 2019 do not use storage groups.
- If you run the MBS_DataBaseStateChange Knowledge Script on an Exchange 2007 server, you can only use the database mount parameters found under the **Monitor Database Mount State** heading on the Values tab. If you run the script on an Exchange 2010, 2013, 2016, or 2019 server, you can use all the parameters on the Values tab.

4.22.1 Resource Objects

- Exchange2007_MailboxServer
- Exchange2007_Store_Database
- Exchange2007_Store_PFDatabase
- Exchange2010_MailboxServer

- Exchange2010_Store_Database
- Exchange2010_Store_PFDatabase
- Exchange2010_DAG_Databases
- Exchange2013_MailboxServer
- Exchange2013_Store_Database
- Exchange2013_Store_PFDatabase
- Exchange2013_DAG_Databases
- Exchange2016_MailboxServer
- Exchange2016_Store_Database
- Exchange2016_Store_PFDatabase
- Exchange2016_DAG_Databases
- Exchange2019_MailboxServer
- Exchange2019_Store_Database
- Exchange2019_Store_PFDatabase
- Exchange2019_DAG_Databases

4.22.2 Default Schedule

By default, this script runs every 15 minutes.

4.22.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_DatabaseStateChange job fails. The default is 5.
Monitor Database Mount State	
Event Notification	
Raise event if database is unmounted?	Select **Yes** to raise an event if a database is unmounted. When a database is unmounted, the Exchange Server cannot store information in it or read information from it. The default is Yes.
Raise event only when database first becomes unmounted?	Select **Yes** to raise an event only when the database first becomes unmounted. The default is Yes.
Event severity when database is or becomes unmounted	Set the severity level, from 1 to 40, to indicate the importance of an event in which the database is or becomes unmounted. The default is 5.
Data Collection	

Parameter	How to Set It
Collect data for database mount state?	Click **Yes** to collect data for charts and reports. When enabled, data collection returns the mount status for each monitored mailbox and public folder database. A mounted mailbox or database has a value of 100, while an umounted mailbox or database has a value of 0. The default is No.
Automatically mount database if it is currently unmounted?	Select **Yes** to automatically mount a database that is currently unmounted. The default is No.
Raise event if database is successfully remounted?	Select **Yes** to raise an event when the database has been successfully remounted. The default is No.
Event severity when database is successfully remounted	Set the severity level, from 1 to 40, to indicate the importance of an event in which the database has been successfully remounted. The default is 25.
Raise event if database fails to mount?	Select **Yes** to raise an event if the database you want to automatically mount fails to mount. The default is no.
Event severity when database fails to mount	Set the severity level, from 1 to 40, to indicate the importance of an event in which the database you want to automatically mount fails to mount. The default is 5.
Monitor Database Copy State	
Event Notification	
Raise event if database copy is suspended?	Select **Yes** to raise an event if the process of copying a database is suspended. The default is Yes.
Raise event only when database first becomes suspended?	Select **Yes** to raise an event only when the database first becomes suspended. The default is Yes.
Event severity when database is or becomes suspended	Set the severity level, from 1 to 40, to indicate the importance of an event in which the database is or becomes suspended. The default is 15.
Raise event if database copy is removed from server?	Select **Yes** to raise an event if a copy of the database is removed. The default is Yes.
Event severity when database copy is removed from the server.	Set the severity level, from 1 to 40, to indicate the importance of an event in which the database is removed from the server. The default is 15.
Monitor Database Active/Passive State	
Event Notification - Database Instances	
Raise event if database is passive?	Select **Yes** to raise an event if a database is passive. The default is Yes.
Raise event only when database first becomes passive?	Select **Yes** to raise an event only when the database first becomes passive. The default is Yes.
Event severity when database is or becomes passive	Set the severity level, from 1 to 40, to indicate the importance of an event in which the database is or becomes passive. The default is 25.
Raise event if database is active?	Select **Yes** to raise an event if a database is active. The default is Yes.
Raise event only when database first becomes active?	Select **Yes** to raise an event only when the database first becomes active. The default is Yes.

Parameter	How to Set It
Event severity when database is or becomes active	Set the severity level, from 1 to 40, to indicate the importance of an event in which the database is or becomes active. The default is 25.
Event Notification - Database Collection	
Raise event if more than N databases are active?	Select **Yes** to raise an event if more than the specified number of databases are active. The default is Yes.
Raise event only when more than N databases become active?	Select **Yes** to raise an event only when more than the specified number of databases become active. The default is Yes.
Event severity when more than N databases are or become active	Set the severity level, from 1 to 40, to indicate the importance of an event in which more than the specified number of databases are or become active. The default is 15.
Threshold - Maximum number of active databases	Set the highest number of databases that can be active before an event is raised. The default is 3.
Raise event if less than N databases are active?	Select **Yes** to raise an event if less than the specified number of databases are active. The default is Yes.
Raise event only when less than N databases become active?	Select **Yes** to raise an event only when less than the specified number of databases become active. The default is Yes.
Event severity when less than N databases are or become active	Set the severity level, from 1 to 40, to indicate the importance of an event in which less than the specified number of databases are or become active. The default is 15.
Threshold - Minimum number of active databases	Set the lowest number of databases that can be active before an event is raised. The default is 1.

4.23 MBS_DatabaseStatus

Use this Knowledge Script to monitor mailbox databases for the size of online maintenance window, defragmentation time, free log space, free file space, and number of mailboxes. This script raises an event if a monitored value exceeds or falls below the threshold you set. In addition, this script generates data streams for number of mailboxes in a mailbox database and number of mailboxes in a storage group.

A job executed on a database in an Exchange Server 2010, 2013, 2016, and 2019 DAG cause the job to run on all servers in the DAG. However, only the server that currently owns the database monitors that database.

NOTE: Exchange Server 2010, 2013, 2016, and 2019 do not use storage groups.

4.23.1 Prerequisite

To run this Knowledge Script on clustered servers, run the AppManager agent as a domain account with Administrator privileges.

4.23.2 Resource Objects

- Exchange2007_Store_Group

- Exchange2007_Store_Database
- Exchange2007_MailboxServer
- Exchange2007_Store_PFDatabase
- Exchange2010_MailboxServer
- Exchange2010_Store_Database
- Exchange2010_Store_PFDatabase
- Exchange2010_DAG_Databases
- Exchange2013_MailboxServer
- Exchange2013_Store_Database
- Exchange2013_Store_PublicFolder
- Exchange2013_DAG_Databases
- Exchange2016_MailboxServer
- Exchange2016_Store_Database
- Exchange2016_Store_PublicFolder
- Exchange2016_DAG_Databases
- Exchange2019_MailboxServer
- Exchange2019_Store_Database
- Exchange2019_Store_PublicFolder
- Exchange2019_DAG_Databases

4.23.3 Default Schedule

By default, this script runs every 15 minutes.

4.23.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_DatabaseStatus job fails. The default is 5.
Monitor Database Defragmentation	
Monitor Size of Online Maintenance Window	
Event Notification	

Parameter	How to Set It
Raise event if online maintenance window is too small or too large?	Select **Yes** to raise an event if online defragmentation occurs too often or not often enough. The default is Yes. You want to ensure that defragmentation of Exchange database occurs often enough, but not too often. Microsoft recommends every 14 days. If you find that defragmentation takes less time, you can shorten your maintenance window. This script compares the values of two Performance Counters to determine whether the size of the maintenance window should be changed: ◆ Online Defrag Pages Freed/Sec ◆ Online Defrag Pages Read/Sec If the read-to-freed ratio is greater than 100:1, then this script raises an event indicating that the size of the maintenance window is too large and should be reduced. If the read-to-freed ratio is less than 50:1, then this script raises an event indicating that the size of the maintenance window is too small and should be increased.
Event severity when online maintenance window is too small or too large	Set the severity level, from 1 to 40, to indicate the importance of an event in which the maintenance window is too small or too large. The default is 15.
Monitor Defragmentation Time	
Event Notification	
Raise event if time to defragment database exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes to defragment a database exceeds the threshold you set. The default is Yes.
Threshold - Maximum database defragmentation time	Set the maximum length of time allowed for defragmentation before an event is raised. The default is 10 hours.
Event severity when time to defragment database exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time it takes to defragment a database exceeds the threshold. The default is 15.
Monitor Disk Space	
Event Notification	
Raise event if free space/ disk utilization for database files crosses the threshold?	Select **Yes** to raise an event if the amount of disk space available for database files or disk utilization for database files crosses the threshold you set. The default is Yes.
Set threshold for free disk space in MegaBytes	Select **Yes** to set the threshold for free disk space for database files. The default is Yes.
Threshold - Minimum free disk space for database files	Set the minimum amount of disk space that must be available for database files to prevent an event from being raised. The default is 1024 MB.
Event severity when free disk space for database files falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the amount of disk space available for database files falls below the threshold. The default is 5.
Set threshold for disk utilization in Percentage	Select **Yes** to set the threshold for disk utilization for database files. The default is No.

Parameter	How to Set It
Threshold- Maximum disk utilization for database files	Set the maximum percentage of disk utilization for database files that should be utilized before an event is raised. The default is 80%.
Event severity when disk utilization for database files exceeds the threshold?	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of disk utilization for database files exceeds the threshold. The default is 5.
Raise event if free space/ disk utilization for log files crosses the threshold?	Select **Yes** to raise an event if the amount of disk space available for log files or disk utilization for log files crosses the threshold you set. The default is Yes.
Set threshold for free disk space in MegaBytes	Select **Yes** to set the threshold for free disk space for log files. The default is Yes.
Threshold - Minimum free disk space for log files	Set the minimum amount of disk space that must be available for log files to prevent an event from being raised. The default is 1024 MB.
Event severity when free disk space for log files falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the amount of disk space available for log files falls below the threshold. The default is 5.
Set threshold for disk utilization in Percentage	Select **Yes** to set the threshold for disk utilization for log files. The default is No.
Threshold- Maximum disk utilization for log files	Set the maximum percentage of disk utilization for log files that should be utilized before an event is raised. The default is 80%.
Event severity when disk utilization for log files exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of disk utilization for log files exceeds the threshold. The default is 5.
Monitor Mailbox Count	
Monitor Number of Mailboxes Per Storage Group (Exchange 2007 only)	
Event Notification	
Raise event if number of mailboxes in a storage group exceeds threshold?	Select **Yes** to raise an event if the number of mailboxes in a storage group exceeds the threshold you set. The default is Yes. A storage group is a logical container only for Exchange Server 2007 databases and their associated system and transaction log files. Exchange Server 2010, 2013, 2016, and 2019 do not use storage groups.
Threshold - Maximum number of mailboxes in a storage group	Set the maximum number of mailboxes that can be in a storage group before an event is raised. The default is 2500 mailboxes.
Event severity when number of mailboxes in a storage group exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of mailboxes in a storage group exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of mailboxes in each storage group?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of mailboxes in a storage group during the monitoring period. The default is No.
Monitor Number of Mailboxes Per Mailbox Database	
Event Notification	

Parameter	How to Set It
Raise event if number of mailboxes in a mailbox database exceeds threshold?	Select **Yes** to raise an event if the number of mailboxes in a database exceeds the threshold you set. The default is Yes. A database stores data, data definitions, indexes, checksums, flags, and other information associated with user mailboxes or public folders.
Threshold - Maximum number of mailboxes in a mailbox database	Set the maximum number of mailboxes that can be in a database before an event is raised. The default is 1000 mailboxes.
Event severity when number of mailboxes in a mailbox database exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of mailboxes in a database exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of mailboxes in each mailbox database?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of mailboxes in a database during the monitoring period. The default is No.
Monitor Disk Activity and Usage	
Data Collection	
Collect data for percentage of elapsed time that the disk was busy servicing read and write requests?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of time that was spent servicing disk reads and disk writes during the monitoring period. The default is No.
Collect data for percentage of elapsed time that the disk was busy servicing read requests?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of time that was spent servicing disk reads during the monitoring period. The default is No.
Collect data for percentage of elapsed time that the disk was busy servicing write requests?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of time that was spent servicing disk writes during the monitoring period. The default is No.
Collect data for average number of both read and write requests that were queued for the disk during the sample interval?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of read and write requests queued for servicing during the monitoring period. The default is No.

4.24 MBS_MailboxAccessibility

Use this Knowledge Script to monitor whether the Mailbox server can access specified mailboxes. This script raises an event if the time it takes to connect to a mailbox exceeds the threshold you set.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see Section 4.43, “Recommended Knowledge Script Group,” on page 162.

4.24.1 Resource Objects

- Exchange2007_MailboxServer
- Exchange2007_Store_Group
- Exchange2007_Store_Database
- Exchange2010_MailboxServer

- Exchange2013_MailboxServer
- Exchange2016_MailboxServer
- Exchange2019_MailboxServer

4.24.2 Default Schedule

By default, this script runs every 15 minutes.

4.24.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_MailboxAccessibility job fails. The default is 5.
Monitor Mailbox Accessibility	
Name of mailbox to be accessed	Provide the name of the mailbox or the mailbox's SMTP address. For example, a mailbox name, `symadmin`, or an SMTP address, `symadmin@golden.local`.
Event Notification	
Raise event if the mailbox cannot be accessed?	Select **Yes** to raise an event if the Mailbox server cannot access the specified mailbox. The default is Yes. A mailbox is inaccessible when it does not exist.
Event severity when the mailbox cannot be accessed	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Mailbox server cannot access the specified mailbox. The default is 5.
Raise event if response time for accessing the mailbox exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes to connect to the specified mailbox exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time for accessing the mailbox	Set the maximum length of time that the Mailbox server should wait to connect with the specified mailbox before raising an event. The default is 1000 milliseconds. The minimum is 1 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time it takes to access the specified mailbox exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for mailbox access response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the response time for mailbox access during the monitoring period. The default is No.

4.25 MBS_MailboxUsage

Use this Knowledge Script to measure the size of mailboxes by either the number of messages in the mailbox, or by total message size in MB. You can monitor average mailbox size and individual mailbox size for the top *n* mailboxes. This script raises an event if average mailbox size and individual mailbox size exceed the threshold you set.

A job executed on a database in an Exchange Server 2010, 2013, 2016, and 2019 DAG cause the job to run on all servers in the DAG. However, only the server that currently owns the database monitors that database.

4.25.1 Resource Objects

- Exchange2007_MailboxServer
- Exchange2007_Store_Group
- Exchange2007_Store_Database
- Exchange2010_MailboxServer
- Exchange2010_Store_Database
- Exchange2010_DAG_Databases
- Exchange2013_MailboxServer
- Exchange2013_Store_Database
- Exchange2013_DAG_Databases
- Exchange2016_MailboxServer
- Exchange2016_Store_Database
- Exchange2016_DAG_Databases
- Exchange2019_MailboxServer
- Exchange2019_Store_Database
- Exchange2019_DAG_Databases

4.25.2 Default Schedule

By default, this script runs every hour.

4.25.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	

Parameter	How to Set It
Measure mailbox size in MB or by number of messages	Select how you want to measure the size of mailboxes: ◆ Choose **Message count** to measure the size of mailboxes by the number of messages in the mailboxes ◆ Choose **Total message size** to measure the size of all messages in the mailboxes in MB. The default is Total message size.
Comma-separated list of mailboxes to ignore	Provide a list of mailbox display names that this script should ignore when measuring mailbox size. Separate the names with a comma. **NOTE:** Ensure you provide the mailbox display name, not the mailbox alias.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_MailboxUsage job fails. The default is 5.
Monitor Average Mailbox Size	
Number of largest mailboxes to be averaged	Set the top *n* mailboxes whose average size you want to monitor. The default is 10 mailboxes, the minimum is 0, and the maximum is 2147483647
Event Notification	
Raise event if average mailbox size exceeds threshold?	Select **Yes** to raise an event if the average size of the top *n* mailboxes exceeds the threshold you set. The default is Yes. Use the *Number of largest mailboxes to be averaged* parameter to determine the value of *n*. AppManager uses Exchange cmdlets to determine the largest mailboxes, based on number and size of mailboxes and messages.
Threshold -- Maximum average mailbox size in MB or by number of messages	Set the maximum average size that the top *n* mailboxes can attain before an event is raised. The default is 100. The average is based on either the total number of messages in the top *n* mailboxes, or the total size in MB of the top *n* mailboxes, depending on your selection in the *Measure mailbox size by total message size or message count* parameter.
Event severity when average mailbox size exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the average size of the top *n* mailboxes exceeds the threshold. The default is 5.
Data Collection	
Collect data for average mailbox size?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns one of the following data streams: ◆ Average number of messages in *n* largest mailboxes ◆ Average size in MB of the *n* largest mailboxes The default is No.
Monitor Individual Mailbox Size	
Number of largest mailboxes to be monitored	Set the top *n* mailboxes whose individual size you want to monitor. The default is 10 mailboxes, the minimum is 0, and the maximum is 2147483647.

Parameter	How to Set It
Event Notification	
Raise event if individual mailbox size exceeds threshold?	Select **Yes** to raise an event if the size of any one of the top *n* mailboxes exceeds the threshold you set. The default is Yes. Use the *Number of largest mailboxes to be monitored* parameter to determine the value of *n*. AppManager uses Exchange cmdlets to determine the largest mailboxes, based on number and size of mailboxes and messages.
Threshold - Maximum individual mailbox size in MB or by number of messages	Set the maximum size that any one of the top *n* mailboxes can attain before an event is raised. The default is 250. The size is based on either the total number of messages in the top *n* mailboxes, or the total size in MB of the top *n* mailboxes, depending on your selection in the *Measure mailbox size by message count or total message size* parameter.
Event severity when individual mailbox size exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the size of any one of the top *n* mailboxes exceeds the threshold. The default is 5.
Data Collection	
Collect data for individual mailbox size?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the following data streams: ◆ Number of messages in each of the *n* largest mailboxes ◆ Size in MB of each of the *n* largest mailboxes Use the *Number of largest mailboxes to be monitored* parameter to determine the value of *n*. The default is No.

4.26 MBS_MailFlow

Use this Knowledge Script to test the flow of mail by sending test e-mail to local or remote Mailbox servers. This script raises an event if the test fails or if response time exceeds the threshold you set.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see Section 4.43, “Recommended Knowledge Script Group,” on page 162.

4.26.1 Resource Objects

- Exchange2007_MailboxServer
- Exchange2010_MailboxServer
- Exchange2013_MailboxServer
- Exchange2016_MailboxServer
- Exchange2019_MailboxServer

4.26.2 Default Schedule

By default, this script runs every 15 minutes.

4.26.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_MailFlow job fails. The default is 5.
Monitor Mail Flow	
Comma-separated list of target Mailbox servers	Provide the hostnames or IP addresses of the Mailbox servers to which you want to send test e-mail. Separate the names or addresses with a comma.
Comma-separated list of recipient e-mail addresses	Provide the e-mail addresses to which you want to send test e-mail. Separate the addresses with a comma.
Event Notification	
Raise event if mail flow test fails?	Select **Yes** to raise an event if test mail cannot be sent to the selected Mailbox servers. The default is Yes.
Event severity when mail flow test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which test mail cannot be sent to the selected Mailbox servers. The default is 5.
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the elapsed time to send mail to the Mailbox servers exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time for mail flow test	Set the maximum number of milliseconds that can elapse while sending mail to the selected Mailbox servers before an event is raised. The default is 10,000 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which response time exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for mail flow response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the response time for the mail flow tests during the monitoring period. The default is No.

4.27 MBS_MessagingRecordsMgmt

Use this Knowledge Script to monitor Messaging Records Management (MRM) tasks such as deleting, journaling, moving, and retention, and to monitor the Windows Event log for MRM-related events. This script raises an event if a threshold is exceeded.

4.27.1 Resource Objects

- Exchange2007_MailboxServer
- Exchange2010_MailboxServer
- Exchange2013_MailboxServer
- Exchange2016_MailboxServer
- Exchange2019_MailboxServer

4.27.2 Default Schedule

By default, this script runs every 15 minutes.

4.27.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_MessagingRecordsManagement job fails. The default is 5.
Monitor Messaging Records Management	
Monitor Messages Deleted But Recoverable	
Event Notification	
Raise event if number of messages deleted but recoverable exceeds threshold?	Select **Yes** to raise an event if the number of deleted, but recoverable, messages exceeds the threshold you set. The default is Yes. Exchange can recover messages that users have deleted from their Deleted Items folders. You can use Exchange System Manager to define how many days a deleted message stays in the mailbox store before being permanently deleted.
Event severity when number of messages deleted but recoverable exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of recoverable messages exceeds the threshold you set. The default is 15.
Threshold - Maximum number of messages deleted but recoverable	Set the maximum number of recoverable messages that can be in the mailbox store before an event is raised. The default is 1000 messages.
Data Collection	
Collect data for number of messages deleted but recoverable?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of recoverable messages deleted during the monitoring interval. The default is Yes.
Monitor Messages Permanently Deleted	
Event Notification	

Parameter	How to Set It
Raise event if number of messages permanently deleted exceeds threshold?	Select **Yes** to raise an event if the number of permanently deleted messages exceeds the threshold you set. The default is Yes. You can use Exchange System Manager to define how many days a deleted message stays in the mailbox store before being permanently deleted.
Event severity when number of messages permanently deleted exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of permanently deleted messages exceeds the threshold you set. The default is 15.
Threshold - Maximum number of messages permanently deleted	Set the maximum number of messages that can be permanently deleted before an event is raised. The default is 1000 messages.
Data Collection	
Collect data for number of messages permanently deleted?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages permanently deleted during the monitoring interval. The default is Yes.
Monitor Messages Journaled	
Event Notification	
Raise event if number of messages journaled exceeds threshold?	Select **Yes** to raise an event if the number of journaled, or archived, messages exceeds the threshold you set. The default is Yes. The Exchange Journaling feature allows users to archive all incoming and outgoing e-mail for a specific mailbox store.
Event severity when number of messages journaled exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of archived messages exceeds the threshold you set. The default is 15.
Threshold - Maximum number of messages journaled	Set the maximum number of messages that can be archived before an event is raised. The default is 1000 messages.
Data Collection	
Collect data for number of messages journaled?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages journaled during the monitoring interval. The default is Yes.
Monitor Messages Moved	
Event Notification	
Raise event if number of messages moved exceeds threshold?	Select **Yes** to raise an event if the number of messages moved from one managed folder to another exceeds the threshold you set. The default is Yes.
Event severity when number of messages moved exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of moved messages exceeds the threshold you set. The default is 15.
Threshold - Maximum number of messages moved	Set the maximum number of messages that can be moved before an event is raised. The default is 1000 messages.
Data Collection	
Collect data for number of messages moved?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages moved during the monitoring interval. The default is Yes.

Parameter	How to Set It
Monitor Messages Past Retention	
Event Notification	
Raise event if number of messages marked as past retention date exceeds threshold?	Select **Yes** to raise an event if the number of deleted messages that have passed their retention date exceeds the threshold you set. The default is Yes. Use Exchange System Manager to define how many days a deleted message stays in the mailbox store.
Event severity when number of messages marked as past retention date exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of expired messages exceeds the threshold you set. The default is 15.
Threshold - Maximum number of messages marked as past retention date	Set the maximum number of messages that can have passed their retention date before an event is raised. The default is 1000 messages.
Data Collection	
Collect data for number of messages marked as past retention date?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages that expired during the monitoring interval. The default is Yes.
Monitor Windows Event Log for Messaging Records Management Events	
Event Notification	
Comma-separated list of event sources to ignore	Provide a list of event sources that this script should ignore when scanning the Windows Event log. Separate the source names with a comma. Event sources are computers whose names are displayed in the Source column of the event log.
Comma-separated list of event categories to ignore	Provide a list of event categories that this script should ignore when scanning the Windows Event log. Separate the category names with a comma.
Comma-separated list of event IDs to ignore	Provide a list of error and warning ID numbers that this script should ignore when scanning the Windows Event log. Separate the numbers with a comma.
Raise event if MRM error events are found?	Select **Yes** to raise an event if MRM error events are found in the Windows Event Log. The default is Yes.
Event severity when MRM error events are found	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Windows Event Log contains MRM error events. The default is 10.
Raise event if MRM warning events are found?	Select **Yes** to raise an event if MRM warning events are found in the Windows Event Log. The default is Yes.
Event severity when MRM warning events are found	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Windows Event Log contains MRM warning events. The default is 20.

4.28 MBS_PublicFolderUsage

Use this Knowledge Script to measure the size of public folders by the number of messages in the folders or by total message size in MB. You can monitor average folder size and individual folder size for the top *n* folders. This script raises an event if average folder size and individual folder size exceed the threshold you set.

4.28.1 Resource Objects

- Exchange2007_Store_Group
- Exchange2007_Store_PFDatabase
- Exchange2010_Store_PFDatabase
- Exchange2013_Store_PFDatabase
- Exchange2016_Store_PFDatabase
- Exchange2019_Store_PFDatabase

4.28.2 Default Schedule

By default, this script runs every one hour.

4.28.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Measure public folder size by message count or total message size	Select how you want to measure the size of public folders: ◆ Choose **Message count** to measure the size of folders by the number of messages in the mailboxes. ◆ Choose **Total message size** to measure the size of all messages in the folders in MB. The default is Total message size.
Comma-separated list of public folders to ignore	Provide a list of public folder names that this script should ignore when measuring folder size. Separate the names with a comma.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_PublicFolderUsage job fails. The default is 5.
Monitor Average Public Folder Size	
Number of largest public folders to be averaged	Set the top *n* public folders whose average size you want to monitor. The default is 10 folders.
Event Notification	

Parameter	How to Set It
Raise event if average public folder size exceeds threshold?	Select **Yes** to raise an event if the average size of the top *n* public folders exceeds the threshold you set. The default is Yes. Use the *Number of largest public folders to be averaged* parameter to determine the value of *n*. AppManager uses Exchange cmdlets to determine the largest public folders, based on number and size of folders and messages.
Threshold - Maximum average public folder size	Set the maximum average size that the top *n* public folders can attain before an event is raised. The default is 25. The average is based on either the total number of messages in the top *n* folders, or the total size in MB of the top *n* folders, depending on your selection in the *Measure public folder size by message count or total message size* parameter.
Event severity when average public folder size exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the average size of the top *n* public folders exceeds the threshold. The default is 5.
Data Collection	
Collect data for average public folder size?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns one of the following data streams: ◆ Average number of messages in *n* largest public folders ◆ Average size (MB) of the *n* largest public folders The default is No.
Monitor Individual Public Folder Size	
Number of largest public folders to be monitored	Set the top *n* public folders whose individual size you want to monitor. The default is 10 folders.
Event Notification	
Raise event if individual public folder size exceeds threshold?	Select **Yes** to raise an event if the size of any one of the top *n* public folders exceeds the threshold you set. The default is Yes. Use the *Number of largest public folders to be monitored* parameter to determine the value of *n*. AppManager uses Exchange cmdlets to determine the largest public folders, based on number and size of folders and messages.
Threshold - Maximum individual public folder size	Set the maximum size that any one of the top *n* public folders can attain before an event is raised. The default is 100. The size is based on either the total number of messages in the top *n* public folders, or the total size in MB of the top *n* public folders, depending on your selection in the *Measure public folder size by message count or total message size* parameter.
Event severity when individual public folder size exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the size of any one of the top *n* public folders exceeds the threshold. The default is 5.
Data Collection	

Parameter	How to Set It
Collect data for individual public folder size?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the following data streams: ◆ Number of messages in each of the *n* largest public folders ◆ Size (MB) of each of the *n* largest public folders Use the *Number of largest public folders to be monitored* parameter to determine the value of *n*. The default is No.

4.29 MBS_Replication

Use this Knowledge Script to monitor replication status and performance for a Mailbox server. This script raises an event when a threshold is exceeded and generates data streams for the following metrics:

- Replication latency
- Number of pending replication transactions
- Replication rate
- Number of replications in the copy and replay queues

This script also monitors the availability of the File Share Witness, a requirement for using the cluster continuous replication (CCR) functionality in Exchange Server 2007. CCR enables the continuous and asynchronous updating of a second copy of a database with the changes that have been made to the active copy of the database. The File Share Witness is a file share that is external to a cluster and helps determine the status of the cluster.

4.29.1 Prerequisite

The AppManager agent (`netiqmc` service) must have permission to access the File Share Witness folder to collect data for File Share Witness usage on a two-node CCR cluster.

4.29.2 Resource Objects

- Exchange2007_MailboxServer
- Exchange2010_MailboxServer
- Exchange2013_MailboxServer
- Exchange2016_MailboxServer
- Exchange2019_MailboxServer

4.29.3 Default Schedule

By default, this script runs every 15 minutes.

4.29.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Communicate only with Exchange servers in the local domain?	Select **Yes** to test only Exchange servers in the same domain as the server on which you run the MBS_Replication job. The default is No. When this option is unselected, the job attempts to contact *all* Exchange Servers in your organization. These attempts will fail if the Exchange accounts in one domain do not have access to other domains.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_Replication job fails. The default is 5.
Monitor Replication Agent	
Event Notification	
Raise event if replication agent is not running?	Select **Yes** to raise an event if the replication agent is not running. The default is Yes.
Event severity when replication agent is not running	Set the severity level, from 1 to 40, to indicate the importance of an event in which the replication agent is not running. The default is 5.
Start replication agent if not running?	Select **Yes** to start the replication agent if it is not running. The default is Yes.
Threshold - Maximum timeout for starting replication agent	Set the maximum length of time the script can attempt to start the replication agent before timing out and raising an event. The default is 60 seconds.
Raise event if replication agent fails to start?	Select **Yes** to raise an event if the script cannot start the replication agent. The default is Yes.
Event severity when replication agent fails to start	Set the severity level, from 1 to 40, to indicate the importance of an event in which the script cannot start the replication agent. The default is 5.
Monitor Replication Copy Status	
Comma-separated list of mailbox stores to ignore	Specify a list of mailbox stores, separated by comma, for which the replication status will not be monitored.
Event Notification	
Raise event if replication is unhealthy?	Select **Yes** to raise an event if replication is unhealthy. The default is Yes. This script uses the `Get-StorageGroupCopyStatus` cmdlet to determine the status, or health, of the replication function. If the status is `Failed` or `Not Supported`, then replication is considered unhealthy. Replication is also considered unhealthy if the number of transactions in the copy queue or the replay queue exceeds the threshold you set.
Threshold - Maximum length of copy queue	Set the maximum number of transactions that can be waiting in the copy queue before an event is raised. The default is 3 transactions.
Threshold - Maximum length of replay queue	Set the maximum number of transactions that can be waiting in the replay queue before an event is raised. The default is 20 transactions.

Parameter	How to Set It
Event severity when replication is unhealthy	Set the severity level, from 1 to 40, to indicate the importance of an event in which replication is determined to be unhealthy. The default is 5.
Data Collection	
Collect data for copy queue length?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of replication transactions in the copy queue for the monitoring period. The default is No.
Collect data for replay queue length?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of replication transactions in the replay queue for the monitoring period. The default is No.
Monitor File Share Witness	
Raise event if File Share Witness is unavailable?	Select **Yes** to raise an event if the File Share Witness is unavailable. The default is Yes.
Event severity when File Share Witness is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which the File Share Witness is unavailable. The default is 15.
Monitor File Share Witness Usage on Two-node CCR Setup	
Data Collection	
Collect data for File Share Witness usage on two-node CCR setup?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of usage for the File Share Witness in a two-node cluster continuous replication environment. The default is No.
Monitor Replication Latency	
Event Notification	

Raise event if replication latency exceeds threshold?	Select **Yes** to raise an event if replication latency exceeds the threshold you set. The default is Yes.
	
	When this parameter is set to **Yes**, the Extended ESE performance counters in the registry are enabled. The following updates are made automatically in the registry values:
	
	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ESE\Performance`
	
	`Value Name: Show Advanced Counters`
	
	`Data Type: REG_DWORD`
	
	`Value: 1`

Threshold -- Maximum replication latency	Set the maximum number of milliseconds allowed for replication latency before an event is raised. The default is 20000 milliseconds.
Event severity when replication latency exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which replication latency exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for replication latency?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the total latency for the monitoring period. The default is No.
Monitor Replication Rate	
Event Notification	

Parameter	How to Set It
Raise event if replication rate exceeds threshold?	Select **Yes** to raise an event if the replication rate exceeds the threshold you set. The default is Yes.
Threshold -- Maximum replication rate	Set the maximum number of replications allowed per minute before an event is raised. The default is 10000 transactions.
Event severity when replication rate threshold exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the replication rate exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for replication rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the replication rate for the monitoring period. The default is No.
Monitor Pending Replication Transactions	
Event Notification	
Raise event if pending replication transactions exceed threshold?	Select **Yes** to raise an event if the number of transactions waiting to be replicated exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of pending replication transactions	Set the maximum number of transactions that can be awaiting replication before an event is raised. The default is 500 transactions.
Event severity when pending replication transactions exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of transactions waiting to be replicated exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for pending replication transactions?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of pending replication transactions for the monitoring period. The default is No.

4.30 Report_CopyQueueLength

As of AppManager for Exchange Server 2007 version 7.3, this Knowledge Script is obsolete. Its functionality has been replaced by an Analysis Center report: Average length of the copy queue.

****

Use this Knowledge Script to display the number of transaction log files waiting to be copied to the passive copy log file folder.

This report uses data collected by the MBS_Replication Knowledge Script.

4.30.1 Resource Object

REPORT_REPExchange

4.30.2 Default Schedule

The default schedule is **Run once**.

4.30.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data source	
Select computer(s)	Click Browse [...] to select the computers for your report.
Select the style	Select the style for the first page of the report: ◆ **By computer** provides links to pages showing the data collected from individual computers. Each page shows all the data streams collected from a single computer. ◆ **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers. ◆ **By computer and data stream** provides links to pages showing a single data stream collected from a computer ◆ **All data streams on one page** generates a report with all data on a single page
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse [...]** to select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: ◆ Minute ◆ Hour ◆ Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 60.
Statistics to show per period	Select a statistical method by which to display data in the report: ◆ **Average**: The average value of data points for the aggregation interval. ◆ **Minimum**: The minimum value of data points for the aggregation interval ◆ **Maximum**: The maximum value of data points for the aggregation interval ◆ **Count**: The number of data points for the aggregation interval ◆ **Sum**: The total value of data points for the aggregation interval ◆ **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) ◆ **Std**: The standard deviation ◆ **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval ◆ **Open**: The first value for the aggregation interval ◆ **Close**: The last value for the aggregation interval
Report settings	
Include parameter help card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.

Parameter	How to Set It
Include Table or Chart?	Set whether to include a table of data stream values and/or a chart of data stream values in the report. Choose from **Both**, **Table**, or **Chart**. The default is Both.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Select Yes to append the job ID to the name of the output folder. The default is No. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Click **Browse [...]** to set the report properties as desired.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of the report, to assign a unique title to each report. The time stamp consists of the date and time the report was generated. Adding a time stamp is useful for running consecutive iterations of the same report without overwriting the previous report. The default is No.
Event notification	
Event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the generated report has no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report generation fails. The default is 5 (red level indicator).

4.31 Report_DiskUsageStatus

As of AppManager for Exchange Server 2007 version 7.3, this Knowledge Script is obsolete. Its functionality has been replaced by an Analysis Center report: Average disk usage.

****

Use this Knowledge Script to summarize the percentage of time required for disk access, read, and write operations. This script also provides the average queued requests relating to disk usage.

4.31.1 Resource Object

REPORT_REPExchange

4.31.2 Default Schedule

The default schedule is **Run once**.

4.31.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data source	
Select computer(s)	Click Browse [...] to select the computers for your report.
Select the style	Select the style for the first page of the report: ◆ **By computer** provides links to pages showing the data collected from individual computers. Each page shows all the data streams collected from a single computer. ◆ **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers. ◆ **By computer and data stream** provides links to pages showing a single data stream collected from a computer ◆ **All data streams on one page** generates a report with all data on a single page
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse [...]** to select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: ◆ Minute ◆ Hour ◆ Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 60.
Statistics to show per period	Select a statistical method by which to display data in the report: ◆ **Average**: The average value of data points for the aggregation interval. ◆ **Minimum**: The minimum value of data points for the aggregation interval ◆ **Maximum**: The maximum value of data points for the aggregation interval ◆ **Count**: The number of data points for the aggregation interval ◆ **Sum**: The total value of data points for the aggregation interval ◆ **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) ◆ **Std**: The standard deviation ◆ **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval ◆ **Open**: The first value for the aggregation interval ◆ **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.

Parameter	How to Set It
Include Table or Chart?	Set whether to include a table of data stream values and/or a chart of data stream values in the report. Choose from **Both**, **Table**, or **Chart**. The default is Both.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Select Yes to append the job ID to the name of the output folder. The default is No. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Click **Browse [...]** to set the report properties as desired.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of the report, to assign a unique title to each report. The time stamp consists of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting the previous report. The default is No.
Event notification	
Event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the generated report has no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report generation fails. The default is 5 (red level indicator).

4.32 Report_DataLostInReplication

As of AppManager for Exchange Server 2007 version 7.3, this Knowledge Script is obsolete.

****

Use this Knowledge Script to generate a report for the time gap between the failure of a node and the last e-mail in the transport dumpster.

4.32.1 Resource Object

Exchange_MailboxServer

4.32.2 Default Schedule

The default interval for this script is **Run once**.

4.32.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data source	
Select computer(s)	Click Browse [...] to select the computers for your report.
Select the style	Select the style for the first page of the report: ◆ **By computer** provides links to pages showing the data collected from individual computers. Each page shows all the data streams collected from a single computer. ◆ **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers ◆ **By computer and data stream** provides links to pages showing a single data stream collected from a computer ◆ **All data streams on one page** generates a report with all data on a single page
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse [...]** to select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: ◆ Minute ◆ Hour ◆ Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 60.
Statistics to show per period	Select a statistical method by which to display data in the report: ◆ **Average**: The average value of data points for the aggregation interval (for example, the average value 1 Hour) ◆ **Minimum**: The minimum value of data points for the aggregation interval ◆ **Maximum**: The maximum value of data points for the aggregation interval ◆ **Count**: The number of data points for the aggregation interval ◆ **Sum**: The total value of data points for the aggregation interval ◆ **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) ◆ **Std**: The standard deviation ◆ **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval ◆ **Open**: The first value for the aggregation interval ◆ **Close**: the last value for the aggregation interval
Report settings	

Parameter	How to Set It
Include parameter help card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include Table or Chart?	Set whether to include a table of data stream values and/or a chart of data stream values in the report. Choose from **Both**, **Table**, or **Chart**. The default is Both.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Select Yes to append the job ID to the name of the output folder. The default is No. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Click **Browse [...]** to set the report properties as desired.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is No.
Event notification	
Event for report success? (yes/no)	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the generated report has no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report generation fails. The default is 5 (red level indicator).

4.33 Report_FileShareWitnessUsage

As of AppManager for Exchange Server 2007 version 7.3, this Knowledge Script is obsolete. Its functionality has been replaced by an Analysis Center report: Average use of File Share Witness.

****

Use this Knowledge Script to summarize the percentage of File Share Witness used at a given instance. This script indicates whether the file share witness is connected between the servers.

NOTE: Run this script on Exchange Server 2007 resources installed only in a CCR (Copy Continuous Replication) environment.

4.33.1 Resource Object

REPORT_REPExchange

4.33.2 Default Schedule

The default schedule is **Run once**.

4.33.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data source	
Select computer(s)	Click Browse [...] to select the computers for your report.
Select the style	Select the style for the first page of the report: ◆ **By computer** provides links to pages showing the data collected from individual computers. Each page shows all the data streams collected from a single computer. ◆ **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers. ◆ **By computer and data stream** provides links to pages showing a single data stream collected from a computer ◆ **All data streams on one page** generates a report with all data on a single page
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse [...]** to select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: ◆ Minute ◆ Hour ◆ Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 60.

Parameter	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: ◆ **Average**: The average value of data points for the aggregation interval. For example, the average value 1 Hour. ◆ **Minimum**: The minimum value of data points for the aggregation interval ◆ **Maximum**: The maximum value of data points for the aggregation interval ◆ **Count**: The number of data points for the aggregation interval ◆ **Sum**: The total value of data points for the aggregation interval ◆ **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) ◆ **Std**: The standard deviation ◆ **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval ◆ **Open**: The first value for the aggregation interval ◆ **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include Table or Chart?	Set whether to include a table of data stream values and/or a chart of data stream values in the report. Choose from **Both**, **Table**, or **Chart**. The default is Both.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Select Yes to append the job ID to the name of the output folder. The default is No. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Click **Browse [...]** to set the report properties as desired.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of the report, making each title unique. The time stamp consists of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is No.
Event notification	
Event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the generated report has no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report generation fails. The default is 5 (red level indicator).

4.34 Report_ReplayQueueLength

As of AppManager for Exchange Server 2007 version 7.3, this Knowledge Script is obsolete. Its functionality has been replaced by an Analysis Center report: Average number of logs in the replay queue.

****

Use this Knowledge Script to summarize the number of transaction log files waiting to be replayed into the passive copy log file folder.

4.34.1 Resource Object

REPORT_REPExchange

4.34.2 Default Schedule

The default schedule is **Run once**.

4.34.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data source	
Select computer(s)	Click Browse [...] to select the computers for your report.
Select the style	Select the style for the first page of the report: ◆ **By computer** provides links to pages showing the data collected from individual computers. Each page shows all the data streams collected from a single computer. ◆ **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers. ◆ **By computer and data stream** provides links to pages showing a single data stream collected from a computer ◆ **All data streams on one page** generates a report with all data on a single page
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse [...]** to select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: ◆ Minute ◆ Hour ◆ Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 60.

Parameter	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: ◆ **Average**: The average value of data points for the aggregation interval. ◆ **Minimum**: The minimum value of data points for the aggregation interval ◆ **Maximum**: The maximum value of data points for the aggregation interval ◆ **Count**: The number of data points for the aggregation interval ◆ **Sum**: The total value of data points for the aggregation interval ◆ **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) ◆ **Std**: The standard deviation ◆ **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval ◆ **Open**: The first value for the aggregation interval ◆ **Close**: The last value for the aggregation interval
Report settings	
Include parameter help card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include Table or Chart?	Set whether to include a table of data stream values and/or a chart of data stream values in the report. Choose from **Both**, **Table**, or **Chart**. The default is Both.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Select Yes to append the job ID to the name of the output folder. The default is No. A job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Click **Browse [...]** to set the report properties as desired.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of the report, to assign a unique title to each report. The time stamp consists of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting the previous report. The default is No.
Event notification	
Event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the generated report has no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report generation fails. The default is 5 (red level indicator).

4.35 Report_TransDumpUsage

As of AppManager for Exchange Server 2007 version 7.3, this Knowledge Script is obsolete. Its functionality has been replaced by an Analysis Center report: Average use of Transport Dumpster queue.

****

Use this Knowledge Script to summarize the number of e-mail in the dumpster at a given instance and also the space allocated for the transport dumpster.

4.35.1 Resource Object

REPORT_REPExchange

4.35.2 Default Schedule

The default interval for this script is **Run once**.

4.35.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data source	
Select computer(s)	Click Browse [...] to select the computers for your report.
Select the style	Select the style for the first page of the report: ◆ **By computer** provides links to pages showing the data collected from individual computers. Each page shows all the data streams collected from a single computer. ◆ **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers. ◆ **By computer and data stream** provides links to pages showing a single data stream collected from a computer ◆ **All data streams on one page** generates a report with all data on a single page
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse [...]** to select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: ◆ Minute ◆ Hour ◆ Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 60.

Parameter	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: ◆ **Average**: The average value of data points for the aggregation interval (for example, the average value 1 Hour) ◆ **Minimum**: The minimum value of data points for the aggregation interval ◆ **Maximum**: The maximum value of data points for the aggregation interval ◆ **Count**: The number of data points for the aggregation interval ◆ **Sum**: The total value of data points for the aggregation interval ◆ **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) ◆ **Std**: The standard deviation ◆ **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval ◆ **Open**: The first value for the aggregation interval ◆ **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include Table or Chart?	Set whether to include a table of data stream values and/or a chart of data stream values in the report. Choose from **Both**, **Table**, or **Chart**. The default is Both.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Select Yes to append the job ID to the name of the output folder. The default is No. A job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Click **Browse [...]** to set the properties parameters as desired.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of the report, making each title unique. The time stamp consists of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is No.
Event notification	
Event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the generated report has no data. The default is 25 (blue level indicator).

Parameter	How to Set It
Severity level for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red level indicator).

4.36 Transport_BackPressure

Use this Knowledge Script to monitor the status of back pressure for the Hub Transport server.

Back pressure monitors system resources, such as available disk space and available memory, on computers that have the Hub Transport server role or Edge Transport server role installed. If resource usage exceeds a certain level, the Exchange server stops accepting new connections and messages, but may continue to deliver existing messages. When resource usage returns to a normal level, the Exchange server accepts new connections and messages.

This script raises events for three levels of resource usage:

- **Normal**. No back pressure is applied to the server: new connections and messages are accepted.
- **Medium**. The resource is slightly overused. Limited back pressure is applied to the server: incoming mail from the authoritative domain is allowed, but new connections and messages from other sources are rejected.
- **High**. The resource is severely overused. Full back pressure is applied to the server: all message flow stops, and all new connections and messages are rejected.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see Section 4.43, “Recommended Knowledge Script Group,” on page 162.

4.36.1 Resource Objects

- Exchange2007_HubTransportServer
- Exchange2007_EdgeTransportServer
- Exchange2010_HubTransportServer
- Exchange2010_EdgeTransportServer
- Exchange2013_HubTransportServer
- Exchange2016_HubTransportServer
- Exchange2019_HubTransportServer

4.36.2 Default Schedule

By default, this script runs every five minutes.

4.36.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	

Parameter	How to Set It
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Transport_BackPressure job fails. The default is 5.
Monitor Back Pressure Status	
Event Notification	
Raise event if back pressure is high?	Select **Yes** to raise an event if resource usage is at a high level. The default is Yes.
Event severity when back pressure is high	Set the severity level, from 1 to 40, to indicate the importance of an event in which resource usage is at a high level. The default is 5.
Raise event if back pressure is medium?	Select **Yes** to raise an event if resource usage is at a medium level. The default is Yes.
Event severity when back pressure is medium	Set the severity level, from 1 to 40, to indicate the importance of an event in which resource usage is at a medium level. The default is 10.

4.37 Transport_ConnectorStatus

Use this Knowledge Script to monitor the status of send, receive, foreign, and delivery agent connectors on Exchange Servers. This script raises an event if any of the connector is disabled or an SMTP-based receive connector is not responding to SMTP requests.

NOTE: The delivery agent connectors are not applicable on Exchange Server 2007.

4.37.1 Resource Objects

- Exchange2007_HubTransportServer
- Exchange2007_EdgeTransportServer
- Exchange2010_HubTransportServer
- Exchange2010_EdgeTransportServer
- Exchange2013_ClientAccessServer
- Exchange2013_HubTransportServer
- Exchange2016_HubTransportServer
- Exchange2019_HubTransportServer

4.37.2 Default Schedule

By default, this script runs every 15 minutes.

4.37.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Transport_ConnectorStatus job fails. The default is 5.
Monitor Connectors	
Monitor Receive Connectors	
Event Notification	
Raise event if any receive connector is disabled	Select **Yes** to raise an event if any of the connector to receive messages on Exchange Server is disabled. The default is Yes. The receive connectors receive e-mail from a Mailbox server or from the Internet when an Edge role is not set up in the Exchange environment.
Comma-separated list of receive connectors to ignore	Specify a list of receive connectors separated by a comma, in the <hostname>\<connectorname> format that you want to exclude from monitoring.
Event severity when any receive connector is disabled	Set the severity level, from 1 to 40, to indicate the importance of an event in which a connector to receive messages on Exchange Server is disabled. The default is 5.
Raise event if an enabled receive connector does not respond to SMTP requests?	Select **Yes** to raise an event if a receive connector is unable to respond to SMTP requests. The default is Yes.
Event severity when a receive connector does not respond to SMTP requests	Set the severity level, from 1 to 40, to indicate the importance of an event in which a receive connector is unable to respond to SMTP requests. The default is 5.
Monitor Send Connectors	
Event Notification	
Raise event if any send connector is disabled	Select **Yes** to raise an event if a connector to send messages from Exchange Server is disabled. The default is Yes. The send connectors send e-mail to the mailbox of the intended recipient or to the Edge Transport server for delivery to another domain.
Comma-separated list of send connectors to ignore	Specify a list of send connector names, separated by a comma, that you want to exclude from monitoring.
Event severity when any send connector is disabled	Set the severity level, from 1 to 40, to indicate the importance of an event in which a connector to send messages from Exchange Server is disabled. The default is 5.
Monitor Foreign Connectors	

Parameter	How to Set It
Raise event if any foreign connector is disabled?	Select **Yes** to raise an event if a foreign connector is disabled. The default is Yes. The foreign connectors move e-mail to a server within the organization that does not communicate using SMTP.
Comma-separated list of foreign connectors to ignore	Specify a list of foreign connector names, separated by a comma, that you want to exclude from monitoring.
Event severity when any foreign connector is disabled	Set the severity level, from 1 to 40, to indicate the importance of an event in which a foreign connector is disabled. The default is 5.
Monitor Delivery Agent Connectors	
Raise event if any delivery agent connector is disabled?	Select **Yes** to raise an event if a delivery agent connector is disabled. The default is Yes.
Comma-separated list of delivery agent connectors to ignore	Specify a list of delivery agent connector names, separated by a comma, that you want to exclude from monitoring.
Event severity when any delivery agent connector is disabled	Set the severity level, from 1 to 40, to indicate the importance of an event in which a delivery agent connector is disabled. The default is 5.

4.38 Transport_QueueStatus

Use this Knowledge Script to monitor the number of messages in Hub Transport server queues:

- **Submission queue**, which contains messages waiting to be categorized and routed to a delivery queue.
- **Mailbox delivery queue**, which contains messages awaiting delivery to mailboxes on a Mailbox server that is located in the same site as the Hub Transport server.
- **Remote delivery queue**, which contains messages awaiting delivery to mailboxes outside the Active Directory site in which the Hub Transport server is located.
- **Poison message queue**, which is a quarantine destination for messages identified as potentially fatal to your Exchange Server environment.
- **Unreachable destination queue**, which contains messages that cannot be routed to their destinations.

This script raises an event if the length of a queue or the change in the length of a queue exceeds the threshold you set.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see Section 4.43, “Recommended Knowledge Script Group,” on page 162.

4.38.1 Resource Objects

- Exchange2007_Queue
- Exchange2007_EdgeTransportServer
- Exchange2007_HubTransportServer
- Exchange2010_Queue

- Exchange2010_EdgeTransportServer
- Exchange2010_HubTransportServer
- Exchange2013_Queue
- Exchange2013_EdgeTransportServer
- Exchange2013_HubTransportServer
- Exchange2016_Queue
- Exchange2016_EdgeTransportServer
- Exchange2016_HubTransportServer
- Exchange2019_Queue
- Exchange2019_EdgeTransportServer
- Exchange2019_HubTransportServer

4.38.2 Default Schedule

By default, this script runs every 15 minutes.

4.38.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Transport_QueueStatus job fails. The default is 5.
Monitor Submission Queue	
Event Notification	
Raise event if number of queued messages exceeds threshold?	Select **Yes** to raise an event if the number of messages in the submission queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of messages in queue	Set the maximum number of messages that can be waiting in the submission queue before an event is raised. The default is 100 messages.
Event severity when number of messages in queue exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of messages in the submission queue exceeds the threshold you set. The default is 15.
Raise event if increase in queued messages exceeds threshold?	Select **Yes** to raise an event if the percentage of increase in the number of messages in the submission queue exceeds the threshold. The script measures the rate of increase since the last iteration of the job. The default is No.
Threshold - Maximum percent increase in queued messages since last job iteration	Set the maximum acceptable percentage of increase in queue size since the last job iteration. AppManager raises an event if the percentage of increase exceeds this value. The default is 50%.

Parameter	How to Set It
Event severity when increase in queued messages exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in the number of messages in the submission queue exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of messages in the submission queue?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages in the submission queue during the monitoring interval. The default is No.
Monitor Mailbox Delivery Queue	
Event Notification	
Raise event if number of queued messages exceeds threshold?	Select **Yes** to raise an event if the number of messages in the mailbox delivery queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of messages in queue	Set the maximum number of messages that can be waiting in the mailbox delivery queue before an event is raised. The default is 250 messages.
Event severity when number of messages in queue exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of messages in the mailbox delivery queue exceeds the threshold you set. The default is 15.
Raise event if increase in queued messages exceeds threshold?	Select **Yes** to raise an event if the percentage of increase in the number of messages in the mailbox delivery queue exceeds the threshold. The script measures the rate of increase since the last iteration of the job. The default is No.
Threshold - Maximum percent increase in queued messages since last job iteration	Set the maximum acceptable percentage of increase in queue size since the last job iteration. AppManager raises an event if the percentage of increase exceeds this value. The default is 50%.
Event severity when increase in queued messages exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in the number of messages in the mailbox delivery queue exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of messages in the mailbox delivery queue?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages in the mailbox delivery queue during the monitoring interval. The default is No.
Monitor Remote Delivery Queue	
Event Notification	
Raise event if number of queued messages exceeds threshold?	Select **Yes** to raise an event if the number of messages in the remote delivery queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of messages in queue	Set the maximum number of messages that can be waiting in the remote delivery queue before an event is raised. The default is 250 messages.
Event severity when number of messages in queue exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of messages in the remote delivery queue exceeds the threshold you set. The default is 15.

Parameter	How to Set It
Raise event if increase in queued messages exceeds threshold?	Select **Yes** to raise an event if the percentage of increase in the number of messages in the remote delivery queue exceeds the threshold. The script measures the rate of increase since the last iteration of the job. The default is No.
Threshold - Maximum percent increase in queued messages since last job iteration	Set the maximum acceptable percentage of increase in queue size since the last job iteration. AppManager raises an event if the percentage of increase exceeds this value. The default is 50%.
Event severity when increase in queued messages exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in the number of messages in the remote delivery queue exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of messages in the remote delivery queue?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages in the remote delivery queue during the monitoring interval. The default is No.
Monitor Poison Message Queue	
Event Notification	
Raise event if number of queued messages exceeds threshold?	Select **Yes** to raise an event if the number of messages in the poison message queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of messages in queue	Set the maximum number of messages that can be waiting in the poison message queue before an event is raised. The default is 0 (zero) messages.
Event severity when number of messages in queue exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of messages in the poison message queue exceeds the threshold you set. The default is 15.
Raise event if increase in queued messages exceeds threshold?	Select **Yes** to raise an event if the percentage of increase in the number of messages in the poison message queue exceeds the threshold. The script measures the rate of increase since the last iteration of the job. The default is No.
Threshold - Maximum percent increase in queued messages since last job iteration	Set the maximum acceptable percentage of increase in queue size since the last job iteration. AppManager raises an event if the percentage of increase exceeds this value. The default is 50%.
Event severity when increase in queued messages exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in the number of messages in the poison message queue exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of messages in the poison message queue?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages in the poison message queue during the monitoring interval. The default is No.
Monitor Unreachable Destination Queue	
Event Notification	
Raise event if number of queued messages exceeds threshold?	Select **Yes** to raise an event if the number of messages in the unreachable destination queue exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum number of messages in queue	Set the maximum number of messages that can be waiting in the unreachable destination queue before an event is raised. The default is 100 messages.
Event severity when number of messages in queue exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of messages in the unreachable destination queue exceeds the threshold you set. The default is 15.
Raise event if increase in queued messages exceeds threshold?	Select **Yes** to raise an event if the percentage of increase in the number of messages in the unreachable destination queue exceeds the threshold. The script measures the rate of increase since the last iteration of the job. The default is No.
Threshold - Maximum percent increase in queued messages since last job iteration	Set the maximum acceptable percentage of increase in queue size since the last job iteration. AppManager raises an event if the percentage of increase exceeds this value. The default is 50%.
Event severity when increase in queued messages exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in the number of messages in the unreachable destination queue exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of messages in the unreachable queue?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages in the unreachable destination queue during the monitoring interval. The default is No.

4.39 UMS_CallActivity

Use this Knowledge Script to monitor call activity on a Unified Messaging server. This script raises an event if a threshold is exceeded and generates data streams for the following types of calls:

- Active voice calls
- Active fax calls
- Active play-on-phone calls
- Active auto-attendant calls
- Active subscriber-access calls
- Active prompt-editing calls

4.39.1 Resource Objects

- Exchange2007_UnifiedMessagingServer
- Exchange2010_UnifiedMessagingServer
- Exchange2013_UnifiedMessagingServer

4.39.2 Default Schedule

By default, this script runs every 15 minutes.

4.39.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UMS_CallActivity job fails. The default is 5.
Monitor Voice Calls	
Event Notification	
Raise event if number of active voice calls exceeds threshold?	Select **Yes** to raise an event if the number of active voice calls exceeds the threshold you set. The default is Yes. Active voice calls are calls that are currently connected to the Unified Messaging server.
Threshold - Maximum number of active voice calls	Set the maximum number of calls that can be simultaneously connected to the Unified Messaging server before an event is raised. The default is 100 calls.
Event severity when number of active voice calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active voice calls exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of active voice calls?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of voice calls that were active during the monitoring period. The default is No.
Monitor Fax Calls	
Event Notification	
Raise event if number of active fax calls exceeds threshold?	Select **Yes** to raise an event if the number of active fax calls exceeds the threshold you set. The default is Yes. Voice calls become fax calls after a fax tone is detected.
Threshold - Maximum number of active fax calls	Set the maximum number of fax calls that can be simultaneously connected to the Unified Messaging server before an event is raised. The default is 100 calls.
Event severity when number of active fax calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active fax calls exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of active fax calls?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of fax calls that were active during the monitoring period. The default is No.
Monitor Play On Phone Calls	
Event Notification	

Parameter	How to Set It
Raise event if number of active play on phone calls exceeds threshold?	Select **Yes** to raise an event if the number of active play-on-phone calls exceeds the threshold you set. The default is Yes. The Exchange Server 2007 Unified Messaging play-on-phone feature enables users to access voice mail messages on the telephone rather than on their computer speakers. Active play-on-phone calls are outbound calls initiated to play back messages.
Threshold - Maximum number of active play on phone calls	Set the maximum number of play-on-phone calls that can be simultaneously active before an event is raised. The default is 100 calls.
Event severity when number of active play on phone calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active play-on-phone calls exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of active play on phone calls?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of play-on-phone calls that were active during the monitoring period. The default is No.
Monitor Auto Attendant Calls	
Event Notification	
Raise event if number of active auto attendant calls exceeds threshold?	Select **Yes** to raise an event if the number of active auto-attendant calls exceeds the threshold you set. The default is Yes. The Unified Messaging auto attendant is a set of voice prompts or .wav files played to callers in place of a human operator when they call into your organization. Active auto-attendant calls are calls that are currently connected to the Unified Messaging server by the auto attendant.
Threshold - Maximum number of active auto attendant calls	Set the maximum number of auto-attendant calls that can be simultaneously active before an event is raised. The default is 100 calls.
Event severity when number of active auto attendant calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active auto-attendant calls exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of active auto attendant calls?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of auto-attendant calls that were active during the monitoring period. The default is No.
Monitor Subscriber Access Calls	
Event Notification	
Raise event if number of active subscriber access calls exceeds threshold?	Select **Yes** to raise an event if the number of active subscriber-access calls exceeds the threshold you set. The default is Yes. Subscriber access is used by users to access their individual mailboxes to retrieve e-mail, voice messages, contacts, and calendaring information. Active subscriber-access calls are logged-on subscribers who are currently connected to the Unified Messaging server.

Parameter	How to Set It
Threshold - Maximum number of active subscriber access calls	Set the maximum number of subscriber-access calls that can be simultaneously active before an event is raised. The default is 100 calls.
Event severity when number of active subscriber access calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active subscriber-access calls exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of active subscriber access calls?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of subscriber-access calls that were active during the monitoring period. The default is No.
Monitor Prompt Editing Calls	
Event Notification	
Raise event if number of active prompt editing calls exceeds threshold?	Select **Yes** to raise an event if the number of active prompt-editing calls exceeds the threshold you set. The default is Yes. Active prompt-editing calls are logged-on users who are editing custom prompts, such as voice-mail greetings.
Threshold - Maximum number of active prompt editing calls	Set the maximum number of prompt-editing calls that can be simultaneously active before an event is raised. The default is 100 calls.
Event severity when number of active prompt editing calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active prompt-editing calls exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of active prompt editing calls?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of prompt-editing calls that were active during the monitoring period. The default is No.

4.40 UMS_Connectivity

Use this Knowledge Script to monitor connectivity to Hub Transport servers, Mailbox servers, Active Directory, and mailboxes enabled for Unified Messaging (UM). This script raises an event if a connectivity test fails or if response time exceeds the threshold you set.

A mailbox that is enabled for UM can receive e-mail, voicemail, and fax messages.

NOTE: On Exchange Server 2013 and 2016, you must drop this script only on the Mailbox server that hosts the Mailbox user that will be used for the test. This script displays an error if you drop this script on any other Mailbox Server that does not host the Mailbox user.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see Section 4.43, “Recommended Knowledge Script Group,” on page 162.

4.40.1 Resource Objects

- Exchange2007_UnifiedMessagingServer
- Exchange2010_UnifiedMessagingServer

- Exchange2013_UnifiedMessagingServer
- Exchange2016_UnifiedMessagingServer

4.40.2 Default Schedule

By default, this script runs every 15 minutes.

4.40.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UMS_Connectivity job fails. The default is 5.
Monitor UM-Enabled Mailbox Accessibility	
Dial plan to use to connect to the UM-enabled mailbox	Identify the dial plan to use to connect to the mailbox you want to monitor.
Phone extension of UM-enabled mailbox to use for accessibility test	Provide the extension number of the mailbox you want to monitor.
PIN of UM-enabled mailbox to use for accessibility test	Provide the Personal Identification Number (PIN) required to access the mailbox you want to monitor.
Event Notification	
Raise event if UM-enabled mailbox cannot be accessed?	Select **Yes** to raise an event if the specified mailbox cannot be tested for connectivity. The default is Yes.
Event severity when UM-enabled mailbox cannot be accessed	Set the severity level, from 1 to 40, to indicate the importance of an event in which the specified mailbox is unavailable for testing. The default is 5.
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the time to connect to the mailbox exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time	Set the maximum number of seconds that AppManager should wait to connect with the mailbox before raising an event. The default is 10000 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which response time exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the length of response time during the monitoring period. The default is No.
Monitor Mailbox Server Connectivity	
Event Notification	

Parameter	How to Set It
Raise event if Mailbox servers are unavailable?	Select **Yes** to raise an event if Mailbox servers cannot be tested for connectivity. The default is Yes.
Event severity when Mailbox servers are unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which Mailbox servers are unavailable for testing. The default is 5.
Monitor Hub Transport Server Connectivity	
Event Notification	
Raise event if Hub Transport servers are unavailable?	Select **Yes** to raise an event if Hub Transport servers cannot be tested for connectivity. The default is Yes.
Event severity when Hub Transport servers are unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which Hub Transport servers are unavailable for testing. The default is 5.
Monitor Mailbox Server Connectivity	
Event Notification	
Raise event if Mailbox servers are unavailable?	Select **Yes** to raise an event if Mailbox servers cannot be tested for connectivity. The default is Yes.
Event severity when Mailbox servers are unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which Mailbox servers are unavailable for testing. The default is 5.
Monitor Active Directory Connectivity	
Event Notification	
Raise event if Active Directory is unavailable?	Select **Yes** to raise an event if Active Directory cannot be tested for connectivity. The default is Yes.
Event severity when Active Directory is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which Active Directory is unavailable for testing. The default is 5.

4.41 UMS_Failures

Use this Knowledge Script to monitor failures of the Unified Messaging server related to redirected calls, disconnected calls, and access to Active Directory, the Hub Transport server, and the Mailbox server. This script raises an event if a threshold is exceeded.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see Section 4.43, “Recommended Knowledge Script Group,” on page 162.

4.41.1 Resource Objects

- Exchange2007_UnifiedMessagingServer
- Exchange2010_UnifiedMessagingServer
- Exchange2013_UnifiedMessagingServer
- Exchange2016_UnifiedMessagingServer

4.41.2 Default Schedule

By default, this script runs every 15 minutes.

4.41.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UMS_Failures job fails. The default is 5.
Monitor Calls Disconnected Due to Internal Errors	
Event Notification	
Raise event if calls disconnected due to internal errors exceed threshold?	Select **Yes** to raise an event if the number of calls disconnected due to internal errors exceeds the threshold you set. The default is Yes. This script uses the value of the `Calls Disconnected on Irrecoverable Internal Error` performance counter, which is the number of calls that were disconnected after an internal system error occurred.
Threshold - Maximum number of calls disconnected due to internal errors	Set the maximum number of calls that can be disconnected due to an internal error before an event is raised. The default is 900 calls.
Event severity when calls disconnected due to internal errors exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of calls disconnected due to internal errors exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for calls disconnected due to internal errors	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls disconnected due to internal errors during the monitoring period. The default is No.
Monitor Calls Disconnected Due to External Errors	
Event Notification	
Raise event if calls disconnected due to external errors exceed threshold?	Select **Yes** to raise an event if the number of calls disconnected due to external errors exceeds the threshold you set. The default is Yes. This script uses the value of the `Calls Disconnected by UM on Irrecoverable External Error` performance counter, which is the total number of calls that have been disconnected after an irrecoverable external error occurred.
Threshold - Maximum number of calls disconnected due to external errors	Set the maximum number of calls that can be disconnected due to an external error before an event is raised. The default is 900 calls.
Event severity when calls disconnected due to external errors exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of calls disconnected due to external errors exceeds the threshold you set. The default is 5.

Parameter	How to Set It
Data Collection	
Collect data for calls disconnected due to external errors?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls disconnected due to external errors during the monitoring period. The default is No.
Monitor Failures to Redirect Calls	
Event Notification	
Raise event if failures to redirect calls exceed threshold?	Select **Yes** to raise an event if the number of failed attempts to redirect calls exceeds the threshold you set. The default is Yes. This script uses the value of the `Failed to Redirect Call` performance counter, which is the number of times the Unified Messaging service did not redirect calls to a Unified Messaging worker process.
Threshold - Maximum number of failures to redirect calls	Set the maximum number of calls that can fail to be redirected before an event is raised. The default is 900 calls.
Event severity when failures to redirect calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of failed attempts to redirect calls exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for failures to redirect calls?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of attempts to redirect calls that failed during the monitoring period. The default is No.
Monitor Mailbox Server Access Failures	
Event Notification	
Raise event if Mailbox server access failures exceed threshold?	Select **Yes** to raise an event if the number of failed attempts to access the Mailbox server exceeds the threshold you set. The default is Yes. This script uses the value of the `Mailbox Server Access Failures` performance counter, which is the number of times the Unified Messaging system did not access a Mailbox server.
Threshold - Maximum number of Mailbox server access failures	Set the maximum number of attempts that can fail to access the Mailbox server before an event is raised. The default is 900 attempts.
Event severity when Mailbox server access failures exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of failed attempts to access the Mailbox server exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for Mailbox server access failures?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of attempts to access the Mailbox server that failed during the monitoring period. The default is No.
Monitor Hub Transport Server Access Failures	
Event Notification	

Parameter	How to Set It
Raise event if Hub Transport server access failures exceed threshold?	Select **Yes** to raise an event if the number of failed attempts to access the Hub Transport server exceeds the threshold you set. The default is Yes. This script uses the value of the `Hub Transport Access Failures` performance counter, which is the number of times that attempts to access a Hub Transport server failed. This number increases only if all Hub Transport servers are unavailable.
Threshold - Maximum number of Hub Transport server access failures	Set the maximum number of attempts that can fail to access the Hub Transport server before an event is raised. The default is 900 attempts.
Event severity when Hub Transport server access failures exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of failed attempts to access the Hub Transport server exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for number of Hub Transport server access failures?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of attempts to access the Hub Transport server that failed during the monitoring period. The default is No.
Monitor Active Directory Access Failures	
Event Notification	
Raise event if Active Directory access failures exceed threshold?	Select **Yes** to raise an event if the number of failed attempts to access Active Directory exceeds the threshold you set. The default is Yes. This script uses the value of the `Directory Access Failures` performance counter, which is the number of times that attempts to access Active Directory failed.
Threshold - Maximum number of Active Directory access failures	Set the maximum number of attempts that can fail to access Active Directory before an event is raised. The default is 900 attempts.
Event severity when Active Directory access failures exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of failed attempts to access Active Directory exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for Active Directory access failures?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of attempts to access Active Directory that failed during the monitoring period. The default is No.

4.42 UMS_Performance

Use this Knowledge Script to monitor the performance of the Unified Messaging server: user response latency, operation response time, queued messages for call answering, queued OCS user notifications, and calls disconnected while playing audio hourglass tones. This script raises an event if a monitored value exceeds the threshold you set. In addition, this script generates data streams for monitored values.

4.42.1 Resource Objects

- Exchange2007_UnifiedMessagingServer

- Exchange2010_UnifiedMessagingServer
- Exchange2013_UnifiedMessagingServer
- Exchange2016_UnifiedMessagingServer

4.42.2 Default Schedule

By default, this script runs every 15 minutes.

4.42.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UMS_Performance job fails. The default is 5.
Monitor User Response Latency	
Event Notification	
Raise event if user response latency exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes for the system to respond to a user's request exceeds the threshold you set. The default is Yes. This script uses the value of the `User Response Latency` performance counter, which is the average response time, in milliseconds, for the system to respond to a user request. This average is calculated over the last 25 calls.
Threshold - Maximum user response latency	Set the maximum length of time it can take to respond to a user request before an event is raised. The default is 1 millisecond.
Event severity when user response latency exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which user response time exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for user response latency?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average user response latency value for the monitoring period. The default is No.
Monitor Operations Response Time	
Event Notification	
Raise event if percentage of operations exceeds threshold?	Select **Yes** to raise an event if Unified Messaging operations it takes a Unified Messaging operation to complete a transaction exceeds the threshold you set. The default is Yes. This script uses the `MSExchangeUMPerformance` category of performance counters.

Parameter	How to Set It
Operations response time	Set a response time, between 2 and 6 seconds. Operations with a response time greater than this value are considered for the *Threshold - Maximum percentage of operations that exceed response time* parameter. The default is 6 seconds. The response time is the number of seconds it takes a Unified Messaging operation to complete, during which a caller is waiting for a response.
Threshold - Maximum percentage of operations that exceed the selected response time	Set the maximum percentage of operations that can exceed the response time you specify in *Operations response time*. This script raises an event if the percentage is greater than the threshold value you specify here. The default is 1%.
Event severity when percentage of operations exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which operation response time exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for percentage of operations that exceeds threshold?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns operation response time for the monitoring period. The default is No.
Monitor Call Answer Queued Messages	
Event Notification	
Raise event if call answer queued messages exceed threshold?	Select **Yes** to raise an event if the number of messages in queue to be answered exceeds the threshold you set. The default is Yes. This script uses the `Call Answer Queued Messages` performance counter, which is the number of messages created and not yet submitted for delivery.
Threshold - Maximum call answer queued messages	Set the maximum number of messages that can be in queue to be answered before an event is raised. The default is 50 messages.
Event severity when call answer queued messages exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of messages in queue to be answered exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for call answer queued messages?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages in queue to be answered for the monitoring period. The default is No.
Monitor Queued OCS User Event Notifications	
Event Notification	
Raise event if queued OCS user event notifications exceed threshold?	If you are using Microsoft Exchange without a service pack applied, select **Yes** to raise an event if the number of Office Communications Server notifications in queue exceeds the threshold you set. The default is Yes. This script uses the `Queued OCS User Event Notifications` performance counter, which is the number of notifications that have been created and not yet submitted for delivery. This performance counter is no longer available with Microsoft Exchange 2010 Service Pack 1.
Threshold - Maximum queued OCS user event notifications	Set the maximum number of notifications that can be in queue before an event is raised. The default is 0 notifications.

Parameter	How to Set It
Event severity when queued OCS user event notifications exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of notifications in queue exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for queued OCS user event notifications?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of notifications in queue for the monitoring period. The default is No.
Monitor Calls Disconnected During Audio Hourglass	
Event Notification	
Raise event if calls disconnected during audio hourglass exceed threshold?	Select **Yes** to raise an event if the number of calls disconnected during the audio hourglass exceeds the threshold you set. The default is Yes. This script uses the `Calls Disconnected by Callers During UM Audio Hourglass` performance counter, which is the number of calls during which the caller disconnected while Unified Messaging was playing the audio hourglass tones. Audio hourglass tones let users know they are still on hold or in queue.
Threshold - Maximum calls disconnected during audio hourglass	Set the maximum number of calls that can be disconnected during the audio hourglass before an event is raised. The default is 0 calls.
Event severity when calls disconnected during audio hourglass exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of disconnected calls exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for calls disconnected during audio hourglass?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls disconnected during audio hourglass for the monitoring period. The default is No.

4.43 Recommended Knowledge Script Group

The following Knowledge Scripts in the AppManager for Exchange2007 module are members of the Exchange2007 recommended Knowledge Script Group (KSG).

- All_BestPracticesAnalyzer
- All_ClockSynchronization
- All_EventLog
- All_ServiceStatus
- CAS_Activity
- CAS_Connectivity
- ETS_ExternalMail
- HTS_Connectivity
- MBS_MailboxAccessibility
- MBS_MailFlow
- Transport_BackPressure

- Transport_QueueStatus
- UMS_Connectivity
- UMS_Failures

You can find the Exchange2007 KSG on the RECOMMENDED tab of the Knowledge Script pane of the Operator Console.

The parameters of all scripts in the KSG are set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab, and then run the Exchange2007 group on an Exchange Server resource.

The Exchange2007 KSG contains Knowledge Scripts for every server role. When you run the KSG on a particular server role, only the scripts in the KSG associated with that role will run. The All_* Knowledge Scripts in the KSG will run on every role.

The Exchange2007 KSG provides a “best practices” usage of AppManager for monitoring Exchange Server in your organization. You can use this KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView. For more information, see “About Policy-Based Monitoring” in the AppManager Help.

A KSG is composed of a subset of a module’s Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the Exchange2007 tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the Exchange2007 tab are not affected.

When deployed as part of a KSG, a script’s default script parameter settings may differ from when the script is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the Exchange2007 KSG and want to restore it to its original form, you can reinstall AppManager for Microsoft Exchange Server and Exchange Online on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\Exchange2007\RECOMMENDED_Exchange2007` directory.

In addition to the Knowledge Scripts in the KSG, NetIQ Corporation recommends using the following scripts for monitoring and managing an Exchange Server environment. The tables below summarize the scripts that are applicable for the unique elements of an Exchange Server 2007, 2010, or 2013 environment. For more information, see the AppManager Help for each script.

For performing benchmarking and trend analyses before deploying AppManager for Microsoft Exchange Server and Exchange Online, run the following scripts from the NT and AD script categories.

Recommended Knowledge Script	Description
NT_CPUByProcess	Monitors CPU usage for each process and the total CPU usage for all processes.
NT_CPULoaded	Monitors total CPU usage and queue length to determine CPU load.
NT_LogicalDiskBusy	Monitors the logical disk activity on one or more disks.
NT_LogicalDiskIO	Monitors logical disk I/O activity, including disk transfers, and reads and writes per second.
NT_MemUtil	Monitors physical memory, virtual memory, and paging files.
NT_NetworkBusy	Monitors the traffic on the network interface cards on a Windows computer.
AD_Authentications	Monitors the number of Active Directory Kerberos and NT LAN Manager (NTLM) authentications per second.

For monitoring the hardware and operating system of the Exchange Server server and components, use the following scripts from the **NT** script category and from the categories appropriate for your hardware, such as **CIM** or **Dell**.

Recommended Knowledge Script	Description
[HardwareModule]_ ArrayPhysicalDiskStatus or ArrayPhysicalDrive	Monitors the status of physical drives in an array set.
[HardwareModule]_FanProbe or FanIndividual	Monitors the status of individual fans.
[HardwareModule]_NICError	Monitors network interface transmission errors.
[HardwareModule]_PowerSupply	Monitors the status of the hardware power supplies.
NT_CPULoaded	Monitors total CPU usage and queue length to determine CPU load.
NT_MemUtil	Monitors physical memory, virtual memory, and paging files.
NT_PhysicalDiskQLen	Monitors the number of disk jobs waiting in the queue.
NT_RunAwayProcesses	Detects runaway processes by sampling CPU usage.
NT_SystemUptime	Tracks the number of hours a computer has been operational since it was last rebooted.
NT_DNSConnectivity	Checks connectivity between a managed computer and its DNS server.

For reporting and analysis purposes, use the following script from the **NT** category.

Recommended Knowledge Script	Description
NT_SystemUptime	Tracks the number of hours a computer has been operational since it was last rebooted.

5 Exchange Online Knowledge Scripts

AppManager for Microsoft Exchange Server and Exchange Online provides Knowledge Scripts for monitoring the Mailbox quota and Service health for Exchange Online domains (tenants).

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**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
MailBoxQuota	Monitors the mailbox quota of the users of the Exchange Online domains.
ServiceHealth	Reports the health status of the Exchange Online service. Monitors the service incidents and maintenance incidents that impact the domains of your Office 365 subscription.

5.1 Specifying Inclusion or Exclusion Filters

Few Exchange Online Knowledge Scripts allows you to apply inclusion or exclusion filters on the services that you want to either monitor or ignore. By default, all the services are monitored. When you apply inclusion or exclusion filter, the Knowledge Script either monitors or ignores the specified services based on your filtering criteria.

For inclusion or exclusion filters, specify the services separated by commas with no spaces.

For example: `Exchange Online,Office Subscription,Office 365 Portal`

Based on your filtering criteria, the specified services are either monitored or excluded from monitoring.

To either monitor or ignore a service of a specific domain, specify the domain name and the service name in the following format:

`<domain name>:<service name>`

For example: `abc.onmicrosoft.com:Exchange Online`

If you specify the above, only the `Exchange Online` service of the `abc.onmicrosoft.com` domain is monitored when you select the **Inclusion** criteria. But if you select the **Exclusion** criteria, then only the `Exchange Online` service of the `abc.onmicrosoft.com` domain is excluded from monitoring. Remaining services are monitored.

Based on your filtering criteria, the format `<domain name>:*` includes or excludes monitoring of all services for the specified domain. For example: `abc.onmicrosoft.com:*` includes or excludes monitoring of all services of the `abc.onmicrosoft.com` domain.

You can also specify a list of domains in the following format to be included or excluded:

`abc.onmicrosoft.com:*,xyz.netiq.com:*`

You can use the regular expressions while specify the inclusion or exclusion filter. For more information, see Using the Regular Expression Filters.

5.2 Using the Regular Expression Filters

A regular expression is a pattern that describes a specific portion of text. Few Exchange Online Knowledge Scripts allows you to use regular expressions to define inclusion or exclusion filters for pattern-matching against the text being evaluated.

The following table lists some commonly used regular expression types and their usage.

For more information about regular expression syntax, see related Web sites such as www.wikipedia.org/wiki/Regular_expression or www.regular-expressions.info.

Regular Expression Type	Description
Alternate Matches	A pipe character, `|`, indicates alternate possibilities. For example: ◆ The expression `a|b|c` indicates a match with `a`, or `b`, or `c`. ◆ The expression `Exchange Online|Office Subscription|Skype for Business` indicates a match with `Exchange Online`, or `Office Subscription`, or `Skype for Business`.
Anchor	Anchors do not match characters. Instead, they match a position before, after, or between characters. They anchor the regular expression match at a certain point. ◆ A `^` matches a position before the first character in a text string. For example, the expression `^a` applied to the text string `abc` returns `a` because `a` is at the beginning of the text string. The expression `^b` applied to the same text string returns no value, because `b` is not at the beginning of the text string. ◆ A `$` matches a position right after the last character in a text string. For example, the expression `c$` applied to the text string `abc` returns `c` because `c` is at the end of the text string. The expression `a$` applied to the same string returns no value, because `a` is not at the end of the text string.
Escape Metacharacter	A backslash character, `\`, preceded with special characters such as `.`, `@`, `|`, `*`, `?`, `+`, `(`, `)`, `{`, `}`, `[`, `]`, `^`, `$` and `\` forces the special characters to be interpreted as normal characters. For example: ◆ A dot (`.`) is usually used as a wildcard metacharacter, but if preceded by a backslash it represents the dot character itself. For information on wildcard metacharacter, see "Wildcard" on page 169. ◆ A colon (`:`) when preceded by a backslash excludes or includes all device names that contains `:` in their names. ◆ An equal sign (=) when preceded by a backslash excludes or includes all device names that contains = in their names.

Regular Expression Type	Description
Literal	A literal expression consists of a single character that matches all the occurrences of that character in the text string. For example, if the expression is `a` and the text string is `The gray cat is purring`, then the match is the `a` in `gray` and `a` in `cat`. All characters except for the following are literals: `.`, `|`, `*`, `?`, `+`, `(`, `)`, `{`, `}`, `[`, `]`, `^`, `$` and `\`. These characters are treated as literals when preceded by a `\`.
Matching Characters or Digits	◆ **`\d`:** Matches a digit. ◆ **`\D`:** Matches a non-digit. ◆ **`\s`:** Matches a whitespace character. ◆ **`\S`:** Matches any character except a whitespace. ◆ **`\w`:** Matches an alphanumeric character. ◆ **`\W`:** Matches an non-alphanumeric character.
Parentheses	Use parentheses, `()`, to group characters and then apply a repetition operator to the group. For example, the expression `(ab)*` returns all of the string `ababab`.
Repeat	A repeat is an expression that is repeated an arbitrary number of times. ◆ A question mark, `?`, indicates that the preceding character in the expression is optional. For example, the expression `ba?` returns `b` or `ba`. ◆ An asterisk, `*`, indicates that the preceding character is to be matched zero or more times. For example, the expression `ba*` returns all instances of `b`, `ba`, `baaa`, and so on. ◆ A plus sign, `+`, indicates that the preceding character is to be matched one or more times. The expression `ba+` returns all instances of `ba` or `baaaa`, for example, but not `b`. ◆ Curly braces, `{}`, indicate a specific amount of repetition. For example, the expression `a{2}` returns the letter a repeated exactly twice. The expression `a{2,4}` returns the letter a repeated between 2 and 4 times. The expression `a{2,}` returns the letter a repeated at least twice, with no upper limit. For example, the expression `ba{2,4}` returns `baa`, `baaa`, and `baaaa`.
Square Brackets	Use square brackets, `[]`, to match any one of the characters that is enclosed in the brackets. You can specify a range of characters by using a hyphen. For example, the expression `[a-i]` that performs the same match as `[abcdefghi]` returns all services that match any one of the characters inside the square brackets such as ‘a’ in “Azure Information Protection”, ‘e’ in “Exchange Online” and ‘i’ in “Identity Service”
Wildcard	The dot wildcard, `.`,matches any single character except line break characters. For example, the expression `gr.y` matches `gray`, `grey`, `gr%y`, and so on.

Regular Expression Type	Description
Word Boundary	◆ **\b:** Matches a zero-width word boundary, such as between a letter and a space. For example: `er\b` matches the `er` in `never` but not the `er` in `verb`. ◆ **\B:** Matches a word non-boundary. For example: `er\B` matches the `er` in `verb` but not the `er` in `never`.

5.3 MailBoxQuota

Use this Knowledge Script to monitor the mailbox quota of the users of the Exchange Online domains.

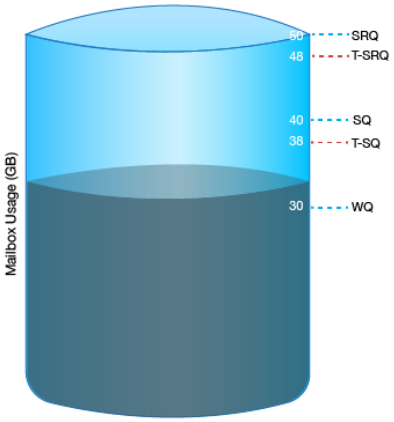
The Knowledge Script monitors the mailbox usage based on the Warning Quota (WQ), the Prohibit Send Quota (SQ) and the Prohibit Send and Receive Quota (SRQ).

This script raises an event in any one of the following conditions:

- Mailbox usage exceeds Warning Quota.
- User is blocked from sending mails when mailbox usage exceeds the Prohibit Send Quota.
- User is blocked from sending and receiving mails when mailbox usage exceeds the Prohibit Send/Receive Quota.

This Knowledge Script lets you specify two threshold values: *Threshold for Prohibit Send Quota (T-SQ)* and *Threshold for Prohibit Send and Receive Quota (T-SRQ)*. The Knowledge Script raises events if your mailbox usage exceeds these thresholds so that you know in advance that your mailbox usage is approaching the limits for sending or receiving mails.

Figure 5-1 *Mailbox usage quotas*



These threshold values are less than the corresponding quotas for which it is specified, that is, T-SQ is less than SQ and T-SRQ is less than SRQ. The threshold values are calculated as follows:

- If WQ is 30 GB and SQ is 40 GB, the threshold (T-SQ) percentage is calculated on the difference between the SQ value and the WQ value. For example, if you set T-SQ to 80%, the T-SQ value will be equal to 38 GB, which is WQ+((SQ-WQ)*80/100). An event is raised if the mailbox usage exceeds 38 GB.

- If WQ is same as SQ, for example, 40 GB, the threshold (T-SQ) percentage is calculated on the SQ value. For example, if you set T-SQ to 80%, the T-SQ value will be equal to 32 GB, which is 80% of SQ. An event is raised if the mailbox usage exceeds 32 GB.
- If SQ is 40 GB and SRQ is 50 GB, the threshold (T-SRQ) percentage is calculated on the difference between the SRQ value and the SQ value. For example, if you set T-SRQ to 80%, the T-SRQ value will be equal to 48 GB, which is SQ+((SRQ-SQ)*80/100). An event is raised if the mailbox usage exceeds 48 GB.
- If WQ is 30 GB, SQ = SRQ = 50 GB and SRQ being high priority than SQ, then only T-SRQ will be considered. In this case, the threshold (T-SRQ) percentage is calculated on the difference between the SRQ value and the WQ value. For example, if you set T-SRQ to 80%, the T-SRQ value will be equal to 46 GB, which is (WQ+(SRQ-WQ)*80/100). An event is raised if the mailbox usage exceeds 46 GB.
- If all the three quotas are same, that is, WQ = SQ = SRQ = 50 GB, with WQ being the lowest priority and SRQ being the highest priority, then only T-SRQ is considered. In this case, the threshold (T-SRQ) percentage is calculated on the SRQ value. For example, if you set T-SRQ to 80%, the T-SRQ value will be equal to 40 GB, which is 80% of SRQ. An event is raised if the mailbox usage exceeds 40 GB.

For more information on Warning, Prohibit Send, and Prohibit Send/.Receive quotas, see Microsoft article.

The Knowledge Script collects data for charts and reports in any one of the following conditions:

- If the mailbox usage exceeds Warning Quota.
- If the mailbox usage exceeds the threshold for Prohibit Send Quota.
- If the user is blocked from sending mails.
- If the mailbox usage exceeds the threshold for Prohibit Send /Receive Quota.
- If the user is blocked from sending and receiving mails.

5.3.1 Resource Objects

ExchangeOnline_MailBox

5.3.2 Default Schedule

By default, this script runs once-daily.

5.3.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notifications	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MailBoxQuota job fails. The default is 5
Mailbox quota monitoring	

Parameter	How to Set It
Comma separated list of Exchange Online domains to exclude from monitoring	Specify the list of Exchange Online domains that you do not want to monitor. Separate the domain names with commas.
Top user mailboxes in terms of mailbox usage	
Raise event to show the top "N" users in terms of mailbox usage?	Select **Yes** to raise an event to view the mailbox users who have the highest usage. The default is unselected.
Number (N) of top user to be displayed	Specify the number of top mailbox users that you want to view. The default is 10.
Warning quota	
Event Notification	
Raise event if mailbox usage exceeds Warning quota?	Select **Yes** to raise an event if the mailbox usage exceeds the warning quota. The default is Yes.
Event severity when mailbox usage exceeds Warning quota	Set the severity level, from 1 to 40, to indicate the importance of an event in which the mailbox usage exceeds the warning quota. The default is 15.
Data Collection	
Collect data if mailbox usage exceeding Warning quota?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of mailbox users that have exceeded the warning quota. The default is No. **IMPORTANT:** Data is collected only when a mailbox usage exceeds the Warning quota.
Prohibit Send quota	
Event Notification	
Raise event if mailbox usage exceeds threshold for Prohibit Send quota?	Select **Yes** to raise an event if the mailbox usage exceeds the threshold that you have set for Prohibit Send quota. The default is Yes.
Set threshold for Prohibit Send quota	Set the threshold percentage for Prohibit Send quota for mailbox usage. An event is raised if the mailbox usage exceeds the threshold value. The default is 80%.
Event severity when mailbox usage exceeds threshold for Prohibit Send quota	Set the severity level, from 1 to 40, to indicate the importance of an event in which the mailbox usage exceeds the threshold for Prohibit Send quota. The default is 5.
Raise event if user is blocked from sending mails?	Select **Yes** to raise an event if the user is blocked from sending mails. Mails cannot be send from the mailbox when the mailbox usage exceeds the Prohibit Send quota. The default is Yes.
Event severity when user is blocked from sending mails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the user is blocked from sending mails. The default is 5.
Data Collection	

Parameter	How to Set It
Collect data if mailbox usage exceeding threshold for Prohibit Send quota?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of mailbox users that have exceeded the threshold for Prohibit Send quota. The default is No. **IMPORTANT:** Data is collected only when a mailbox usage exceeds the threshold for Prohibit Send quota.
Collect data if user is blocked from sending mails?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of mailbox users that are blocked from sending mails. The default is No. **IMPORTANT:** Data is collected only when mailbox users are blocked from sending mails.
Prohibit Send/Receive quota	
Event Notification	
Raise event if mailbox usage exceeds threshold for Prohibit Send/Receive quota	Select **Yes** to raise an event if the mailbox usage exceeds the threshold that you have set for Prohibit Send/Receive quota. The default is Yes.
Set threshold for Prohibit Send/ Receive quota	Set the threshold percentage for Prohibit Send/Receive quota for mailbox usage. An event is raised if the mailbox usage exceeds the threshold value. The default is 80%.
Event severity when mailbox usage exceeds threshold for Prohibit Send/Receive quota	Set the severity level, from 1 to 40, to indicate the importance of an event in which the mailbox usage exceeds the threshold for Prohibit Send/ Receive quota. The default is 5.
Raise event if user is blocked from sending and receiving mails	Select **Yes** to raise an event if the user is blocked from sending and receiving mails. Mails are not received in the mailbox if the mailbox usage exceeds the Prohibit Send/Receive quota. The default is Yes.
Event severity when user is blocked from sending and receiving mails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the user is blocked from sending and receiving mails. The default is 5.
Data Collection	
Collect data if mailbox usage exceeds the threshold for Prohibit Send/Receive quota?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of mailbox users that have exceeded the threshold for Prohibit Send/Receive quota. The default is No. **IMPORTANT:** Data is collected only when a mailbox usage exceeds the threshold for Prohibit Send and Receive quota.
Collect data if user is blocked from sending and receiving mails?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of mailbox users that are blocked from sending and receiving mails. The default is No. **IMPORTANT:** Data is collected only when mailbox users are blocked from sending and receiving mails.

5.4 ServiceHealth

Use this Knowledge Script to report the health status of the Exchange Online service and all other Office 365 services (workloads) that you have subscribed. The Knowledge Script monitors the services and raises events if the services are either healthy or unhealthy. A service is healthy if there are no active maintenance events or service incidents on the service.

This Knowledge Script raises events that display the service incidents and maintenance incidents that impact the domain of your Office 365 subscription.

5.4.1 Resource Object

- ExchangeOnline_Service

5.4.2 Default Schedule

By default, this script runs every one hour.

5.4.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ServiceHealth job fails. The default is 5.
Raise event if the service is healthy?	Select **Yes** to raise an event if the state of the service is healthy. The default is Yes.
Event severity when the service is healthy	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of Exchange Online service is healthy. The default is 25.
Raise event if the service is not healthy?	Select Yes to raise an event if the state of the service is not healthy. The default is Yes.
Event severity when the service is not healthy	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of Exchange Online service is unhealthy. The default is 5.
Include the latest updates of the service incidents	Select **Yes** to include the latest message of each service incident or maintenance event that are active on the service. The default is Yes.
Collect data for service health?	Select **Yes** to collect data for charts and data. When enabled, data collection returns the status of service health. The default is Yes. The chart displays the service health status as follows: ◆ 0: Service is unhealthy ◆ 100: Service is healthy
Inclusion or Exclusion filter	

Parameter	How to Set It
Inclusion or exclusion criteria	Select one of the filtering criteria: ◆ **Inclusion**: If you want the Knowledge Script to monitor the services that are specified in the *Comma separated list of services* parameter only. ◆ **Exclusion**: If you do not want the Knowledge Script to monitor the services that specified in the *Comma separated list of services* parameter only.
Comma separated list of services	Specify the list of services that you want the Knowledge Script to monitor or exclude from monitoring depending on the Inclusion or exclusion criteria. For more information, see Specifying Inclusion or Exclusion Filters.

6 Troubleshooting AppManager for Microsoft Exchange Server and Exchange Online

This chapter describes how to troubleshoot AppManager for Microsoft Exchange Server and Exchange Online.

6.1 ExchangeOnline_MailboxQuota job throws an error after running for a longer duration

When you run the ExchangeOnline_MailboxQuota Knowledge Script, the Knowledge Script takes a long time to run and then throws the following error:

```
System.ServiceModel.CommunicationException: The server did not provide a meaningful reply; this might be caused by a contract mismatch, a premature session shutdown or an internal server error.
```

This error is observed in an environment in which there are large number of mailboxes but it might also happen in other scenarios when the Knowledge Script runs longer than the time limit specified in the `MCPSHostServer.exe.config` file.

To resolve this error, follow the steps:

1. On the agent machine, go to the `C:\Program Files (x86)\NetIQ\AppManager\bin\PowerShell` path.
2. Locate the `MCPSHostServer.exe.config` file (on 64-bit agent) or the `MCPSHostServer32.exe.config` file (on 32-bit agent).
3. Open the file in a notepad.
4. Increase the value of the `receiveTimeout` argument based on the execution time required by the Knowledge Script in your environment. The default value is 01:00:00, that is, one hour.
5. Save and close the file.

6.2 MCPSHostServer.exe consuming too much CPU

If you observe that the `MCPSHostServer.exe` process is consuming too much CPU, then follow the steps to restrict the CPU usage for the process:

1. On the agent machine, go to the `C:\Program Files (x86)\NetIQ\AppManager\bin\PowerShell` path.
2. Locate the `MCPSHostServer.exe.config` file (on 64-bit agent) or the `MCPSHostServer32.exe.config` file (on 32-bit agent).
3. Open the file in a notepad.

4 Specify the value of the `maxProcessorUtilization` key from 0 to n, where n is the maximum number of logical CPUs in the agent machine. This value denotes the number of logical CPUs that you want to assign to the `MCPSHostServer.exe` process. The default value is 0, which means that all the logical CPUs (100%) in the agent machine can be utilized for the `MCPSHostServer.exe` process.

   For example, if the agent machine has eight logical CPUs and you want to assign only two logical CPUs (25%) for the `MCPSHostServer.exe` process, then specify `value="2"` for the `maxProcessorUtilization` key. Similarly, if you want to assign four logical CPUs (50%), then specify `value="4"` or if you want to assign six logical CPUs (75%), then specify `value="6"`. The highest value that can be assigned for the `maxProcessorUtilization` key is 8, which is the maximum number of logical CPUs in this agent machine.

5 Save and close the file.