Quest® Unified Communications Diagnostics 8.6.3

User Guide

Contents

Introducing Unified Communications Diagnostics

- About Unified Communications Diagnostics
- Getting Started Using the Management Console
- Introducing Management Console health tests
- Health tests available from the Exchange organization node
- Health tests available from the Lync/Skype for Business Environment
- Resolving Problems with Native Tools
- Launching the Diagnostic Console from the Management Console
- Launching UC Analytics from the Management Console
- Reporting Using Web Reports

About Unified Communications Diagnostics

Unified Communications Diagnostics helps administrators detect problems in their messaging environment, accurately locate the root cause, and resolve the problems from a single, easy-to-use interface. It provides a robust and informed troubleshooting solution for Exchange, BlackBerry, Office Communications Server (OCS), Lync, Skype for Business, and Office 365.

UC Diagnostics monitors the following environments:

Table 1. Supported environments.

Environment	Description
Exchange	Helps diagnose and resolve problems for your entire Microsoft Exchange server organization.
BlackBerry	Provides real-time representation of messaging system processes and components within your BlackBerry server and a messaging and collaboration server such as Exchange.
OCS/Lync/Skype for Business	Shows any issues with instant messaging (IM), presence, conferencing, and Voice-Over-IP (VoIP) in your integrated unified communications solution.
Office 365	Provides health tests to show Office 365 subscription status, to monitor connectivity for Exchange Online and Skype for Business Online, and to monitor message delivery for Exchange Online.

UC Diagnostics contain the following components and features:

Table 2. UC Diagnostics Components.

Component	Description
Management Console	The Management Console is an Microsoft Management Console (MMC) snap-in that gives the overall picture of your servers. It helps you visualize and monitor the health of all your servers. It contains the following features: • Automatic discovery process — initially discovers and displays all your servers in the Management Console. Discovery runs automatically once a day to detect changes to your environment. • Monitoring and detection — allows you to monitor the health of your environment and detect any problems before they happen • Detailed web reports — provide historical reporting and trending and analysis over time **NOTE:** For more information on the Management Console, see About the Management Console on page 11.
Diagnostic Console	The Diagnostic Console allows you to view one server at a time. It contains the following features: • Real-time diagnostics — provides visual representation of process flows within a server so you can observe actual server activity in real time • Auto calibration — determines the normal range of values for your server and sets the visual indicators accordingly • Rapid resolutions — displays the details of problem areas including user connections, clients, and server resources for rapid problem resolutions • Effective warnings — provides visual warnings to alert you when performance metrics exceed acceptable thresholds • Detailed drilldown tables and graphs — provide detailed information allowing you to identify the source of each problem
Web Reports	Web Reports allow you to view trending and historical data using preconfigured and custom reports, graphs, and tables. **NOTE:** For more information on Web Reports, see Reporting Using Web Reports on page 182.

Home Page

UC Diagnostics provides a Home Page to help you become familiar with the following functional features from which you can choose:

- Connecting to a server. For more information, see Connecting to a Platform on page 13.

- Configuring Global Settings (Notification Settings, Alternate Credential Settings, and Default Test Settings). For more information, see Specifying the test configuration on page 28.

- Creating Health Tests. For more information on health tests, see Introducing Management Console health tests on page 25.

Getting Started Using the Management Console

- About the Management Console
- Connecting to a Platform
- Connecting to Diagnostic Services
- Importing and Exporting Topology Layout
- Viewing an OCS Environment
- Viewing Link Types
- Viewing a Lync/Skype Environment
- Managing Custom Groups
- Grouping Servers by Type
- Managing Global Filters
- Putting Servers in Maintenance Mode
- Managing Missing Objects
- Viewing Database Availability Groups (DAG)

About the Management Console

The Management Console is a Microsoft Management Console (MMC) snap-in and hosts the administrative tools that you use to administer your networks, computers, services and other system components.

Your BlackBerry servers are located under the Exchange organizations in the treeview.

To open the Management Console

- Click **Start | Program Files | Quest | UC Diagnostics | UC Diagnostics Management Console**

The Management Console consists of the following components:

Table 1. Management Console components.

Management Console Section	Description
Menu	Contains the standard menu items, plus others: • File — allows you to set console options • Action — allows you to connect to an organization or environment, group sites, set global filters, create a health test, force discovery, and import/export topologies • View — allows you to show and hide items in the Management Console • Windows — allows you to set the view of the current window and indicates what windows are open • Help — allows you to open help topics and view the version number of MMC and UC Diagnostics
Treeview	Allows you to: • configure Global Settings • view Web Reports • view organizations, groups, and servers. Groups are displayed as a collection of servers, and servers are displayed as icons within the collections in the topology
Results pane	Allows you to: • view the topology in a graphical format • drag and drop servers for better organization • view the status and details about discovery • view test results
Actions pane	Allows you see all the actions on the currently selected object
Properties Pane	• Shows details of your selected server, such as: Site name Exchange, BlackBerry, OCS, Lync, or Skype for Business version Operating System Version Operating System Service Pack • Shows details of your selected link, such as: Link name Relation of the link from one server to another • Gives instructions on how to zoom, pan, and auto-arrange your topology layout

Connecting to Diagnostic Services

To use the Management Console, you must be connected to the Diagnostic Services. The Management Console automatically connects to the Diagnostic Services on the local host, if a Diagnostic Services server is available. If Diagnostic Services are not available, you are prompted to enter the name of the Diagnostic Services server.

Once you connect to a Diagnostic Services server, the connection is saved to an .msc file. Once you have connected to the Diagnostic Services for the first time, it is not necessary to do so again unless you wish to connect to Diagnostic Services located on a different server.

To connect to the Diagnostic Services

1   Right-click the **UC Diagnostics** node and select **Select Different Diagnostic Services Server**.

2   Enter the name of the Diagnostic Services Server.

3   Click **OK**.

> The account used to run the Management Console must be a member of the Local Administrators group on the server where the Diagnostic Services are running, and must have sufficient rights to access the Spotlight Management Framework database. For more information, see the *Unified Communications Diagnostics Deployment Guide.*

How Management Consoles Share Information

Multiple consoles can be connected to the same Diagnostic Services simultaneously, and have full read/write access to all UC Diagnostics functionality. Changes made in one console appear in the other consoles. If different users edit the same test at the same time, the user who saves the changes last has these settings preserved.

Information such as discovery, tests, credentials, test settings, custom groups, and global settings are shared amongst the Management Consoles. Global filters, Topology layout, and Group By settings are not shared amongst the Management Consoles.

Different Management Consoles can be connected to different organizations. For example, one Management Console can be connected to an Exchange organization, while another is connected to an OCS environment.

When you connect to an Exchange organization, the Management Console discovers and displays your entire Exchange organization. Discovery is initially configured to run automatically once a day to detect changes to your environment.

For information about the permissions run diagnostic services on the BlackBerry, Exchange, OCS, Lync, or Skype for Business platforms, see the *Unified Communications Diagnostics Deployment Guide.*

For information about permissions required to access the SQL data and for information about cluster support, see the *Unified Communications Diagnostics Deployment Guide.*

Connecting to a Platform

The Management Console displays all your servers at a glance, whether they exist in a single location or span the globe. It is the framework where the layout of your servers are displayed, tests are performed, notifications are configured, and server data is displayed.

You can use the Management Console to connect to an Exchange, BlackBerry, OCS, Lync, Skype for Business, or Office 365 platform.

The first time you connect to a platform, all servers are discovered. Discovery locates your available servers, then gets the properties of those servers. Discovery can take some time depending on the size of your organization or environment. Discovery then occurs every 24 hours to check for changes you may have made.

If you select Repeat Discovery, discovery runs at the start time initially indicated, then runs at the new setting configured in the Every...hours box. This overrides the daily start time.

For more information on discovery, see the *Unified Communications Diagnostics Deployment Guide*.

To connect to an Exchange organization

1   Right-click the **UC Diagnostics** node and select **Connect to an Exchange Organization**.

2   Enter a global catalog (or domain name or Exchange server name).

   For an Exchange Online hybrid deployment

     a   If you have a hybrid Exchange and Exchange Online deployment, select the **Exchange Online** check box.

     b   Enter a valid Office 365 user name for the tenant.

User name must be in email format (UserName@Domain.com). It can contain alphanumeric characters and only the following symbols -.,_ @.

    c   Enter the password for the Office 365 credential.

3   If you are connecting to one of the Microsoft National clouds, you must enter the URL that is to be used for the remote PowerShell connection and the URL for the Azure AD Authorization Endpoint.

For example, to connect to Office 365 operated by 21Vianet in China, you could enter:

Remote PowerShell URL:

https://partner.outlook.cn/PowerShell-LiveID

Azure AD Authorization Endpoint URL:

https://login.chinacloudapi.cn/common

If you are connecting to Office 365 Global, the default connections can be used and the fields can be left empty.

4   Click **OK**.

If you are connecting to an Exchange cluster, you must use a virtual server name.

To connect to a native Office 365 environment

1   Right-click the **UC Diagnostics** node and select **Connect to Office 365**.

2   For Connection, enter a name to identify the Office 365 tenant to which you are connecting.

3   Enter a valid Office 365 user name for the tenant.

User name must be in email format (UserName@Domain.com). It can contain alphanumeric characters and only the following symbols -.,_ @.

4   Enter the password for the Office 365 credential.

5   If you are connecting to one of the Microsoft National clouds, you must enter the URL that is to be used for the remote PowerShell connection and the URL for the Azure AD Authorization Endpoint.

For example, to connect to Office 365 operated by 21Vianet in China, you could enter:

Remote PowerShell URL:

https://partner.outlook.cn/PowerShell-LiveID

Azure AD Authorization Endpoint URL:

https://login.chinacloudapi.cn/common

If you are connecting to Office 365 Global, the default connections can be used and the fields can be left empty.

6   Click **OK**.

For native Office 365, nodes for Exchange Online and Skype for Business Online are displayed if the licensing plan has these services enabled.

For hybrid environments, you can add the Exchange Online or Skype for Business Online credentials through the Exchange Connection properties or the Lync/Skype for Business Connection properties.

To connect to an OCS environment

1   Right-click the **UC Diagnostics** node and select **Connect to an OCS Environment**.

2   Enter a global catalog (or domain name or OCS 2007 or OCS 2007 R2 server name) and click **Connect**.

To monitor a mixed environment (Lync/Skype for Business and OCS), you must establish two connections to the same environment: one Lync/Skype connection and one OCS connection.

To connect to a Lync/Skype for Business environment

1   Right-click the **UC Diagnostics** node and select **Connect to a Lync/Skype Environment**.

2   Enter a Lync/Skype Pool FQDN and user credentials.

For a Skype for Business Online hybrid deployment

   a   If you have a hybrid Lync/Skype for Business and Skype for Business Online deployment, select the **Skype for Business Online** check box.

   b   Enter a valid Office 365 user name for the tenant.

   User name must be in email format (UserName@Domain.com). It can contain alphanumeric characters and only the following symbols -.,_ @.

   c   Enter the password for the Office 365 credential.

3   If you are connecting to one of the Microsoft National clouds, you must enter the URL that is to be used for the remote PowerShell connection and the URL for the Azure AD Authorization Endpoint.

   For example, to connect to Office 365 operated by 21Vianet in China, you could enter:

   Remote PowerShell URL:

   https://partner.outlook.cn/PowerShell-LiveID

   Azure AD Authorization Endpoint URL:

   https://login.chinacloudapi.cn/common

   If you are connecting to Office 365 Global, the default connections can be used and the fields can be left empty.

4   Click **OK**.

   You can select a Lync/Skype Environment from the drop-down list of those to which you have previously connected.

The next time you run the Management Console and connect to the same environment, the environment is not rediscovered upon connecting. If changes are made to the environment and are not shown in the Management Console, right-click the connection node in the treeview and select **Force Discovery**.

To connect to a BlackBerry environment

You must be connected to an Exchange organization before you can connect to a BlackBerry domain.

1   Right-click the Exchange organization node and select **Connect to BlackBerry Servers**.

   - OR -

   If you are already connected to a BlackBerry domain, select **Edit BlackBerry Servers Connection Properties.**

2   In the Connect to BlackBerry Servers dialog box, click **Add**.

3   Enter the BlackBerry Database location and the BlackBerry Database name.

   ▪   If you are using a BlackBerry database that is installed on a named SQL instance, you must specify the instance name, such as MyServer/MySQLInstance.

   ▪   If the SQL instance hosting the BlackBerry database is configured to use a non-default port, you can specify the port number in the Database Location box separated by comma, such as: MyServer/MySqlInstance,1345 where 1345 is the port number.

   ▪   You do not need to specify a port number if your alias is configured for the SQL named instance hosting BlackBerry database on the SQL server, or if the SQL Server Browser service is installed and running on SQL server.

4   Windows authentication is selected by default. If you prefer to use SQL authentication, select this option from the drop down menu and enter a valid user name and password.

5   Click **OK**.

   To add multiple BlackBerry domains, repeat steps 2 through 5.

To modify a BlackBerry Server connection

Because BlackBerry server and Exchange organization discovery takes place at the same time, if you want to change BlackBerry connection properties, you must change them at the Exchange organization level.

1   Right-click the Exchange organization.

2   Select **Edit BlackBerry Servers Connection Properties**.

3   Make the required changes.

To add a generic server

In addition to servers that are automatically discovered, you may want to monitor other servers that are critical to the functioning of your environment, such as a domain controller server. To do this, you can manually add them to your organization/environment.

1   From the treeview in the Management Console, right-click an Exchange or BlackBerry organization or an OCS/Lync/Skype for Business environment, and select **Add Generic Server**.

2   Enter a server name and click **OK**.

    These servers have the same functionality as other servers, such as the ability to create health tests, launch Computer Management, Services, and Event Viewer.

To delete generic servers

•   Right-click a generic server and click **Delete**.

To customize connection properties

You can customize your connection properties to allow discovery to occur at times other than every 24 hours.

•   Right-click the connection in the treeview and select **Properties**.

Use the View Connection Properties dialog box to change or customize parameters as necessary.

To disconnect from an organization/environment

1   From the treeview, right-click an organization or environment.

2   Select **Disconnect from Organization** if you are connected to an Exchange organization)

    - OR -

    Select **Disconnect from Environment** if you are connected to an OCS/Lync/Skype for Business environment.

    Disconnecting from your organization/environment removes the organization/environment from the treeview only. No data is deleted. Scheduled tests are still executed, data is still collected, and discovery still runs.

To remove the organization/environment

1   From the treeview, right-click an organization or environment.

2   Select **Remove Organization** if you are connected to an Exchange organization

    - OR -

    Select **Remove Environment** if you are connected to an OCS/Lync/Skype for Business environment.

    Removing your organization/environment stops UC Diagnostics from collecting any information about that organization/environment. All data, such as test results history, web report data, and test settings, related to the organization or environment is permanently deleted.

To remove a BlackBerry domain

1   From the treeview, right-click the Exchange organization node and select **Edit BlackBerry Servers Connection Properties**.

2   In the Connect to BlackBerry Servers dialog box, select a BlackBerry database.

3   Click **Remove**.

Importing and Exporting Topology Layout

You can export your current topology layout to be imported to another topology. In general, one topology layout is saved per grouping node in the .msc file. The Importing and exporting function allows you to have several possible topology layouts.

You cannot save different topology layouts over different grouping modes. For example, if you export a topology layout that was grouped by site, you cannot import that layout if your current topology layout is grouped by domain.

To export a topology layout

1   Right-click an organization in the treeview or right-click your topology layout.

2   Select **Export Topology Layout**.

3   Enter the name for the file and save it as a .topology file.

To import a topology layout

1   Right-click a server node in the treeview or right-click your topology layout.

2   Select **Import Topology Layout**.

3   Select the topology file you want to import.

Viewing an OCS Environment

Once you are connected to an OCS environment, you can perform the following actions:

- Discovering Federated Partners in OCS
- Viewing Pool Properties in OCS
- Viewing OCS Server Properties
- Viewing Link Types

Discovering Federated Partners in OCS

Federation provides your environment with the ability to communicate with other environments to share IM and presence. You can also federate with an audio conference provider.

You can allow automatic discovery of federated partners or manually configure federation by using Computer Management native tool (select **Computer Management | Services and Applications | Microsoft Office Communications Server 2007**).

For more information, see http://technet.microsoft.com/en-us/library/bb663635.aspx.

Viewing Pool Properties in OCS

Right-click a pool in your Topology tab in your OCS environment to find the following list of properties:

Table 2. Viewing OCS pool properties.

Pool property	Description
Settings	Lists the connection pool settings.
Endpoints	Lists the number of clients connected to each Front-End in the pool.
Conferences	Lists all types of participants in a conference such as those that organize or control a conference (Unique Organizers, Enterprise participants, and external participants). It also tells you the conferences that are queued (Allocated Conferences) and those that are currently in session (Active Conferences).
Client Filter	Displays the status and configuration settings for the Client Filters.
IM Filter	Displays configuration and settings information related to the Instant Message Filter.

Viewing OCS Server Properties

Right-click a server in your pool in your OCS environment to find the following list of properties:

Table 3. Viewing OCS server properties in a pool.

Server property	Description
General	Lists the DNS name, IP address, and installed roles of the server.
System	Lists information related to the computer's environment, such as Operating System, Memory Usage and Processors.
Ports	List the ports being used by the OCS 2007 or OCS 2007 R2 roles installed on the computer.

You can also right-click a server that is not part of a pool to find the following list of properties:

Table 4. Viewing OCS server properties not in a pool

Server property	Description
General	Lists the DNS name, IP address, and installed roles of the server.
System	Lists information related to the computer's environment, such as Operating System, Memory Usage, and Processors.
Ports	List the ports being used by the OCS 2007 or OCS 2007 R2 roles installed on the computer.
Archiving	List the Archiving database server, Archiving database name, threads available, MSMQ queue name, and message retention period configured for the Archiving server. * Available on Archiving servers only.
CWA	Specifies the authentication type and modes, timeout periods for public and private connections, and ports used by the Communicator Web Access server. The name in brackets represents the site name configured when you install CWA. * Available on CWA servers only.
Mediation	Lists the encryption level, Media Gateway and proxy settings, and the ports used by the Mediation server. * Available on Mediation servers only.
QoE Monitor	Lists the listening addresses and ports, data retention period, database instance name, report URL, MSMQ queues, and file system log settings for the Quality of Experience (QoE) monitoring server. * Available on QoE monitoring servers only.
Access Edge	Lists the external listening address and ports used by the Access Edge server. * Available on Access Edge servers only.
A/V Edge	Lists the external IP address and the external and internal ports used by the Audio/Video and MRAS servers. * Available on A/V Edge servers only.
MRAS	Lists the timeout periods if your session is either left idle or running, and, if applicable, any alternate TURN servers. * Available on A/V Edge servers only.
Web Conferencing Edge	Lists the external listening address and ports used by the Web Conferencing edge server. * Available on Web Conferencing servers only.

Viewing Link Types

Links show the flow of information from one server to another.

There are two types of links in your organization:

Table 5. Viewing links between servers.

Links	Description
Routing Group Connectors	Shows the connectors that evaluate the optimal path for emails from one server to another. The links can be bidirectional or unidirectional. The properties of a Routing Group connector (which are shown in the Properties Pane when a Routing Group connector link is selected) include Cost and Bridgeheads.

Table 5. Viewing links between servers.

Links	Description
Site Connectors	Shows the connectors that evaluate the optimal path of network traffic. Sites are shown when you group by sites in all platforms.
	The properties of a Site connector (which are shown in the Properties Pane when a Site connector link is selected) include Cost and Group Membership (which lists sites that are associated with the connector).

Viewing a Lync/Skype Environment

Once you are connected to a Lync/Skype for Business environment, you can perform the following:

- Viewing Lync/Skype Pool Properties
- Viewing Lync/Skype Server Properties

Viewing Lync/Skype Pool Properties

Click a pool name in the Topology tab in your Lync or Skype for Business environment to see the following pool properties in the lower panel:

Table 6. Viewing pool properties.

Pool Property	Description
Lync/Skype Pool FQDN	Fully qualified domain name of the pool
Lync/Skype Site	Name of the site in which the pool is located
Lync/Skype Services	List of all services defined for the pool

Viewing Lync/Skype Server Properties

Click a server within a pool in the Topology tab in your Lync or Skype for Business environment to see the following server properties in the lower panel:

Table 7. Viewing server properties.

Server Property	Description
Server name	Name of the server
Domain	Domain to which the server belongs
Site	Name of the associated Active Directory site
Operating System Version	Version of the operating system that is installed on the server
Operating System Version Service Pack	Shows the latest service pack that is installed on the server
Lync/Skype Site	Name of the site in which the pool is located
Lync/Skype Version	Version of Lync or Skype that is installed

Managing Custom Groups

Custom groups allow you to create arbitrary groups of servers to simplify test management. For example, you can a create a group of servers once and use that custom group as the target for multiple tests. If you change the custom group, the tests automatically target the new group of selected servers.

Custom groups appear under the Custom Groups node in the treeview. Since custom groups are used as test targets, they are shared between all users of the console. Custom groups do not appear in the topology view.

There are two types of custom groups which you can create.

Table 8. Types of custom groups.

Custom Group Type	Description
Static	A user-selected group of arbitrary servers
Dynamic	A group of servers that meet a set of criteria defined by a user based on properties of the servers

Use the following sections to perform the following group functions:

- Creating a Static Custom Group
- Creating a Dynamic Custom Group
- Editing a Custom Group
- Deleting a Custom Group
- Grouping Servers by Type

Creating a Static Custom Group

To create a static custom group

1. Right-click a server and select **New Static Custom Group**.

   - OR -

   Right-click the **Custom Groups** node in the treeview and select **Create Static Custom Group**.

2. In the New Custom Group dialog box, select the servers you want included in the group.

3. Enter a name for the custom group and click **OK**.

Creating a Dynamic Custom Group

To create a dynamic custom group

1. Right-click the **Custom Groups** node in the treeview and select **Create Dynamic Custom Group**.

2. In the New Custom Group dialog box, enter a name for the custom group.

3. Select the type of server for which you want to search.

4. Click **Add** to insert criteria for the selected servers.

5. Click **OK**.

Property criteria are cumulative — only servers that match all of the selected criteria are part of the custom group.

Editing a Custom Group

To edit a custom group

- Right-click your custom group node under the **Custom Groups** node in the treeview and select **Edit Custom Group**.

Deleting a Custom Group

To delete a custom group

- Right-click your custom group node under the **Custom Groups** node in the treeview and select **Delete**.

Grouping Servers by Type

You can group OCS. Lync, Skype for Business, or Exchange servers by type.

Table 9. Grouping servers by type.

Server Type	Group by
OCS	- Pool - Site - Domain The default grouping is Pool.
Lync/Skype for Business	- Pool - Site - Domain The default grouping for is Pool.
Exchange	- Site - Administrative Group - Routing Group - Domain - None The default grouping is Site.

To group servers by type

1. Right-click the connection in the treeview and select **Group By**.
2. Select the grouping that you want for the servers.

   The servers appear in the treeview according to the grouping that you have selected.

Managing Global Filters

A global filter allows you to hide servers in which you are not interested. The filter hides the servers from both the treeview and topology view.

To enable or customize global filter

1. Right-click your root connection node and select **Set Global Filter**.

2   In the Global Filter dialog box, select the servers you want to remain visible and click **OK**.

- ▪ To select all servers, right-click the top node and click **Select All**.

- ▪ To clear your selection, right-click the top node and click **Clear All**.

To remove global filters

- • Right-click your root connection node and select **Remove Global Filter**.

Global filters do not affect tests that are scheduled to run against the hidden servers. Global filters are stored in the MMC configuration file (.msc), so different .msc files can store different global filters. The MMC description bar indicates when global filters are enabled to remind you that some servers are hidden.

Global filters can be customized per console. For example, if two different users have their own console and are sharing the same Diagnostic Services, they can each set different global filters.

Putting Servers in Maintenance Mode

Maintenance mode, which affects all users, allows you to mark servers as offline so that you can perform maintenance on those servers. When any test runs, the Management Console skips any servers that are in maintenance mode.

To put a server into maintenance mode

1   Select target servers.

2   Right-click and select **Start Maintenance Mode**.

To remove a server from maintenance mode

1   Select target servers.

2   Right-click and select **Stop Maintenance Mode**.

While a server is in maintenance mode, the icon for the server is darkened to indicate the state of the server.

Managing Missing Objects

If you decommission a server, the server remains in the topology and treeview, but is inactive. You cannot perform any actions on that server. The server is preserved to keep any historical data for Web Reports. If you recommission the server, the server becomes active again.

If the server is no longer required, you can delete it.

To delete a server

- • Right-click the server and select **Delete**.

Viewing Database Availability Groups (DAG)

If you have DAGs configured in your Exchange organization, the DAGs dialog box displays the following information for each DAG:

- • member servers

- mailbox databases that are configured to replicate within the DAG

- database copies for each mailbox database

You can view DAGs for organizations running Exchange 2010 and later.

Prerequisites

To view DAGs, you must meet the following requirements:

- Be part of the domain.

- Have Windows PowerShell 2.0 or later installed on the Management Console computer.

- Have sufficient rights to connect to the remote Exchange computer and execute PowerShell cmdlets:

  - Be a member of the Local Administrators group

  - Be a member of the View-Only Organization Management group

To view DAGs

1   From the treeview, right-click the Exchange 2010, 2013, or 2016 organization node.

2   Select **Database Availability Groups**.

The data that is shown is for informational purposes. You cannot edit the information in the dialog box. To refresh the information, press F5 or close then reopen the dialog box.

In some situations, UC Diagnostics can fail to retrieve some of the information. If this happens, the missing value

- is displayed as N/A

- is marked with the grey icon

- shows the reason for the failure in the Details column

For more information on DAG, see http://technet.microsoft.com/en-us/library/dd298065(EXCHG.140).aspx.

3

Introducing Management Console health tests

Introducing health tests

You can use health tests to monitor the health and performance of individual servers or for the entire organization or environment. Health tests detect problems by collecting and analyzing data or simulating user interaction with the server at regular intervals. Because UC Diagnostics is a monitoring tool, its functions only discover the servers in your organization and run health tests against the servers.

Each health test can run against individual servers or against groups of servers. Some tests, such as the Active Directory Account Lockout Health Test, cannot be run against individual servers and are run at the Exchange organization or Skype for Business/Lync environment level.

When you create a test from the Home Page, the entire organization is targeted by default. In a clustered environment, health tests run against the active node only. Health tests read information from nodes as a whole through a virtual server name.

By default, health tests are executed using the Diagnostic Services account. The Remote Registry Service is required for some health tests. Ensure this is running on your client. Only health tests that are relevant to available servers are shown when you right-click a server and select Detect. You can configure any test against a group.

All health tests use global settings such as notifications and alternate credentials. It is recommended you configure your global settings before you configure your health tests. For more information on configuring global settings, see .

Types of health tests

The Management Console includes the following health tests:

Table 1. Available health tests.

Organization/Environment	Health Tests
Exchange	• Exchange Server Health Test
	• Exchange Internal Server Delivery Health Test
	• Exchange Internal Mailbox Delivery Health Test
	• Exchange External Message Delivery Health Test
	• Exchange Modern Message Delivery Health Test
	• Exchange Storage Health Test
	• Exchange Queue Health Test
	• Internal Outlook Web Access (OWA) Availability Health Test
	• External Outlook Web Access (OWA) Availability Health Test
	• Exchange Replication Health Test
	• Exchange System Health Test
	• Active Directory Account Lockout Health Test
Office 365 (Exchange Online)	• Exchange Online Connectivity Health Test
	• Exchange Online Mailbox Logon Health Test
	• Exchange Online Message Delivery Health Test
	• Office 365 Subscription Health Test
BlackBerry	• BlackBerry Server Health Test
	• BlackBerry Message Delivery Health Test
Lync/Skype for Business	• Lync/Skype Server Health Test
	• Lync/Skype Instant Messaging Health Test
	• Lync/Skype Instant Messaging Conference Health Test
	• Lync/Skype Peer-to-Peer Audio/Video Call Health Test
	• Lync/Skype Audio/Video Conferencing Health Test
	• Lync/Skype Presence Status Health Test
	• Lync/Skype Logon Registration Health Test
	• Lync/Skype Address Book Service Health Test
	• Lync/Skype Persistent Chat Message Health Test
	• Active Directory Account Lockout Health Test
Office 365 (Skype for Business Online)	• Skype for Business Online DNS Connectivity Health Test
	• Office 365 Subscription Health Test
Office Communications Server (OCS	• OCS Server Health Test

By default, it is recommended that these tests be run every 30 minutes except for the server health tests. For more information about server health tests, see About server health tests on page 43

Creating and configuring health tests

You can perform the following functions with health tests:

- Creating a health test
- Specifying the test configuration
- Customizing counters
- Setting data collection options
- Managing health tests
- Cloning a health test
- Viewing test results

Creating a health test

If you select a container for a health test, the test runs against all servers in the group at the time of execution. Typically, the test would be configured for all servers. If you add a new server, the test automatically runs against that server (without needing to be updated). You can configure a test to run only once or at regular intervals during a specified time period.

When creating a test, you can set the conditions, error thresholds, and warning thresholds. You can also specify the number of alarms to be skipped before notifications are sent. You might want to ignore notifications for occasional spikes, and only be notified if there are consecutive alarms.

For example, if your tests are configured to alert on errors only, you might decide to ignore notifications until a counter exceeds the error threshold four times consecutively. You would enter 3 in the Alarms to skip before sending notifications box. In this case, you are notified after the error threshold is exceeded four times in a row.

To create a health test

1 Right-click the Exchange organization node or the Lync/Skype environment node and select **Detect | <test name>**.

   - OR -

2 Right-click a selected server and select **Detect | <test name>**.

3 On the General Test Information dialog box, specify the Test Name and Test Targets and click **Next**.

4 Review the test execution schedule, test credentials and notification settings in the Test Settings dialog box. Make any required changes to the selections and click **Next**.

   For more information on configuring Test Settings, see Specifying the test configuration on page 28.

5 Select the server type in the left pane of the New <platform type> Server Health Test dialog box to indicate the type of server whose metrics you want to specify.

   This dialog is displayed for selected tests and environments. Skip this step if the dialog is not displayed.

6 Review the metrics you want to monitor for the selected target by configuring and selecting the Network, Volumes, Services, Performance Counters and Event Log metrics.

7 Review the Condition, Warning Threshold and Error Threshold values and click **Next**.

8 Use the Summary page to review and confirm the general, test and notification settings you have made then click **Finish** to accept the settings.

Once the test is created, it runs immediately.

The Server Health test is preconfigured with general defaults. Some tests have counters preconfigured to skip an alarm the first time it occurs before sending a notification. For a list of these counters, see Counters with Non-Zero Alarm Values on page 187.

Specifying the test configuration

When scheduling health tests, you must provide details about the following settings:

- Configuring the execution schedule
- Configuring notification settings
- Adding notification recipients
- Adding notification groups
- Configuring alternate credentials
- Managing database settings

Configuring the execution schedule

Use the Execution schedule panel to set up the frequency and the time frames during which you want the tests to run. The following options are available in the Execution Schedule panel:

Table 2. Scheduling options.

Option	Description
Run once	Select this to run the test immediately, and on demand.
Run every (minutes)	Select this to enter the time interval in minutes after which the next test starts. **NOTE:** If a test is scheduled to run every ten minutes (for example 12:00), but a test iteration takes 15 minutes, the test skips the next iteration (that is, 12:10), and the next iteration does not run until the next scheduled time (that is 12:20).
Use execution window	Select this check box to only run within a specific time window. You must specify a Start time and End time for the Test Execution Schedule.
Run every day at	Select this to schedule the test to run once daily at this specific time.

For information on setting notifications and credentials, Configuring notification settings on page 28 and Configuring alternate credentials on page 33 respectively.

To run the test now

- Expand the Tests node in the Management Console treeview, right-click the test you want and select **Run Now.**

You can use the Run Now option on scheduled or unscheduled tests.

Configuring notification settings

Use the Notification Settings panel to select the group that is notified when the server counter values exceed the configured threshold. You can configure notification settings to alert users about errors only or about both errors and warnings. To save time, configure the global settings before you configure individual tests.

When you specify the SMTP server to be used for notifications, you can use the default values of port 25 and anonymous authentication or you can specify any or all of the following options:

- enter a custom port number
- specify that STARTTLS protocol be used
- use specific credentials for SMTP server authentication

You can create notification groups to allow specified groups to receive messages about alarms, warnings, or errors on a per counter basis. You can send notifications only to groups, not to individual users.

Use the Add Recipients dialog box to specify the members of each group. You can include the same recipients across notification groups.

You can specify the following notification parameters:

- whether you want the emails in HTML or Plain Text format
- the level of severity at which you want to receive email messages
- an arbitrary command line executable to be run

Adding notification recipients

To create recipients to receive notifications

1 If you are in the process of creating a test, click **Manage Notifications** in the Test Settings page.

- OR -

Expand the Global Settings node in the Management Console treeview and select **Notifications**.

2 Enter the name of an SMTP server in the Primary SMTP Server field.

    a If you need to specify a custom port for the SMTP server, enter the number in the **Port** field.

      By default, port 25 is used.

    b If you need to use STARTTLS protocol, select the check box beside **Use STARTTLS**.

3 Optionally, enter the name of a second SMTP server in the Secondary SMTP Server field.

    a If you need to specify a custom port for the SMTP server, enter the number in the **Port** field.

      By default, port 25 is used.

    b If you need to use STARTTLS protocol, select the check box beside **Use STARTTLS**.

4 If you require specific credentials for the SMTP server authentication, click **Add** in the Notification Credentials section.

    a Enter the email address for the account to be used.

    b Enter the password and confirm it.

    c Click **OK**.

5 In the Notification Recipients section, click **Add**.

    a Enter the recipient's name and email address.

    b Select the format of emails the recipient is to receive: either HTML or Plain Text.

    c Select the type of alarms the user is to receive: errors and warnings or only errors.

    d If you require that a credential be used for authentication when sending the test message, select the **Use credential for send test** check box and select a credential from the list you created under the Notifications Credentials section.

    e Click **OK**.

      You can send a test message to see if the SMTP server is working by clicking the **Send Test** button. This ensures that UC Diagnostics can deliver a message to the specified email address.

6 Click **OK**.

Adding notification groups

After you have added recipients, you can create notification groups that include the recipients.

To add a notification group

1 Expand the Global Settings node in the Management Console treeview and select **Notifications**.

2 In the Notification Groups section, click **Add**.

3   Enter the sender's name and email address.

4   If credentials are required for SMTP authentication, select the **Use credential for SMTP server authentication** check box.

    a   Select a credential from the list of Notification Credentials and click **Add**.

5   Select the recipients to receive notification messages.

6   Select an external application command line to execute processes such as Passing alerts using SNMP on page 32.

7   Set limits on notifications. For more information, see Setting limits on notifications on page 30.

8   Click **OK**.

Tokens supported by the external command line

The following list shows the tokens that are supported for the external application command line. The tokens are replaced with corresponding real time results, when the external application is run.

Notification tokens:

- $SenderName$
- $SenderEmail$

Counter tokens:

- $CounterName$
- $CounterGroupName$
- $CounterValue$
- $CounterOutcome$
- $CounterOperator$
- $CounterThreshold$

Server tokens:

- $ServerName$
- $ServerOutcome$

Test tokens:

- $TestOutcome$
- $TestName$

The tokens dictate how many times the external application is called. The Notifications tokens are general tokens. With the Counter tokens, the external application is called once per test per each server per counter. With the Server tokens, the external application is called once per test per each server. With the Test tokens, the external application is called once per test.

Setting limits on notifications

You can configure notification groups to:

- receive unlimited notification messages
- receive a notification when an alarm clears
- set the maximum number of notification messages a user is to receive per each alarm

Best practices for setting notifications

The following best practices are recommended when you set notifications:

You can receive a notification when an error occurs for a specified number of times. If the error still occurs after the specified number of times, you do not receive further notifications. In this cas you can receive a notification when the alarm is cleared. To do this:

1   Deselect the **Send unlimited notifications for an alarm** check box.

2   In the **Maximum number of notifications to send per alarm** box, enter a number for the maximum number of times you would like to receive a notification.

3   Select the **Send alarm cleared notification when alarm ends** check box.

You can receive unlimited error or warning notifications, but choose not receive cleared notifications. This assumes that once you stop receiving error or warning notifications, the alarm has been cleared. To do this:

1   Select the **Send unlimited notifications for an alarm** check box.

2   Deselect the **Send alarm cleared notification when alarm ends** check box.

To receive messages on cleared alarms

A cleared alarm is an alarm that recipients need not manage - either the problem has been resolved or has become less severe. For example, if you are receiving notifications on errors only, and the status changes from error to warning, the alarm is considered cleared. If you are receiving notifications on both errors and warnings, and the status changes to success, the alarm is considered cleared.

1   Add a notification group.

2   Select the **Send alarm cleared notification when alarm ends** check box.

3   Click **OK**.

If a specific event is found in the event log while you run a Server Health Test (such as an Exchange Server Health Test), an event notification is sent to the notification recipients with the corresponding severity. The next time that the Server Health Test runs, the test scans only the event logs from beyond the time of the previous test run.

If no identical event is found during the second run, the notification engine does not issue the cleared notification for the event. If the event is not found during the second test run, the problem is not necessarily resolved. It only means there are no new events logged for the exact same problem.

To receive unlimited notification messages

This feature allows you to receive unlimited notifications about alarms on counters.

1   Add a notification group.

2   Select the **Send unlimited notifications for an alarm** check box.

3   Click **OK**.

Selecting this option overrides the maximum number of notification messages you may have set.

To set the maximum number of notification messages per alarm

This feature can help you limit the number of notification emails you receive if you encounter problems with the same counter.

1   Add a notification group.

2   Enter a number in the **Maximum notifications to send per alarm** box.

3   Click **OK**.

For example, if you have a recipient configured to receive a maximum number of 3 notifications, you receive a notification the first time the alarm occurs, then two other times, if there is still a problem with the counter.

Also, you can have your notifications set to receive errors only if your performance counters on your Front-End server exceeds its error threshold, and you have selected the **Send alarm cleared notification when**

problem ends check box. You receive a notification the first time the error occurs, and two more times if the error occurs on that performance counter again. If the fourth time, the error threshold is no longer exceeded, you receive a cleared notification.

Passing alerts using SNMP

You can pass alerts to external applications using Simple Network Management Protocol (SNMP).

1   Add a notification group.

2   Click in the Execute command line box, and enter the following:

```
"<Program Files>\Quest\UC
Diagnostics\ManagementConsole\Binaries\iwsnmptrap.exe" <server> <community
name> 6 0 "$CounterOutcome$ on $ServerName$ - $CounterName$ = $CounterValue$"
```

where

- <Program Files> indicates the Program Files directory path of the computer running Diagnostic Services

- <server> indicates the computer name to receive the SNMP trap

- <community name> indicates the SNMP community name (usually "public")

    For example, you can enter:
    ```
    "C:\Program Files\Quest\UC Diagnostics\ManagementConsole
    \Binaries\iwsnmptrap.exe" 10.4.60.95 public 6 0 "CounterOutcome$ on
    $ServerName$ - $CounterName$ = $CounterValue$"
    ```

3   Click **OK**.

    Apply the notification group to the tests for which you want to generate SNMP traps.

Passing only errors using SNMP

If you want to pass errors only using SNMP, you can create a batch file that contains the tokens you want to use in your notifications.

1   Create a batch file, and enter:
    ```
    If %1 == error "C:\Program Files\Quest\UC
    Diagnostics\ManagementConsole\Binaries\iwsnmptrap.exe" 10.4.60.95 public 6 0
    "%1 on %2 - %3 = %4".
    ```

2   Name the batch file snmp.bat.

3   In the Notifications dialog box, add a Notifications group. Enter a Sender name and email address.

4   In the External application command line, enter:
    ```
    "<directory of snmp.bat file>\snmp.bat" "$CounterOutcome$" "$ServerName$"
    "$CounterName$" "$CounterValue$", and save the notification group.
    ```

Using SMS notifications

You can configure UC Diagnostics for Short Message Service (SMS) notifications.

To configure SMS notifications

1   Add a notification group.

2   In the Execute command line box, enter:

```
<Directory of sms.vbs file>\sms.vbs "$TestName$" "$ServerName$" "$ServerOutcome$"
```

    If the directory path to your sms.vbs file contains spaces, enclose the path with quotes.

3   Create the following sms.vbs file:

```
if (Wscript.Arguments.Count = 3) then
dim message
set message = CreateObject("CDO.Message")
```

```
message.From = "SOM@yourdomain.com"
message.To = "XXXXX@yourdomain.com"
message.Subject = Wscript.Arguments(1) & " - " & Wscript.Arguments(2) & " - " &
Wscript.Arguments(0)
message.Textbody = ""
message.Configuration.Fields.Item("http://schemas.microsoft.com/cdo/configuration/s
endusing") = 2
message.Configuration.Fields.Item("http://schemas.microsoft.com/cdo/configuration/s
mtpserver") = "relay.yourdomain.com"
message.Configuration.Fields.Item("http://schemas.microsoft.com/cdo/configuration/s
mtpserverport") = 25
message.Configuration.Fields.Update
message.Send
end if
```

> This script displays Text name, Service name, and Status only, and does not send an SMS message directly. It only demonstrates a way to tailor the notification and run an external application/script.
>
> Sending SMS messages usually depends on you service provider. They may provide you an application or some web based way to submit it. A common practice is to provide "email to text message" service.

4   Save the file to the computer where the Diagnostic Services is installed at the following location: <Program Files>\Quest\UC Diagnostics\ManagementConsole\Binaries.

Configuring alternate credentials

By default, user credentials are specified when you install the Diagnostic Services used for test execution. You can override the initial credentials for a specific test by specifying and configuring alternate credentials. Alternate credentials are used to run tests under different credentials than those specified in the Diagnostic Test Engine (DTE). The credentials are stored encrypted in the database.

If you are using alternate credentials on Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Microsoft Windows Server 2019 or Windows Server 2022, you must disable UAC on the client from the Registry Editor. Restart your computer for the changes to take effect.

You cannot run PowerShell cmdlets across domains with alternate credentials.

> **i** | **TIP:** To save time, configure the global settings before configuring your tests.

To manage alternate credentials

•   If you are in the process of creating a test, click **Manage Credentials** in the Test Settings page.

    Otherwise, expand the Global Settings node in the Management Console treeview and select **Alternate Credentials**.

Managing database settings

Database Settings identify the server on which your database is installed, the size of your database, and how much free space you have within your database.

Database retention controls the length of time that the health test result data is kept in the database before being purged. You can set the database settings for weekly or hourly retention rates. The test result data is aggregated into hourly and daily historical data. This data is used for the Web Reports.

You can also use Database Settings to set Test Results History and purge test results from the database after the specified number of days. Test results are purged upon the next test execution after midnight (UTC).

If you want to purge the data from the daily Web Reports and Test Results before the specified execution time, click the Purge Now button next to the Web Reports daily data retention (days) or the Test Results data retentions days boxes.

Due to the amount of space that test history requires in the database, you can increase the value for Test History retention (days). For more information, see the section titled Historical Reporting Database Usage Estimates in the *Unified Communications Diagnostics Deployment Guide*.

Customizing counters

You can perform several customizing functions on counters, depending on the type of health test and the nature of the counter. These functions are divided into ones that can performed in the Server Health test only, and those available in other health tests.

Customizing Counters in the Server Health Test

> Adding services
>
> Adding performance counters
>
> Adding event log entries
>
> Deleting services, performance counters, and event log entries

Editing Counter Thresholds

> Editing counters while creating a health test
>
> Editing Individual server thresholds while creating a health test
>
> Editing counter thresholds in the test results pane

Adding services

You can include additional services that you want to monitor for the specific server health test that you want to run.

To add services

1   Click **<Add Services>** located under the Services sections in the listview of the server health test that you select.

2   Enter a name to query a list of current services you want to monitor and the services you want to add in the Select Services dialog box and click **OK**.

3   Configure the thresholds you want to monitor for the new service you have added.

Adding performance counters

You can include additional performance counters that you want to monitor for the specific server health test that you want to run.

You can add more than one instance of the same performance counter if you want to monitor for different conditions. For example, two instances of the counter "MSExchangeTransport Queues\Retry Mailbox Delivery Queue Length (_Total)" are pre-defined.

•   The first instance is set to detect a large value of the counter (a value greater than 100 generates a warning, and a notification is sent the second consecutive time it happens).

•   The second instance is set to detect several consecutive small values of the counter (a value of 1 generates a warning, 2 or more generates an alarm, but notifications are sent only when this happens 4 times in a row).

To add performance counters

1   Click **<Add Performance Counters>** located under the Performance Counters section in the listview of the server health test that you select.

2   Enter the name of the server you want to monitor, the performance object and counter you want to add, and select the instances, if applicable, you want to monitor in the Performance Counters dialog box and click **OK**.

3   Configure the thresholds you want to monitor for the new performance counter you have added.

> **i** | **TIP:** The Network Interface(*)\Bytes Total/sec counter indicates the rate at which the network adapter is processing data bytes.
>
> - If you are using a 100-MBps network adapter, set the counter to less than 6000000 - 7000000 bytes.
> - If you are using a 1000-MBps network adapter set the counter to less than 60000000 - 70000000 bytes.
>
> Exchange health tests with preconfigured counters use the threshold value for 1000-MBps network adapter, which is 73400320 bytes. If you are using a 100-Mbps network adapter, you may modify the counter to 7340032 bytes.

For more information on counters, see Counters with Non-Zero Alarm Values on page 187.

Adding event log entries

You can include additional Event Log Entries that you want to monitor for the specific server health test that you want to run.

To add event log entries

1   Click **Add Event Log Entries** located under the Event Log section in the listview for the server health test you selected.

2   Enter the event log name for the log file in the Event Log field.

3   Enter the event provider name in the Source field.

> **i** | **IMPORTANT:** If you view the Windows event log properties in the Event Viewer, the event source is not the Source that appears in the General tab. The source that you specify when adding event log entries is the Provider Name that appears under the Details tab.
>
> You can also enter a wild card character (*) at the end of the source string. For example, BlackBerry* would match the BlackBerry Policy Service, BlackBerry Router, etc.

4   Enter the event IDs you want to add in the Event IDs. For more information, see Options for specifying event IDs on page 35.

5   Click **OK**.

6   Configure the metrics you want to monitor for the new event log entry you have added.

Options for specifying event IDs

You can monitor specific event logs by filtering by event IDs or by text in the event ID descriptions. You can specify the following:

- a specific event ID, such as 1000
- multiple event IDs separated by commas
- ranges, such as 1000-2000 (no spaces)
- " * " to monitor all event IDs
- an event ID or range of event IDs with text separated by a colon, as in the following examples:
    - **1000:Error** to monitor events with event ID 1000 and containing the word 'Error'
    - **1000–2000:Error** to monitor events within the range of event IDs 1000 to 2000 and containing the word 'Error'
    - **1004:!Error** to monitor events with the event ID 1004 and not containing the word 'Error'

- **1004–1005:!Succeeded** to monitor events within the range of event IDs 1004 to 1005 and not containing the word 'Succeeded'
- **1000–2000:Error,1010:!Warning** to monitor all events between event ID 1000 and 2000 that contains the word 'Error', except those with event ID 1010 that contains the word 'Warning'
- **1000:Long Phrase** to monitor events with the event ID 1000 that contains the specified long phrase. It cannot contain a comma.
- **1000:Error, 1000:Warning** to monitor all events with the event ID 1000 and contains the word 'Error' or 'Warning'

The following rules apply:

- If you have both an inclusive filter and an exclusive filter for the same ID, the exclusion filter takes precedence.
- If you want to look for multiple words that are not a phrase, you must add them separately.

Event log entries for Exchange crimson channels

The Exchange Applications and Services event logs store the events from a single application or component instead of events that have system-wide impact. This category of event logs is known as an application's crimson channel.

When creating a server health test for Exchange 2013 and Exchange 2016 mailbox servers, you will see the Microsoft-Exchange-HighAvailability/Monitoring log entry is set by default in the event log list.

For other crimson channel log entries or for earlier versions of Exchange, Lync or Skype for Business, or Blackberry, you can manually add an log entry for an Applications and Services event log.

To manually add an log event entry for an Applications and Services event log

1. In the Microsoft Windows Event Viewer, navigate to the event log that you want,
2. Right-click on the event log.
3. Click **Properties** and copy the name that appears in the **Full Name** field.
4. In the UC Diagnostics Management Console, when creating the server health test, click **Add Event Log Entries** located under the Event Log section.
5. Enter the full log name that you copied from the log properties page to the Log Name field.
6. Specify * as the Source.
7. Enter the event IDs you want to add in the Event IDs.
8. Click **OK**.
9. Configure the metrics you want to monitor for the new event log entry you have added.

Deleting services, performance counters, and event log entries

To delete services, performance counters, and event log entries

- Right-click the description of a service, performance counter, or event log entry, and select **Delete**.

You can select multiple services, performance counters, or event log entries to delete them at the same time.

Editing counters while creating a health test

For many counters, you can change the following fields in the New Health Test wizard:

- description

- role

- condition

- warning and error thresholds (numerical counters only). In addition to specifying default thresholds (for all servers), you can create server-specific thresholds, which override default values.

- alarms to skip before sending notification

Some of these fields do not exist for some counters. In some counters, certain fields cannot be changed. If you cannot perform the following procedures, this is an indication that the field in the current counter cannot be changed.

To edit a description

1 Right-click somewhere on the counter, and click **Edit Counter Name**.

2 Change the description in place.

If you enter invalid characters, the description does not change.

To edit a role

1 Click the current Role value.

2 In the dialog that appears, click one or more check boxes to select or deselect the roles for this counter. To select all roles, select **All**.

3 Click **Close** to remove the dialog.

To edit a condition

1 Click the current Condition value.

2 In the drop-down list, select the new value for the condition.

Changing the condition may cause current threshold values to become invalid. You must correct the thresholds or restore the condition value before leaving the wizard. Values that must be corrected are red.

To edit default warning or error thresholds for all servers

1 Click on the current value and enter a new value in place.

You cannot edit a warning threshold or error threshold if the value in the Condition column is set to Informational or Disabled. If you leave a threshold field with an invalid value, the previous value is restored.

To add or edit warning or error thresholds for individual servers

1 Right-click somewhere on the counter and click **Edit Server Thresholds**.

2 If the target server is listed, select it and click **Edit**, or double-click the target server.

If the target server is not listed, click **Add**. In the Server Thresholds dialog, click **Browse**. In the Select Servers dialog, check the boxes for one or more servers, or group. Click **OK**.

You can add several servers and apply server-specific thresholds to them together. But once listed, you can only select one server to edit. To modify multiple servers that are listed, click **Add**, reselect them, and specify new thresholds.

3 In the Server Thresholds dialog, enter values for the Error threshold and/or Warning threshold.

Warning thresholds may need to be higher or lower than Error thresholds, depending on the current condition. Violations are indicated by a red warning bullet. You cannot leave this dialog with invalid threshold values.

4 Click **OK** to accept changes and exit the Server Thresholds dialog.

5 Click **OK** to return to the Health Test wizard.

Notice that servers with server-specific thresholds are listed in the Overrides column for the counter. Position the cursor over this field to see an expanded list of servers (up to 5) that have server-specific

thresholds. Right-click and select **Edit Server Thresholds** to view all servers with server-specific thresholds.

To edit the alarms to skip before sending notification

1   Click on the current value and enter a new value in place.

By skipping the specified number of alarms before a notification is sent you can avoid notifications on occasional spikes in the counter values. See Creating a health testCreating a health test for more information.

Editing Individual server thresholds while creating a health test

In the Edit Server Thresholds dialog, if no Server is shown, click the Browse button. In the Select Servers dialog, check the boxes for one or more servers, or group. Click OK to return.

Specify Error and/or Warning threshold values for the selected Server. If only one threshold is specified, the other threshold assumes the value shown in the Default counter thresholds, if present.

These values override the default threshold values for this server only, and only in this health test.You cannot leave this dialog with invalid threshold values specified.

In the health test creation wizard, up to 5 servers that have a server specific threshold defined are listed in the Overrides column for that counter. To view all servers with override values, right-click on the counter and select **Edit Server Thresholds**.

Editing counter thresholds in the test results pane

You can edit counter thresholds in the Test Results section without opening an associated health test wizard.

You can edit default error and warning thresholds that apply to all servers. You can also specify server-specific error and warning thresholds. These override the default values.

Counters with the same name may be defined on the same page of the Exchange Server Health test wizard. Both counters are required to define test conditions. Do not change the thresholds for either one of these counters in the Test Results area because both counters are changed which significantly alters test conditions and test results.

To edit the threshold of a counter

1   In the Test Results tab, select a test result.

2   In the lower panel, double-click a counter with highlighted thresholds. Alternatively, right-click on a highlighted threshold and select **Edit Thresholds**.

The Edit Counter Thresholds dialog contains the following sections:

Table 3. Counter thresholds for test results.

Section Name	Description
Counter thresholds at the time of test execution	ndicates the default or server-specific counter threshold values set at the time the test was executed. These values cannot be changed.
Current default counter thresholds	indicates the threshold values for servers that do not have server-specific thresholds set
Current server-specific counter thresholds	indicates the threshold values for the current server, if applicable for the specific test type.

3   Enter new warning and/or error thresholds for the current default counter thresholds, or for a specific server.

To remove a server-specific threshold, delete any current value in the threshold box and leave the field empty.

4   Click **OK**.

The new threshold values are in effect on the next test execution.

Some counters are configured to use wildcards. If you edit the threshold of a particular counter (in Test Results) using one of the instances reported in test results, then the new threshold value is applied to all instances of the counter.

For example, if you create an Exchange Server Health Test, there is a performance counter called Network Interface\Packets Outbound Errors (<All instances>). When you view the test results, you will notice that there are two instances of Network Interface\Packets Outbound Errors that were monitored.

If you edit the threshold of one instance of this counter in the test results pane, then the threshold of the other instance of this counter is also changed.

This applies to performance counters only.

Setting data collection options

Data collection options can affect the server health test results that are returned for volumes, network availability, and services:

This section describes some of the configuration options that can be used to affect the Server Health tests:

- Volumes - Allowing API fallback if WMI fails

- Network Availability - Disabling reverse DNS lookup alarm

- Services - Ignoring warnings for some services

For the Exchange System Health test, there is a data collection configuration option used to ignore warnings for target servers on which health sets are not installed. For information about health sets and the Exchange System Health test, see Exchange System Health Test on page 67.

- Health Sets - Ignoring warnings if health sets not installed

Volumes - Allowing API fallback if WMI fails

WMI is used to retrieve accurate disk space information when using mount points. If you do not use mount points, you can configure your tests to use Windows API if WMI fails.

When you make this change in one server type, all other server types are changed for the test.

To allow Windows API fallback

1   In the Server Health Test, select a server type.

2   Click **Data collection options**.

3   Cick the **Volumes** tab and select **Allow API fallback if WMI fails**.

Do not use Allow Windows API fallback if WMI fails if the volume is mounted on a network-attached storage device because the metrics returned may not be accurate.

4   Click **OK**.

Network Availability - Disabling reverse DNS lookup alarm

The Server Health test always performs a reverse DNS lookup to validate that DNS server has a record that maps the IP address of the target server to the host name. By default, the reverse DNS lookup alarm is enabled. If you do not want the test to alarm if the names returned by a DNS lookup do not match the FQDN of the target server, you can disable this option.

When you make this change in one server type, all other server types are changed.

To disable alarm on reverse DNS lookup

1   In the Server Health Test, select a server.

2   Click **Data collection options**.

3   Click the **Network Availability** tab and clear the **Alarm on reverse DNS lookup** check box.

4   Click **OK**.

Services - Ignoring warnings for some services

The Server Health test normally reports all warnings and errors that exceed their thresholds. However, you can ignore warnings for services that are not installed in the target server or warnings for services that are not configured to start automatically.

To ignore warnings for certain services

1   From the Server Health Test, select a server.

2   Click **Data collection options**.

3   Click the **Services** tab.

4   To ignore warnings from uninstalled services, select **Ignore services not installed**.

5   To ignore warnings from services that are not started up automatically, check **Ignore services with non-automatic startup type**.

Health Sets - Ignoring warnings if health sets not installed

The Exchange System Health test monitors the health state for different groups of monitors, called health sets. If all a health set's monitors are healthy, the health set is in a healthy state. If any monitor is not in a healthy state, the health set state is determined by its least healthy monitor.

If health sets are not installed on the target server, the counters would be shown with a status of "Not Complete". You can use the following option to ignore warnings for health sets that are not installed in the target server.

To ignore warnings for certain health sets

1   From the System Health Test, select a server.

2   Click **Data collection options**.

3   Click the **Health Sets** tab.

4   To ignore warnings for health sets that are not installed on the selected server, select **Ignore health sets not installed**.

If, at a later date, health sets are installed on the Exchange target server, you can clear the check box.

Managing health tests

After you create health tests, you can modify the test settings (schedule, notifications, credentials), disable or enable a test, or delete a test.

To edit a test

1   Expand the Tests node in the Management Console treeview, right-click the test you want to edit, and select **Edit**.

2   Edit the existing settings you want to change in the Execution Schedule, Notification Settings, and Alternate Credentials Settings dialog boxes and click **Next**.

3   Edit the metrics you want to change in the test-specific pages and click **Finish**.

The edited test is displayed under the Tests node.

To enable/disable a test

- Expand the Tests node in the Management Console treeview, right-click the test you want to edit, and select **Enable** or **Disable**.

To delete a test

- Expand the Tests node in the Management Console treeview, right-click the test you want to delete, and select **Delete.**

Raw historical data is deleted; aggregated data is kept and is purged as scheduled.

Cloning a health test

A cloned test allows you to create a new health test based on an existing one, thus eliminating the need to create a new test from the beginning.

To clone a test

- Expand the Tests node in the Management Console treeview, right-click the test that you want to clone, and select **Clone.**

  The Edit wizard appears with the information identical to that in the original test, except the test name appears as Copy of <name of original test>. You can change the name of the test, notifications, schedule, credentials, and make other changes to the server counters. When you finish editing the cloned test, the new test appears in the treeview.

Viewing test results

The Management Console allows you to view the results of generated tests. You can view test results by clicking a target in the topology view or treeview, then selecting the Test Results tab.

If you click a group in the treeview, results are displayed for all targets in the group.

Colored icons adjacent to a test in the Test node, servers in the organization node, or tests in the Test Results window indicate the following test status:

Table 4. Test result icons.

Icon	Definition
	Test is in progress
	Test has completed successfully
	Error threshold was violated
	Warning threshold was violated
	Value could not be retrieved
No icon	No tests are currently running

If the server is part of a group, the group shows the colored icon of the server with the worst severity. For example, if the group contains three servers: one server has a green icon, the other has a red icon, and the last has a grey icon. The group appears red.

You can hide the counters with successful results or hide informational counters to focus on the counters with errors or warnings.

To hide successful results

- From the Test Results tab, select **Hide successful results** from the Display drop-down.

  The selection is applied to all test results in your organization**.**

Viewing details on test results

You can click a counter test result to see detailed results about the test per target server, such as target name and test start and completion time. You can view details about a warning, error, or an incomplete test result on the counters in any test. If the counter is not successful, the details provide a summary of the warning or error, possible reasons why the counter is not successful, and possible solutions to remedy the problem.

To view more information

- Select a counter, the click the **Details** button.

Browsing test result history

You can view the data of test results that has been collected in the last seven days (by default), or view the data from tests results that were collected more than seven days ago.

To set the test results history

1 From the treeview, select **Global Settings | Database Settings**.

2 In the **Test Results History data retention (days)** box, enter the number of days.

To view the test results history

- From the Test Results tab, click the Results drop-down arrow to pick a date of which test results you would like to view.

  You can also use the left and right arrows to pick a date.

  Each test result has a colored icon attached to the left of the date to indicate if the test was successful or had warnings or errors.

Clearing the health test results

To clear the test results

- Expand the Tests node in the Management Console treeview, right-click the test whose results you want to clear, and select **Clear Test Results.**

The test results are cleared only in the Management Console. The next time you open the Management Console, the test results appear.

You can run the test again to bring back the results by right-clicking the test and selecting Run Now.

About server health tests

Use the server health tests to monitor the overall health and performance of your Exchange, BlackBerry, OCS or Lync/Skype servers. The test verifies various performance counters, services, event logs, disk space, and network availability. You can schedule the Server Health test to proactively check the status of your servers before problems occur, or you can schedule tests to run after you fix an issue to ensure the server problem is resolved.

It is recommended that you configure two server health tests - one without monitoring event logs with an interval of 30 minutes and the second for monitoring event logs that run only once a day.

The following server health tests are available for the various platforms:

- Exchange Server Health Test
- BlackBerry Server Health Test
- Lync/Skype Server Health Test
- OCS Server Health Test

For more information on test settings, see Specifying the test configuration on page 28.

For information on creating and configuring a server health test, see Creating and configuring health tests on page 27.

It is recommended that you configure two server health tests - one test without monitoring event logs with an interval of 30 minutes and the second test for monitoring event logs that run only once a day. For more information on test settings, see Creating and configuring health tests on page 27.

Health tests available for multiple platforms

Most health tests are specific to a certain platform such as Exchange or Skype for Business. However, some tests can be run for more than one platform.

Active Directory Account Lockout Health Test

The Active Directory Account Lockout Health test provides information about how many and which Active Directory accounts are currently locked out. The test shows accounts that are locked out due to invalid passwords being submitted and accounts that are locked because the password has expired. The test detects the domain accounts that are currently locked out and provides information about the lockout event.

You run the test against a domain to which an Exchange organization or a Lync/Skype for Business environment belongs. You cannot run the test against the individual servers.

i | **NOTE:** Information about locked-out accounts is available only for the first 1000 accounts.

The Active Directory Account Lockout Health test contains the following counters:

Table 5. Active Directory Account Lockout health test counters.

Category	Counter
General	• Total accounts locked out
Lockout information	• User status
	• Last time bad password was submitted
	• Number of login attempts with bad password
	• Date and time account was locked out
	• Last time password was changed
	• Next expiry date for password

Active Directory Account Lockout Health test prerequisites

The following tables show the test targets for the test and the permissions required by the test credentials.

Table 6. Active Directory Account Lockout Health test targets.

Platform Versions	Target Type
Exchange 2007/2010/2013/2016	Organization
Lync 2010/2013 and Skype for Business 2015	Environment

The test credentials must have read permission on User objects in Active Directory.

Table 7. Active Directory Account Lockout Health test credential required permissions.

Platform	Permissions Required for Test Credentials
Exchange	• Member of View-Only Exchange Administrators group or View-Only Organization Management group.
Lync/Skype for Business	• Member of CSHelpDesk, CSServerAdministrator, or CSViewOnlyAdministrator group

Office 365 Subscription Health Test

The Office 365 Subscription Health test provides an overview of your Office 365 licensing plans. Licensing plans define the Office 365 services that are available to users. The test shows license activity such as the number of licenses that are currently assigned to users (used) and how many licenses are due for renewal.

About the Office 365 subscription lifecycle

During the first 30 days after an Office 365 subscription ends, the Office 365 tenant account is in a period known as the expired state. During the expired period, users can still access data. After 30 days, the tenant account enters the disabled state for 90 days. During this period, users cannot access data. An Office 365 administrator can log in, backup data, or reactivate the subscription.

At the end of the disabled state, 120 days after the subscription has ended, the account enters the deprovisioning state. During the deprovisioning state, the data from user accounts and also email data and documents, is permanently deleted.

Table 8. Office 365 subscription health test counters.

Category	Counter
Total licenses	Total number of purchased licenses in the licensing plan.
Number of licenses used	Number of licenses that have been assigned to users in the specified licensing plan.
Number of licenses used (%)	Percentage of licenses that have been assigned to users in the specified licensing plan.
Number of licenses that must be renewed	Number of licenses in the licensing plan that have not been renewed and that will expire after the 30-day grace period.
Next lifecycle date	Next date on which a subscription lifecycle event occurs. Lifecycle events can include states such as active, expired, disabled, or deprovisioned.
Next lifecycle date (days)	Date on which the next subscription lifecycle event will occur that is less than the specified number of days. You can set thresholds for warning and error notifications.

Table 9. Office 365 subscription health test targets.

Platform	Target Type
Office 365	All services

The following software is required.

Table 10. Office 365 subscription health test required software.

Platform	Software Required on the UC Diagnostics computer
Office 365	• Windows PowerShell 5.0 or later • Microsoft Online Service Sign-in Assistant • Microsoft Azure Active Directory Module for Windows PowerShell • Microsoft Exchange Online PowerShell Module

Table 11. Office 365 subscription health test credential required permissions.

Platform	Permissions Required for Test Credentials
Office 365	Valid Office 365 credential that was used to connect to Office 365.

If the password of the Office 365 credential is changed, you must change the password on Office 365 connection properties.

Health tests available from the Exchange organization node

- About the Exchange-based health tests
- Exchange Server Health Test
- Prerequisites for Exchange Delivery Health Tests
- Exchange Internal Server Delivery Health Test
- Exchange Internal Mailbox Delivery Health Test
- Exchange External Message Delivery Health Test
- Exchange Modern Message Delivery Health Test
- Exchange Storage Health Test
- Exchange Queue Health Test
- Internal Outlook Web Access (OWA) Availability Health Test
- External Outlook Web Access (OWA) Availability Health Test
- Exchange Replication Health Test
- Exchange System Health Test
- Active Directory Account Lockout Health Test
- Exchange Online Connectivity Health Test
- Exchange Online Mailbox Logon Health Test
- Exchange Online Message Delivery Health Test
- Office 365 Subscription Health Test
- BlackBerry Server Health Test
- BlackBerry Message Delivery Health Test
- Creating test mailboxes for Exchange
- Configuring Exchange impersonation for the Modern Message Delivery health test
- Registering UC Diagnostics with the Microsoft Azure portal

About the Exchange-based health tests

The following health tests are available when you right-click the Exchange organization node:

Table 1. Available health tests for Exchange organization.

Organization/Environment	Health Tests
Exchange	• Exchange Server Health Test • Exchange Internal Server Delivery Health Test • Exchange Internal Mailbox Delivery Health Test • Exchange External Message Delivery Health Test • Exchange Modern Message Delivery Health Test • Exchange Storage Health Test • Exchange Queue Health Test • Internal Outlook Web Access (OWA) Availability Health Test • External Outlook Web Access (OWA) Availability Health Test • Exchange Replication Health Test • Exchange System Health Test • Active Directory Account Lockout Health Test
Office 365	• Exchange Online Connectivity Health Test • Exchange Online Mailbox Logon Health Test • Exchange Online Message Delivery Health Test • Office 365 Subscription Health Test

You can also create a Generic Server Health Test to monitor your generic servers. To create a Generic Server Health Test, see Creating and configuring health tests on page 27.

Exchange Server Health Test

The Exchange Server Health Test allows you to monitor the basic health of all your Exchange servers. This test allows you to monitor the following types of information:

- Network availability (like ping time)
- Operating system disk space usage
- Any Performance Counter
- Any Windows service
- Any Event Log entry

You can run the server health test against any version of Exchange.

For information about the required configuration on each Exchange server and the required permissions for the test credentials, see the *Unified Communications Diagnostics Deployment Guide*.

Prerequisites for Exchange Delivery Health Tests

The following prerequisites are common to all the Exchange delivery health tests:

Table 2. Software required for the Exchange delivery health tests.

Exchange Version	Required Software
Exchange 2007/2010/2013	• For Exchange 2007, 2010, or 2013, install MAPI & CDO (version 8.3.0.8353.000 or later). You can download MAPI & CDO here:: • https://www.microsoft.com/download/details.aspx?id=42040
Exchange 2010 and later	• PowerShell 2.0 or later

See the individual test descriptions for information about required configuration and permissions needed to run each test:

> Exchange Internal Server Delivery Health Test
>
> Exchange Internal Mailbox Delivery Health Test
>
> Exchange External Message Delivery Health Test
>
> Exchange Modern Message Delivery Health Test

Exchange Internal Server Delivery Health Test

The Exchange Internal Server Delivery Health test is used to monitor the sending and receipt of messages within an Exchange organization.This test sends a test message from each target server in the test to every other target server.

The Exchange Internal Server Delivery Health test sends a test message from each selected server to every other selected server. For example, if you select your whole organization as the test target and your organization has five mailbox servers, this test sends 20 test messages (5 source servers x 4 destination servers) at each monitoring interval.

This health test is not supported for Exchange 2013 and later. This test is also not useful for Exchange 2010 organizations that have implemented Database Availability Groups (DAGs) since mailboxes in a DAG are not linked to a specific server.

On Exchange 2007 servers, when the test runs, it looks for a test mailbox on each server. The test mailbox can be on any store on that server. You need one test mailbox per server to run this test. If there are multiple test mailboxes on each server, the test uses the first mailbox it finds. By default, the test mailbox creation scripts create one test mailbox per store.

You can configure this test to collect tracking information to trace the test message that flows through the Exchange servers.

For Exchange 2007, you can use the Internal Mailbox Delivery Health test to monitor the sending and receiving of messages between mailboxes. For Exchange 2010 and later, you can use the Exchange Modern Message Delivery Health test.
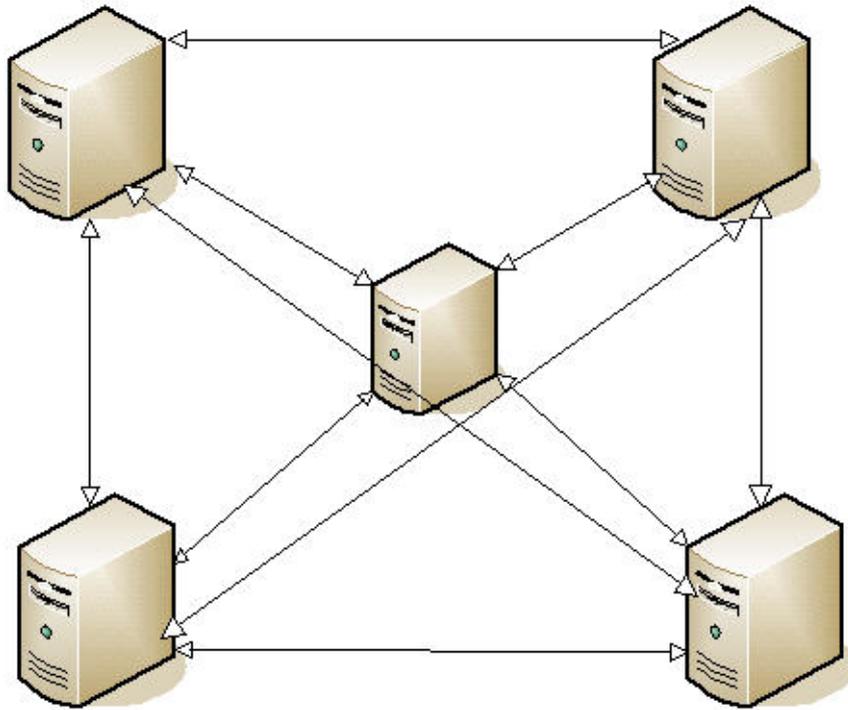
Figure 1. A test message is sent from each server to every other server.

You must manually create test mailboxes and match the name to the mailbox mask specified in the test configuration. For more information, see Creating test mailboxes for Exchange on page 80.

Recommendations for Performance Optimization

For large organizations, select a subset of the servers to reduce the amount of traffic generated. For example, select one server per geographical region. You can also decrease the monitoring frequency.

For Exchange 2007 servers, create a test mailbox that matches the mailbox mask in at least one store on each server in the organization. However, it is recommended that you create a test mailbox in each store on each server.

For Exchange 2010 servers, create a test mailbox that matches the mailbox mask in at least one mounted mailbox database copy on each server in the organization. However, it is recommended that the test mailbox be created in each mailbox database on each server. When the test runs, it looks for a test mailbox on each server. The test mailbox is in a mailbox database. If there are multiple test mailbox boxes on each server, the test uses the first one it finds. By default, the test mailbox creation scripts create one test mailbox per mailbox database.

While the test is executing, storage groups and stores are enumerated in alphabetical order. If the test takes a long time to complete, you can create a test mailbox in the first storage group in the first store (in alphabetical order) on every server to speed up the query.

For example, you have a server called AMER-MBX-01 with the following stores:

- First-Mailbox-Store (in storage group First-Storage-Group)

- Second-Mailbox-Store (in storage group First-Storage-Group)

- Third-Mailbox-Store (in storage group Second-Storage-Group)

If the mailbox mask specified in the test is the default mask
(SOM_<ServerName>_<StorageGroupName>_<StoreName>, then the test looks for the following mailboxes for
AMER-MBX-01 until it finds one that is accessible:

- SOM_AMER-MBX-01_First-Storage-Group_First-Mailbox-Store

- SOM_AMER-MBX-01_First-Storage-Group_Second-Mailbox-Store

- SOM_AMER-MBX-01_Second-Storage-Group_Third-Mailbox-Store

For example, you have a server called AMER-MBX-01 containing Database1 and Database2. If the mailbox mask
specified in the test is the default mask (SOM_<ServerName>_<DatabaseName>, then the test looks for the
following mailboxes for AMER-MBX-01 until it finds one that is accessible:

- SOM_AMER-MBX-01_Database1

- SOM_AMER-MBX-01_Database2

    <DatabaseName> token is optional.

All test messages sent are automatically deleted from the internal test mailboxes. But other mail, such as NDR
messages, is not automatically deleted. You must manually clean out your test mailboxes periodically.

To enable this test to collect tracking information

- From the All Exchange Servers tab, select the **Collect message tracking information** check box.

    The tracking information is located in the Delivery details counter.

Table 3. Exchange Internal Server Delivery Health Test counters

Category	Counter
Internal Server Delivery	• Delivery time in seconds • Delivery status (within timeout) • Delivery details

Creating test mailboxes for Exchange

Creating and configuring health tests

Exchange Internal Server Delivery Health Test Prerequisites

The following tables show the test target servers, required configuration to run the test, and the permissions
required by the test credentials.

Table 4. Internal server delivery health test targets

Exchange Server Version	Target Type
Exchange 2007/2010	Mailbox role

The Exchange server must be configured as follows:

Table 5. Exchange internal server delivery health test configuration.

Exchange Server Version	Required Configuration
Exchange 2007/2010	• Create test mailboxes on each server that match the mailbox mask specified in the test configuration. For more information, see Creating test mailboxes for Exchange on page 80. • Enable message tracking logs on each Exchange server through which the test message passes.

The test credentials must have the following permissions:

Table 6. Exchange internal server delivery health test credential required permissions.

Exchange version	Permissions required for test credentials
Exchange 2007/2010	• Full access permissions to each test mailbox to access the mailbox inbox to send and receive test messages • Member of Local Administrators group on each Exchange server through which the message passes
Exchange 2007	• Must be a member of View-Only Exchange Administrators group
Exchange 2010	• Must be a member of View-Only Organization Management group

Exchange Internal Mailbox Delivery Health Test

For Exchange 2007 to Exchange 2013, you can use the Exchange Internal Mailbox Delivery Health Test to monitor the sending and receipt of messages between mailboxes in an Exchange organization. This test supports DAGs.

For Exchange 2010 and later, it is recommended that you run the Exchange Modern Message Delivery Health Test instead, especially in scenarios in which the CAS server is behind a load balancer.

Table 7. Exchange Internal Mailbox Delivery Health Test counters

Category	Counter
Message Delivery	• Delivery time in seconds • Delivery status (within timeout) • Delivery details

Creating test mailboxes for Exchange

Creating and configuring health tests

Exchange Internal Mailbox Delivery Health Test Prerequisites

The following tables show the test target servers, required configuration to run the test, and the permissions required by the test credentials.

You can run the test against the following target servers.

Table 8. Exchange internal mailbox delivery health test targets.

Exchange Server Version	Target Type
Exchange 2007/2010/2013	Mailbox role

> **i** | **TIP:** For Exchange 2010 and later, it is recommended that you run the Exchange Modern Message Delivery Health Test instead.

The Exchange server must be configured as follows:

Table 9. Exchange internal mailbox delivery health test configuration.

Exchange Server Version	Required Configuration
All	• Create user mailboxes or dedicated test mailboxes for source and target mailbox pairs. For more information, see Creating test mailboxes for Exchange on page 80.

The test credentials must have the following permissions.

Table 10. Internal mailbox delivery health test permissions needed by test credentials.

Exchange Version	In an organization without Exchange 2013	In an organization with Exchange 2013
All Exchange versions	• Member of the Local Administrators group on each Exchange server through which the message passes • Full access permissions to each test mailbox to access the mailbox inbox to send and receive test messages	• Member of the Local Administrators group on each Exchange server through which the message passes • Full access permissions to each test mailbox to access the mailbox inbox to send and receive test messages
Additional for Exchange 2007	• Member of the Exchange View-Only Administrators group	• Member of the Exchange View-Only Administrators group • Send on Behalf permission to each test mailbox to allow to send email on behalf of the mailbox
Additional for Exchange 2010	• Member of View-Only Organization Management group • Member of Public Folder Management group	• Member of View-Only Organization Management group • Member of Public Folder Management group • Send on Behalf permission to each test mailbox to allow to send email on behalf of the mailbox
Additional for Exchange 2013	Not applicable	• Member of View-Only Organization Management group • Member of Public Folder Management group • All extended rights permission to each test mailbox in Active Directory.

Exchange External Message Delivery Health Test

For Exchange 2007 to Exchange 2013, you can use the Exchange External Message Delivery Health test to monitor the health of message delivery to and from an external target.

For Exchange 2010 and later, it is recommended that you run the Exchange Modern Message Delivery Health Test instead, especially in scenarios in which the CAS server is behind a load balancer.

This test tracks the time it takes a test email to leave your organization and the time it takes the message to return to the original server.

For this test, you must enter the names of:

• Source mailbox to send a message to an SMTP address and receive replies from that address

• Destination email address to indicate where test messages are sent

For more information about test prerequisites, see *Unified Communications Diagnostics Deployment Guide*.

About the test

This test targets your entire organization, not individual servers. You must create a test mailbox to run this test.

To monitor round-trip messages, the external mailbox must be configured to automatically bounce the message back to the original mailbox. You would enable the Round-Trip Delivery counter in the test.

All test messages sent are automatically deleted from the internal test mailbox. But any other mail, like NDR messages, are not automatically deleted. You may need to periodically clean out your test mailboxes.

By default, the Organization Exit counters are disabled because they are not fully supported when the source mailbox is hosted on Exchange 2013.The Round-trip Delivery counters are enabled because the external email account needs to be configured to automatically bounce the test message back to the originating mailbox.

Table 11. External message delivery health test counters.

Category	Counter
Organization Exit	• Organization exit time in seconds
	• Organization exit status (within timeout)
	• Organization exit details
Round-trip Delivery	• Round trip delivery time in seconds
	• Round trip delivery status (within timeout)
	• Round trip delivery details

Creating test mailboxes for Exchange

Creating and configuring health tests

External Message Delivery Health Test Prerequisites

The following tables show the test target servers, required configuration to run the test, and the permissions required by the test credentials.

You can run the test against the following target servers.

Table 12. Exchange external message delivery health test targets.

Exchange Server Version	Target Type
Exchange 2007/2010/2013	Exchange organization

> **i** | **TIP:** For Exchange 2010 and later, it is recommended that you run the Exchange Modern Message Delivery Health Test instead.

The Exchange server must be configured as follows:

Table 13. Exchange external message delivery health test configuration.

Exchange Server Version	Required Configuration
All	• Create a source test mailbox. For more information, see Creating test mailboxes for Exchange on page 80. • Create an external test mailbox. For more information, see Creating a test mailbox for External Message Delivery Health Test on page 83. • For Organization Exit counters, enable message tracking logs on each Exchange server through which the test message passes.

The test credentials must have the following permissions.

Table 14. Exchange external message delivery health test required permissions for test credentials.

Exchange Version	In an organization without Exchange 2013	In an organization with Exchange 2013
All Exchange versions	• Member of the Local Administrators group on each Exchange server through which the message passes • Full access permissions to each test mailbox to access the mailbox inbox to send and receive test messages	• Member of the Local Administrators group on each Exchange server through which the message passes • Full access permissions to each test mailbox to access the mailbox inbox to send and receive test messages
Additional for Exchange 2007	• Member of the Exchange View-Only Administrators group	• Member of the Exchange View-Only Administrators group • Send on Behalf permission to each test mailbox to allow to send email on behalf of the mailbox
Additional for Exchange 2010	• Member of View-Only Organization Management group • Member of Public Folder Management group	• Member of View-Only Organization Management group • Member of Public Folder Management group • Send on Behalf permission to each test mailbox to allow to send email on behalf of the mailbox
Additional for Exchange 2013	Not applicable	• Member of View-Only Organization Management group • Member of Public Folder Management group • All extended rights permission to each test mailbox in Active Directory.

Exchange Modern Message Delivery Health Test

The Exchange Modern Message Delivery Health test monitors overall message delivery health for Exchange 2010, Exchange 2013, and Exchange 2016. The test provides information about both internal and external message delivery.

Depending on how you configure the test, it sends a test email to a target email address or tracks the time it takes an email to leave the Exchange organization. By default, the organization exit counters are enabled and the round trip counters are disabled.

The Modern Exchange Message Delivery Health test uses Exchange Web Services (EWS) for internal and external message delivery tests, and also uses the Exchange message tracking logs for internal and external message delivery tests. The prerequisites for the modern message delivery health test are as follows.

To create a modern message delivery health test

1   Right-click the organization node and select **Detect | Exchange Modern Message Delivery Health Test**.

2   On the General Test page, specify a Test name to identify the test and click **Next**.

3   On the Test Settings page, review the test schedule, credentials, and notification settings. Make any required changes and click **Next**.

4   On the Source and Destination page, click **Add**.

5   Enter the source mailbox display name and the destination email address for the test messages and specify if the message delivery is internal or external.

6   Click **OK** and click **Next**.

    If you do not want to use the Exchange autodiscover service to connect to the test mailboxes, you can specify the EWS URLs to be used. This setting is optional.

7   On the EWS URL Settings (Optional) page, you can select the **Use specified EWS URL(s) to find Exchange mailboxes** check box and click **Add**.

8   Enter the URL and click **OK**.

9   Repeat steps 8 and 9 until you have added all the URLs that you want and click **Next**.

    Internal Delivery Settings

    a   If you are creating a test for internal message delivery, specify the time the test should wait for delivery in the **Timeout (in minutes)** box.

    b   Review the metrics you want to monitor for the selected target.

    c   Review the Condition, Warning Threshold, Error Threshold, and Alarms to Skip Before values and click **Next**.

    External Delivery Settings

    a   If you are creating a test for external message delivery, specify the time the test should wait for delivery in the **Timeout (in minutes)** box.

    b   Review the metrics you want to monitor for the selected target.

    c   Review the Condition, Warning Threshold, Error Threshold, and Alarms to Skip Before values and click **Next**.

10 Review the test setting on the Summary page and click **Finish**.

Exchange modern message delivery health test counters

The Exchange modern internal message delivery health test contains the following counters:

Table 15. Exchange modern Internal message delivery health test counters

Category	Counter
Internal Message Delivery	• Delivery time in seconds
	• Delivery status (within timeout)
	• Delivery details

The Exchange modern external message delivery health test contains the following counters:

Table 16. Exchange modern external message delivery health test counters.

Category	Counter
Organization Exit	• Organization exit time in seconds • Organization exit status (within timeout) • Organization exit details
Round-trip Delivery	• Round trip delivery time in seconds • Round trip delivery status (within timeout) • Round trip delivery details

Creating test mailboxes for Exchange

Creating and configuring health tests

Exchange modern message delivery health test prerequisites

The following tables show the test target servers, required configuration to run the test, and the permissions required by the test credentials.

Table 17. Exchange modern message delivery health test targets

Exchange Server Version	Target Type
Exchange 2010/2013/2016	Exchange organization

Table 18. Exchange modern message delivery health test general (internal and external message delivery) configuration.

Exchange Server Version	Required Configuration
Exchange 2010/2013/2016	• Create an Exchange 2010 or later mailbox for the test credentials. You must enable MAPI for the mailbox.

For the internal message delivery test, the Exchange servers must be configured as follows:

Table 19. Exchange modern internal message delivery health test configuration.

Exchange Server Version	Required Configuration
Exchange 2010/2013/2016	• Create user mailboxes or dedicated test mailboxes for source and target mailbox pairs. For more information, see Creating test mailboxes for Exchange on page 80.

For the external message delivery test, the Exchange servers must be configured as follows:

Table 20. Exchange modern external message delivery health test configuration.

Exchange Server Version	Required Configuration
Exchange 2010/2013/2016	• Create a source test mailbox. For more information, see Creating test mailboxes for Exchange on page 80. • Create an external test mailbox. For more information, see Creating a test mailbox for External Message Delivery Health Test on page 83. • For Organization Exit counters, enable the message tracking logs on each Exchange server through which the test message passes.

The test credentials must have the following permissions.

Table 21. Modern message delivery health test permissions needed by test credentials.

Exchange Versions	Permissions required
Exchange 2010/2013/2016	• Member of View-Only Organization Management group • Member of the Local Administrators group on each Exchange server • Credentials used to access the test mailboxes require Exchange impersonation access. For more information, see Configuring Exchange impersonation for the Modern Message Delivery health test on page 86.

Exchange Storage Health Test

The Exchange Storage Health test monitors the overall function of storage subsystems. This test allows you to ensure the following:

- All of your stores or databases are mounted or healthy
- There is sufficient disk space on your Exchange system drive
- There is sufficient disk space for your transaction logs
- There is sufficient disk space for your mailbox database and public folder

WMI is required to support retrieving accurate disk space information when using mount points. If you do not use mount points, you can disable the requirement for WMI. For information on enabling WMI, see Volumes - Allowing API fallback if WMI fails on page 39.

Stores in recovery storage groups have the following special behavior:

- For Exchange 2010/2013/2016 servers, all the recovery database copies are not monitored.
- For Exchange 2007 servers, the store status counter is reported, but the error or warning condition is ignored. For example, if the counter is configured to set an alarm when the store is offline, no alarm or notification is generated, and the result for the counter is reported as "Informational".

Storage health test counters for Exchange 2007

The Exchange Storage Health Test contains the following counters for Exchange 2007.

Table 22. Exchange 2007 storage health test counters.

Category	Counter
Exchange System	• Application Path • Available space in MB • % Free space
Storage Groups	• Transaction log file path • Transaction log file base name • Transaction log files total size (MB) • Available space (MB) • % Free space • Age of oldest transaction log file in hours

Table 22. Exchange 2007 storage health test counters.

Category	Counter
Stores	• Store Type • Store Status • Database file path • Database file size in MB • Available space in MB • % Free space • Hours since last full backup • Hours since last incremental backup • Hours since last differential backup • Hours since last copy backup

Storage health test counters for Exchange 2010/2013/2016

The Exchange Storage Health test contains the following counters for Exchange 2010/2013/2016:

Table 23. Exchange 2010/2013/2016 storage health test counters.

Category	Counter
Exchange System	• Application path • Available space in MB • % Free space
Active Mailbox Database Copy	• Database status • Database file path • Database file size in MB • Database available space in MB • Database % free space • Database white space in MB • Database % white space • Transaction log file path • Transaction log file base name • Transaction log files total size (MB) • Transaction log available space (MB) • Transaction log % free space • Age of oldest transaction log file in hours • Hours since last full backup • Hours since last incremental backup • Hours since last differential backup • Hours since last copy backup • Activation preference • Active on preferred servers

Table 23. Exchange 2010/2013/2016 storage health test counters.

Category	Counter
Passive Mailbox Database Copy	• Mounted on server • Database status • Database file path • Database file size in MB • Database available space in MB • Database % free space • Database white space in MB • Database % white space • Transaction log file path • Transaction log file base name • Transaction log files total size in MB • Transaction log available space in MB • Transaction log % free space • Age of oldest transaction log file in hours • Hours since last full backup • Hours since last incremental backup • Hours since last differential backup • Hours since last copy backup
Public Folder **NOTE:** The public folder health test counters are available only for Exchange 2010.	• Status • Database file path • Database file size • Database available space in MB • Database % Free space • Transaction log file path • Transaction log file base name • Transaction log files total size in MB • Transaction log available space in MB • Transaction log % free space • Age of oldest transaction log file in hours • Hours since last full backup • Hours since last incremental backup • Hours since last differential backup • Hours since last copy backup

Creating test mailboxes for Exchange

Creating and configuring health tests

Exchange storage health test prerequisites

The following tables show the test target servers, required configuration to run the test, and the permissions required by the test credentials.

Table 24. Exchange storage health test targets.

Exchange Server Version	Target Type
Exchange 2007/2010/2013/2016	Mailbox role

Table 25. Exchange storage health test required software.

Exchange Server Version	Software Required on the UC Diagnostics computer
Exchange 2010/2013/2016	PowerShell 2.0 or later
Exchange 2007	Exchange Management Console (EMC) Service Pack 1 Rollup 1 or later

Table 26. Exchange storage health test configuration.

Exchange Server Version	Required Configuration
All	Enable WMI
	NOTE: WMI is required to support retrieving accurate disk space information when using mount points. If you do not use mount points, you can disable the requirement for WMI by clicking the Data Collection options link in the Storage Health test wizard.

Table 27. Exchange storage health test credential required permissions.

Exchange Version	Permissions required for test credentials
All	• Member of Local Administrators group to retrieve disk space
Exchange 2007	• Member of View-Only Exchange Administrators group to collect store status
Exchange 2010, 2013 and 2016	• Member of View-Only Organization Management group to collect store status

Exchange Queue Health Test

Use the Exchange Queue Health test to monitor the health and performance of email and message queues.

This test allows you to ensure the following:

- Messages are not backing up (that is, messages are being delivered in a timely manner)
- Large number of queues are not being created (for example in virus outbreaks)

The Exchange Queue Health test contains the following counters for Exchange 2007 and later versions:

Table 28. Exchange 2007/2010/2013/2016 queue health test counters

Category	Counter
For all queues combined	• Total Queue Count
	• Total Queue Length
	• Total Queue Size in KB
For individual queues	• Queue Length
	• Queue Size in KB
	• Age of oldest message in hours
	• Queue Status
	• Last error (if available)
	• Last retry time (if available)
	• Next retry time (if available)

Creating test mailboxes for Exchange

Creating and configuring health tests

Exchange Queue health test prerequisites

The following tables show the test target servers, required configuration to run the test, and the permissions required by the test credentials.

Table 29. Exchange queue health test targets.

Exchange server version	Target type
Exchange 2013/2016	Mailbox role
Exchange 2007/2010	Hub role

Table 30. Exchange queue health test required software.

Exchange Server Version	Software Required on UC Diagnostics computer
Exchange 2010/2013/2016	PowerShell 2.0 or later
Exchange 2007	Exchange Management Console (EMC) Service Pack 1 Rollup 1 or later

Table 31. Exchange queue health test configuration.

Exchange Server Version	Required Configuration
Exchange2007/ 2010/2013/2016	N/A

Table 32. Exchange queue health test credential required permissions.

Exchange version	Permissions Required for Test Credentials
All	• Member of Local Administrators group
Exchange 2007	• Member of View-Only Exchange Administrators group
Exchange 2010/2013/2016	• Member of View-Only Organization Management group **NOTE:** To run the Exchange Queue Health Test against Exchange 2010 SP3 RU 6, you must add the test credentials to the Organization Management group.

Internal Outlook Web Access (OWA) Availability Health Test

The Exchange Internal Outlook Web Access Availability Health test verifies a user can log on to a mailbox through Outlook Web Access (OWA) from inside your organization.

This test does not run on Exchange 2013 or later because the Microsoft Exchange Management Shell does not support OWA Connectivity testing for Exchange 2013 or later. For Exchange 2013 or Exchange 2016, you can use the Exchange System Health test to monitor OWA health.

The Exchange Internal Outlook Web Access Availability Health test monitors all web sites configured within a CAS server. You cannot monitor one web site at a time. This test uses internal server URL names only. It does not test external availability or OWA using your public URL

This test allows you to ensure the following:

- Mailbox is accessible

- Mailbox logon latency is within expected threshold

The Exchange Internal Outlook Web Access Availability Health test contains the following counters for all Exchange Servers:

Table 33. Internal OWA availability health test counters.

Category	Counter
Mailbox logon	• Mailbox logon time in seconds • Mailbox logon status within timeout • Mailbox logon details

Exchange 2007/2010 considerations

For Exchange 2010 Client Access (CAS) servers, UC Diagnostics attempts to log on to Exchange 2010 mailbox in the same Active Directory site, if one exists.

For Exchange 2007 CAS servers, UC Diagnostics attempts to log on to an Exchange 2007 mailbox if there are Exchange 2007 mailbox servers in the same site. If logon fails or no mailbox servers are found, UC Diagnostics logs on to any Exchange 2007 mailbox server in the organization.

The Internal OWA Health Test for Exchange 2007 requires at least one Exchange 2007 mailbox server within your organization. The Internal OWA Health Test for Exchange 2010 requires at least one Exchange 2010 mailbox server in the same site.

The Internal OWA Health Test for Exchange 2007/2010 does not use specified alternate credentials. Before running this test, use the Exchange PowerShell script called new-TestCasConnectivityUser.ps1 (located in Scripts folder in the Exchange Server installation directory) to create test mailboxes. This test automatically manages the mailboxes credentials while it logs onto the mailboxes. For more information, see Creating a test mailbox for the Internal Mailbox Delivery Health Test on page 84.

For Exchange 2007/2010, you must specify a logon method and timeout to signify the maximum amount to time to wait between logon attempts.

Creating test mailboxes for Exchange

Creating and configuring health tests

Internal OWA availability health test prerequisites

The following tables show the test target servers, required configuration to run the test, and the permissions required by the test credentials.

Table 34. Internal OWA availability health test targets.

Exchange Server Version	Target Type
Exchange 2007/2010	Client Access role

Table 35. Internal OWA availability health test software.

Exchange Server Version	Software Required on UC Diagnostics computer
Exchange 2010	PowerShell 2.0 or later
Exchange 2007	Exchange Management Console (EMC) Service Pack 1 Rollup 1 or later

Table 36. Internal OWA availability health test configuration.

Exchange Server Version	Required Configuration
Exchange 2007/2010	Create at least one test mailbox. For more information, see Creating a test mailbox for the Internal Mailbox Delivery Health Test on page 84.

Table 37. Internal OWA availability health test credential required permissions.

Exchange Server Version	Permissions Required for Test Credentials
All	• Receive As permission for the test mailbox to log on to the mailbox

External Outlook Web Access (OWA) Availability Health Test

The External OWA Availability Health test monitors the availability of OWA functionality in your organization through an external URL. This test verifies that the users associated with the alternate credentials can logon to their mailboxes through an external OWA URL. This test uses an external or internal URL. If an external URL is specified, ensure that the DNS server can resolve this URL.

This test is applicable only to organizations with at least one Exchange 2007/ 2010 server. This test does not run on Exchange 2013 or later because the Microsoft Exchange Management Shell does not support OWA Connectivity testing for Exchange 2013 or later. For Exchange 2013 or Exchange 2016, you can use the Exchange System Health test to monitor OWA health.

This test uses mailboxes associated with alternate credentials. You must explicitly choose the alternate credentials on the Test Settings page when you create this test. You cannot configure the test if you have selected the **Use Diagnostic Services Credentials** option.

- For an Exchange 2010 mailbox, a PowerShell 2.0 cmdlet is run on each Exchange 2010 CAS server in the organization until the mailbox logon attempt is successful.

- For an Exchange 2007 mailbox, logons to the mailbox are attempted using a local Exchange 2007 Management Shell cmdlet.

If you would like to test External OWA functionality using both types of mailboxes, you must configure two tests - one using credentials of the user who has 2007 mailbox, and the second using credentials of the user with 2010 mailbox.

This test allows you to ensure the following:

- Mailbox is accessible

- Mailbox logon latency is within expected threshold.

Creating test mailboxes for Exchange

Creating and configuring health tests

External OWA availability health test prerequisites

The following tables show the test target servers, required configuration to run the test, and the permissions required by the test credentials.

Table 38. External OWA availability health test targets.

Exchange Server Version	Target Type
All	Exchange organization

Table 39. External OWA availability health test software.

Exchange Mailbox Version	Software required on UC Diagnostics computer
Exchange 2010	PowerShell 2.0 or later
Exchange 2007	Exchange 2007 Management Console (EMC) Service Pack 1 Rollup 1 or later

Table 40. External OWA availability health test configuration.

Exchange Mailbox Version	Required configuration
Exchange 2010	Account specified in the alternative credentials for the test must have mailbox on the Exchange 2010 server. The alternate credentials must have Exchange View-Only Organization Management privileges.
Exchange 2007	Account specified in the alternative credentials for the test must have mailbox on the Exchange 2007 server. The alternate credentials must have Exchange View-Only Administrator privileges.

Table 41. External OWA availability health test credential required permissions.

Exchange version	Permissions required for test credentials
Exchange 2007/2010	• Account specified in alternate credentials must have an Exchange 2007/2010 mailbox, and sufficient rights to browse the Exchange container in Active Directory.
Exchange 2007	• Diagnostic services account must have sufficient rights to execute Exchange 2007 Management Shell Service Pack 1.0 cmdlets on the server where UC Diagnostics is installed.
Exchange 2010	• Diagnostic services account must have sufficient rights to execute Exchange cmdlets using PowerShell 2.0 on the Exchange 2010 CAS server in the Exchange organization.

Exchange Replication Health Test

The Exchange Replication Health test monitors the health of transaction log replication on your Exchange 2007, Exchange 2010, Exchange 2013, and Exchange 2016 mailbox servers. This test detects whether replication is configured and what type of replication is configured.

For Exchange 2010 and later, there is also information provided about lagged database copies if you have configured the Exchange lagged database copy function.

The Exchange Replication Health test contains the following counters for Exchange 2007:

Table 42. Exchange 2007 replication health test counters.

Category	Counter
Cluster Continuous Replication	• Copy status • Copy queue length • Replay queue length • Hours since last log inspection • Target transaction log path
Local Continuous Replication	• Copy status • Copy queue length • Replay queue length • Hours since last log inspection • Target transaction log path
Standby Continuous Replication	• Copy status • Copy queue length • Replay queue length • Hours since last log inspection • Target transaction log path

The Exchange Replication Health test contains the following counters for Exchange 2010:

Table 43. Exchange 2010 replication health test counters.

Category	Counter
Passive Mailbox Database Copy	• Master • Mounted on server • Copy status • Copy queue length • Replay queue length • Hours since last log inspection • Activation preference • Active on preferred servers • Replay lag status • Configured lag time

The Exchange Replication Health test contains the following counters for Exchange 2013 and Exchange 2016:

Table 44. Exchange 2013 and Exchange 2016 replication health test counters.

Category	Counter
Passive Mailbox Database Copy	• Master
	• Mounted on server
	• Copy status
	• Copy queue length
	• Replay queue length
	• Hours since last log inspection
	• Activation preference
	• Active on preferred servers
	• Replay lag status
	• Configured lag time
	• Actual lag time
	• Lag percentage
	• Lag play down reason

Transaction log replication is handled by Database Availability Groups (DAGs) for Exchange 2010, Exchange 2013, and Exchange 2016. For more information, see Viewing Database Availability Groups (DAG) on page 23.

Creating test mailboxes for Exchange

Creating and configuring health tests

Exchange replication health test prerequisites

The following tables show the test target servers, required software, and the permissions needed by the test credentials.

Table 45. Exchange replication health test targets.

Exchange Server Version	Target Type
Exchange 2007/2010/2013/2016	Mailbox role

Table 46. Exchange replication health test software.

Exchange Server Version	Software Required on the UC Diagnostics computer
Exchange 2010/2013/2016	PowerShell 2.0 or later
Exchange 2007	Exchange Management Console (EMC) Service Pack 1 Rollup 1 or later

Table 47. Exchange replication health test credential required permissions.

Exchange version	Permissions required for test credentials
Exchange 2007	• Member of View-only Exchange Administrators group to enumerate storage groups and replication configurations in Active Directory
Exchange 2010, 2013, and 2016	• Member of View-only Organization Management group to enumerate storage groups and replication configurations in Active Directory using PowerShell

Exchange System Health Test

The Exchange System Health test monitors the health state for different groups of monitors, called health sets. Monitors that are similar or are related to a component's architecture are grouped to form a health set. Health sets provide the health information for applications and services such as Outlook Web App, Exchange ActiveSync, the Information Store service, content indexing, and transport services on your Exchange 2013 Client Access Servers (CAS) and mailbox servers and on your Exchange 2016 mailbox servers.

If all a health set's monitors are healthy, the health set is in a healthy state. If any monitor is not in a healthy state, the health set state is determined by its least healthy monitor.

This test is available only for Exchange 2013 and later.

The health sets are organized into four main health groups:

- Customer Touch Points
- Service Components
- Server Components
- Dependency Availability

Customer Touch Points health group

The Customer Touch Points health group is comprised of monitors for components that affect real-time user interactions such as protocols or the Information Store. The test shows the condition of healthy or unhealthy for each of the following health set counters:

Table 48. Counters for the Customer Touch Points health group.

Server roles	Health set counter
Exchange 2013 CAS Exchange 2016 Mailbox	• Autodiscover • Compliance • EWS (Exchange Web Services) • IMAP (IMAP4 proxy infrastructure) • Outlook • OWA (Outlook Web App) • POP (POP3 service and POP3 client connectivity) • UM (Unified Messaging)
Exchange 2013 CAS Exchange 2013 and 2016 Mailbox	• ActiveSync • ECP (Exchange Administration Center (EAC) and of the Outlook Web App user setting service) • RPS (Remote PowerShell service)
Exchange 2013 and 2016 Mailbox	• Public Folders • Site Mailbox

Service Components health group

The Service Components health group is comprised of monitors for components without direct, real-time user interactions such as the Microsoft Exchange Mailbox Replication service or the offline address book generation process (OABGen). The test shows the condition of healthy or unhealthy for each of the following health set counters:

Table 49. Counters for the Service Components health group.

Server roles	Health set counter
Exchange 2013 CAS Exchange 2016 Mailbox	• ActiveSync.Proxy • Autodiscover.Proxy • ClientAccess.Proxy • ECP.Proxy (Exchange Administration Center proxy infrastructure) • EWS.Proxy (Exchange Web Services proxy) • FfoUMC (Forefront administration website) • FfoWebService (Forefront web service) • IMAP.Proxy • MailFlow • OAB.Proxy • Outlook.Proxy • OWA.Proxy • POP.Proxy • Transport
Exchange 2013 CAS Exchange 2013 and 2016 Mailbox	• Data Protection (redundancy of databases in a database availability group (DAG)) • EDS (Exchange Diagnostic Service thresholds) • FIPS (Federal Information Processing Standards) • FrontendTransport • HubTransport • Monitoring • PowershellDataProvider (Exchange Management Shell) • RemoteMonitoring • RPS.Proxy (Remote PowerShell service) • Search • SMTP • UM.CallRouter • UserThrottling

Table 49. Counters for the Service Components health group.

Server roles	Health set counter
Exchange 2013 and 2016 Mailbox	• ActiveSync.Protocol • Antimalware • Antispam • Autodiscover.Protocol • Classification (Data Loss Prevention (DLP) feature) • Ediscovery.Procotol • Event Assistants • EWS.Protocol • FfoQuarantine (Forefront message quarantine) • FfoTransport (Forefront transport components) • FreeBusy • IMAP.Protocol • MailboxMigration • MailboxTransport • MessageTracing • MRS (Mailbox Replication Service) • MSExchangeCertificateDeployment • OAB (Offline Address Book) • Outlook.Procotol (MAPI protocol) • OWA.Protocol (Outlook Web App protocol) • POP.Protocol (POP3 protocol) • PushNotifications.Protocol • RPS.Protocol (Remote PowerShell protocol) • Store • UM.Protocol (Unified Messaging protocol)

Server Components health group

The Server Components health group is comprised of monitors for the server physical resources such as disk space, memory, and networking. The test shows the condition of healthy or unhealthy for each of the following health set counters:

Table 50. Counters for the Server Components health group.

Server Roles	Counter
Exchange 2013 CAS Exchange 2013 and 2016 Mailbox	• DiskSpace • Memory
Exchange 2013 and 2016 Mailbox	• Clustering (Windows cluster services) • MailboxSpace

Dependency Availability health group

The Dependency Availability health group monitors the server's ability to access necessary dependencies, such as Active Directory, DNS, and instant messaging. The test shows the condition of healthy or unhealthy for each of the following health set counters:

Table 51. Counters for the Dependency Availability health group.

Server Roles	Counter
Exchange 2013 CAS Exchange 2013 and 2016 Mailbox	• AD (Active Directory) • Network (in Domain Name System (DNS))
Exchange 2013 and 2016 Mailbox	• OWA.Protocol.Dep (instant messaging services in Outlook Web App between Exchange and Skype for Business/Lync)

Exchange system health test prerequisites

The following tables show the test target servers, required software, and the permissions required by the test credentials.

Table 52. Exchange system health test targets.

Exchange Server Version	Target Type
Exchange 2013	Client Access Server (CAS) role Mailbox role
Exchange 2016	Mailbox role

Table 53. Exchange system health test software.

Exchange Server Version	Software Required on the UC Diagnostics computer
Exchange 2013/2016	PowerShell 2.0 or later

Table 54. Exchange system health test credential required permissions.

Exchange Server Version	Permissions Required for Test Credentials
All	Be a member of the following groups: • Member of View-only Organization Management

Creating and configuring health tests

Active Directory Account Lockout Health Test

The Active Directory Account Lockout Health test provides information about how many and which Active Directory accounts are currently locked out. The test shows accounts that are locked out due to invalid passwords being submitted and accounts that are locked because the password has expired. The test detects the domain accounts that are currently locked out and provides information about the lockout event.

You run the test against a domain to which an Exchange organization or a Lync/Skype for Business environment belongs. You cannot run the test against the individual servers.

> **ⓘ** | **NOTE:** Information about locked-out accounts is available only for the first 1000 accounts.

The Active Directory Account Lockout Health test contains the following counters:

Table 55. Active Directory Account Lockout health test counters.

Category	Counter
General	• Total accounts locked out
Lockout information	• User status
	• Last time bad password was submitted
	• Number of login attempts with bad password
	• Date and time account was locked out
	• Last time password was changed
	• Next expiry date for password

Active Directory account lockout health test prerequisites

The following tables show the test targets for the test and the permissions required by the test credentials.

Table 56. Active Directory Account Lockout Health test targets.

Platform Versions	Target Type
Exchange 2007/2010/2013/2016	Organization
Lync 2010/2013 and Skype for Business 2015	Environment

The test credentials must have read permission on User objects in Active Directory.

Table 57. Active Directory Account Lockout Health test credential required permissions.

Platform	Permissions Required for Test Credentials
Exchange	• Member of View-Only Exchange Administrators group or View-Only Organization Management group.
Lync/Skype for Business	• Member of CSHelpDesk, CSServerAdministrator, or CSViewOnlyAdministrator group

Exchange Online Connectivity Health Test

The Exchange Online Connectivity Health test allows you to determine network quality and identify issues that can affect network performance between your client computers and Exchange Online.

You can view the time (in milliseconds) a round trip takes from your computer to Exchange Online (Office 365). You can also view any warnings and errors for the different ports used to access Exchange Online services.

Table 58. Exchange Online Connectivity health test counters.

Category	Counter
Basic Network	• Network *Reachable/Unreachable* • Network Latency (ms) Shows network latency to Office 365 service. Good is < 50 ms. Warning is >50 ms. Error is >275 ms. • Packet Loss (%) Shows the percentage of packet loss to the Content Delivery Network (CDN) endpoint. Warning is 2%. Error is 5%. **NOTE:** If packet loss is 1% or greater, you should investigate.
Advanced Network (round-trip time) Warning: >50 ms Error: >275 ms **NOTE:** If one of the counters is in error, check your firewall or router settings to ensure the port is not blocked.	• HTTP - TCP Port 80 (ms) Affects ability to reach the Microsoft web site. • HTTPS - TCP Port 443 (ms) Affects whether Outlook and mobile devices can connect or synchronize. • IMAP - TCP Port 993 (ms) Affects ability to receive email. • POP - TCP Port 995 (ms) Affects ability to receive email. • SMTP - TCP Port 587 (ms) Affects ability to send email.

Table 59. Exchange Online connectivity health test targets.

Platform	Target Type
Office 365	Exchange Online

Table 60. Exchange Online connectivity health test required software.

Platform	Software Required on the UC Diagnostics computer
Office 365	• Windows PowerShell 5.0 or later • Microsoft Online Service Sign-in Assistant • Microsoft Azure Active Directory Module for Windows PowerShell • Microsoft Exchange Online PowerShell Module

Exchange Online Mailbox Logon Health Test

The Exchange Online Mailbox Logon Health test verifies mailbox accessibility by logging on to Exchange Online. The test uses the Office 365 credential that you specified for either a hybrid Exchange Online connection or for a native Office 365 connection. The credential must have an associated Exchange Online mailbox.

When the logon process succeeds, the test displays Logon Succeeded. Logon latency shows the time that elapsed during the logon process (in seconds).

If you are using OAuth 2.0 to connect to Office 365, you must provide Application ID, Tenant ID, and Client Secret that were assigned when the UC Diagnostics application was registered with the Microsoft Azure portal. For more information, see Registering UC Diagnostics with the Microsoft Azure portal on page 87.

Table 61. Exchange Online mailbox logon health test counters.

Threshold Name	Condition	Warning Threshold	Error Threshold
Logon status	Equal	N/A	Logon Failed
Logon latency in seconds	Informational		

Table 62. Exchange Online mailbox logon health test targets.

Platform	Target Type
Office 365	Exchange Online

Table 63. Exchange Online mailbox logon health test required software.

Platform	Software Required on the UC Diagnostics computer
Office 365	• Windows PowerShell 5.0 or later • Microsoft Online Service Sign-in Assistant • Microsoft Azure Active Directory Module for Windows PowerShell • Microsoft Exchange Online PowerShell Module

Table 64. Exchange Online mailbox logon health test credential required permissions.

Platform	Permissions Required for Test Credentials
Office 365	• Be a valid Office 365 credential that is assigned the Exchange Online service with an active mailbox

If you are using OAuth 2.0 authentication for the test, the required API permissions are:

Table 65. Exchange Online mailbox logon health test required API permissions.

Platform	Required API Permissions for OAuth 2.0 authentication
Office 365	• EWS.AccessAsUser.All • full_access_as_app

If the password of the Office 365 credential is changed, you must also change the credential password on either the native Office 365 or hybrid Exchange connection properties.

Exchange Online Message Delivery Health Test

The Exchange Online Message Delivery Health test monitors overall message delivery health for both hybrid and native Exchange Online, including test messages sent internally and externally.

- Internal message delivery can be between Exchange on-premise mailboxes and Exchange Online mailboxes, or between mailboxes within Exchange Online. For hybrid environments, you could set either the source or target mailbox to be on-premise or Exchange Online. For native environments, both mailboxes would be Exchange Online.

- External message delivery detects message delivery between Exchange Online and the internet. You must create an internal mailbox as source mailbox and an external mailbox as the destination mailbox. The source mailbox is an Exchange Online mailbox. The destination mailbox must be configured to send an auto-reply message.

The Exchange Online Message Delivery Health test uses Exchange Web Services (EWS) for internal and external message delivery tests.

If you are using OAuth 2.0 to connect to Office 365, you must provide Application ID, Tenant ID, and Client Secret that were assigned when the UC Diagnostics application was registered with the Microsoft Azure portal. For more information, see Registering UC Diagnostics with the Microsoft Azure portal on page 87.

The process to create an Exchange Online message delivery health test is as follows.

To create an Exchange Online message delivery health test

1 Right-click the organization node and select **Detect | Exchange Online Message Delivery Health Test**.

2 On the General Test Information page, specify a Test name to identify the test and click **Next**.

3 On the Test Settings page, review the test schedule, credentials, and notification settings. Make any required changes and click **Next**.

4 On the Source and Destination page, click **Add**.

5 Enter the source mailbox email address and the destination email address for the test messages and specify if the message delivery is internal or external.

> You must enter the primary SMTP address for the mailboxes.

6 Click **OK** and click **Next**.

> If you do not want to use the Exchange autodiscover service to connect to the test mailboxes, you can specify the EWS URLs to be used. This setting is optional.

7 On the EWS Authentication page, select either **Basic** or **OAuth 2.0** authentication.

> If you select OAuth 2.0, enter the Application ID, Tenant ID, and Client Secret that were assigned when the UC Diagnostics application was registered with the Microsoft Azure portal. For details, see Registering UC Diagnostics with the Microsoft Azure portal on page 87.

8 On the EWS URL Settings (Optional) page, you can select the **Use specified EWS URL(s) to find Exchange mailboxes** check box and click **Add**.

9 Enter the URL and click **OK**.

10 Repeat steps 8 and 9 until you have added all the URLs that you want and click **Next**.

Internal Delivery Settings

   a If you are creating a test for internal message delivery, specify the time the test should wait for delivery in the **Timeout (in minutes)** box.

   b Review the metrics you want to monitor for the selected target.

   c Review the Condition, Warning Threshold, Error Threshold, and Alarms to Skip Before values and click **Next**.

External Delivery Settings

   a If you are creating a test for external message delivery, specify the time the test should wait for delivery in the **Timeout (in minutes)** box.

   b Review the metrics you want to monitor for the selected target.

   c Review the Condition, Warning Threshold, Error Threshold, and Alarms to Skip Before values and click **Next**.

11 Review the test setting on the Summary page and click **Finish**.

Exchange Online message delivery health test counters

The Exchange Online internal message delivery health test contains the following counters:

Table 66. Exchange Online Internal message delivery health test counters

Category	Counter
Internal Message Delivery	• Delivery time in seconds
	Verifies whether the message can be sent and received successfully internally within the timeout
	• Delivery status (within timeout)

The Exchange Online external message delivery health test contains the following counters:

Table 67. Exchange Online external message delivery health test counters.

Category	Counter
Round-trip Delivery	• Round trip delivery time in seconds
	Verifies whether the message can be sent out and transferred back successfully within the timeout.
	• Round trip delivery status (within timeout)

Exchange Online message delivery health test prerequisites

The following tables show the test targets, required configuration to run the test, and the permissions required by the test credentials.

Table 68. Exchange Online message delivery health test targets

Platform	Target Type
Exchange Online hybrid	Exchange organization
Exchange Online native	Office 365 tenant

For the internal message delivery test, Exchange Online must be configured as follows:

Table 69. Exchange Online internal message delivery health test configuration.

Platform	Required Configuration
Exchange Online (native and hybrid)	• Create user mailboxes or dedicated test mailboxes for source and target mailbox pairs.

For the external message delivery test, Exchange Online must be configured as follows:

Table 70. Exchange Online external message delivery health test configuration.

Platform	Required Configuration
Exchange Online (native and hybrid)	• Create a source test mailbox.
	• Create an external test mailbox.

The following software is required.

Table 71. Exchange Online message delivery health test required software.

Platform	Software Required on the UC Diagnostics computer
Office 365	• Windows PowerShell 5.0 or later
	• Microsoft Online Service Sign-in Assistant
	• Microsoft Azure Active Directory Module for Windows PowerShell
	• Microsoft Exchange Online PowerShell Module

The test credentials must have the following permissions.

Table 72. Exchange Online message delivery health test permissions needed by test credentials.

Platform	Permissions required by test credential
Office 365	• Must be granted impersonation rights on the internal test mailboxes. The test credential is the credential used to connect to Office 365.

If you are using OAuth 2.0 authentication for the test, the required API permissions are:

Table 73. Exchange Online message delivery health test required API permissions.

Platform	Required API Permissions for OAuth 2.0 authentication
Office 365	• EWS.AccessAsUser.All
	• full_access_as_app

Office 365 Subscription Health Test

The Office 365 Subscription Health test provides an overview of your Office 365 licensing plans. Licensing plans define the Office 365 services that are available to users. The test shows license activity such as the number of licenses that are currently assigned to users (used) and how many licenses are due for renewal.

About the Office 365 subscription lifecycle

During the first 30 days after an Office 365 subscription ends, the Office 365 tenant account is in a period known as the expired state. During the expired period, users can still access data. After 30 days, the tenant account enters the disabled state for 90 days. During this period, users cannot access data. An Office 365 administrator can log in, backup data, or reactivate the subscription.

At the end of the disabled state, 120 days after the subscription has ended, the account enters the deprovisioning state. During the deprovisioning state, the data from user accounts and also email data and documents, is permanently deleted.

Table 74. Office 365 subscription health test counters.

Category	Counter
Total licenses	Total number of purchased licenses in the licensing plan.
Number of licenses used	Number of licenses that have been assigned to users in the specified licensing plan.
Number of licenses used (%)	Percentage of licenses that have been assigned to users in the specified licensing plan.
Number of licenses that must be renewed	Number of licenses in the licensing plan that have not been renewed and that will expire after the 30-day grace period.

Table 74. Office 365 subscription health test counters.

Category	Counter
Next lifecycle date	Next date on which a a subscription lifecycle event occurs. Lifecycle events can include states such as active, expired, disabled, or deprovisioned.
Next lifecycle date (days)	Date on which the next subscription lifecycle event will occur that is less than the specified number of days. You can set thresholds for warning and error notifications.

Table 75. Office 365 subscription health test targets.

Platform	Target Type
Office 365	All services

The following software is required.

Table 76. Office 365 subscription health test required software.

Platform	Software Required on the UC Diagnostics computer
Office 365	• Windows PowerShell 5.0 or later • Microsoft Online Service Sign-in Assistant • Microsoft Azure Active Directory Module for Windows PowerShell • Microsoft Exchange Online PowerShell Module

Table 77. Office 365 subscription health test credential required permissions.

Platform	Permissions Required for Test Credentials
Office 365	Valid Office 365 credential that was used to connect to Office 365.

If the password of the Office 365 credential is changed, you must change the password on Office 365 connection properties.

BlackBerry Server Health Test

The BlackBerry Server Health test allows you to monitor the basic health of all your BlackBerry servers. This test allows you to monitor the following types of information:

- Network availability
- Operating system disk space usage
- Any Performance Counter
- Any Windows service
- Any Event Log entry

The BlackBerry Server Health Test monitors BlackBerry 4 Enterprise, BlackBerry 4 Configuration, BlackBerry 5 Enterprise, and BlackBerry 5 Configuration servers.

All SQL-related performance counters for BlackBerry configuration database servers target the SQL Server Enterprise version of SQL (unnamed instance). Any BlackBerry configuration database servers that are installed on the named instance of the SQL server.will show a grey icon for the test results. The Error details will specify that the object is unavailable - the performance counter is either uninstalled or disabled.

To monitor BlackBerry configuration database servers installed on a named instance of SQL server, replace the SQL-related performance counters with corresponding performance counters for the named instance. For more information, see the Troubleshooting section of the *Unified Communications Diagnostics Deployment Guide.*

BlackBerry Server Health Test Prerequisites

The following tables show the test target servers, required configuration to run the test, and the permissions required by the test credentials.

Table 78. BlackBerry server health test targets.

BlackBerry server version	Server type
4.1.2 - 5.0.4 (including 5.0.4 MR4)	BlackBerry servers and BlackBerry Enterprise Database servers
	For SQL server prerequisites, see the *Unified Communications Diagnostics Deployment Guide*.

Table 79. BlackBerry server health test required configuration.

BlackBerry server version	Required Configuration
4.1.2 - 5.0.4 (including 5.0.4 MR4)	Enable WMI on each BlackBerry server
	NOTE: WMI is required to support retrieving accurate disk space information when using mount points. If you do not use mounts, you can disable the requirement for WMI by clicking the Data Collection options link in the Server Health Test wizard.

Table 80. BlackBerry server health test credential required permissions.

BlackBerry server version	Permissions Required for Test Credentials
4.1.2 - 5.0.4 (including 5.0.4 MR4)	• Member of Local Administrators group on each BlackBerry server to have:
	Read access to operating system drive to retrieve disk space
	Read access to Windows system directory to access Event Logs
	Read access to Service Control Manager
	Read access to Registry to access Performance Counters and Event Logs

BlackBerry Message Delivery Health Test

Use the BlackBerry Message Delivery Health test to monitor the overall message delivery health between your Exchange organization and your BlackBerry devices. The test tracks the time it takes for an email message to be sent and returned by sending a test message from a source mailbox to one or more target BlackBerry devices or to BlackBerry simulators.

If the source mailbox is hosted on an Exchange 2010 or later mailbox database, the Exchange organization must have at least one available Exchange 2010 or 2013 CAS server or one Exchange 2016 Mailbox server on the same site as the server that hosts the active mailbox database copy.

You manually create test mailboxes required for this test. You can reuse test mailboxes created for the Exchange health tests as the source mailbox.

Table 81. BlackBerry message delivery health test counters.

Category	Counter
Device delivery	• Organization exit time in seconds • Organization exit status (within timeout) • Device delivery time in seconds • Device delivery status (within timeout) • Delivery details
Round trip delivery	• Round trip delivery time in seconds • Round trip delivery status (within timeout) • Round trip delivery details

The BlackBerry message delivery health test is not performed on standby BlackBerry servers. Test results show a status of Skipped for these servers.

Creating test mailboxes for Exchange

Creating and configuring health tests

BlackBerry Message Delivery Health Test Prerequisites

The following tables show the test target servers, required configuration to run the test, and the permissions required by the test credentials.

Table 82. BlackBerry message delivery health test targets

Blackberry Server version	Target Type
4.1.2 - 5.0.4 (including 5.0.4 MR4)	BlackBerry server

Table 83. BlackBerry message delivery health test software perquisites.

BlackBerry server version	Software required on UC Diagnostics computer
4.1.2 - 5.0.4 (including 5.0.4 MR4)	• Exchange System Manager (ESM) Service Pack 1 or later MAPI & CDO (version 8.3.0.8353.000 or later).

Table 84. BlackBerry message delivery health test required configuration.

BlackBerry server version	Required configuration
4.1.2 - 5.0.4 (including 5.0.4 MR4)	• Create test mailboxes. • To track test messages, enable message tracking logs on each Exchange server through which the test message passes.

Table 85. BlackBerry message delivery health test credential required permissions.

BlackBerry server version	Permissions required for test credentials
4.1.2 - 5.0.4 (including 5.0.4 MR4)	• To track test messages, be a member of Local Administrators group on each Exchange server that the message passes through to have: Read access to tracking logs • Full access permissions to each test mailbox to have: Access to mailbox to send and receive test messages

Creating test mailboxes for Exchange

Dedicated test mailboxes must be created to run the following tests:

- Internal Server Delivery Health - requires at least one mailbox per server

- Internal Mailbox Delivery Health - requires source and destination mailbox pairs

- External Message Delivery Health - requires one source mailbox

- Modern Message Delivery Health - requires source and destination mailbox pairs for internal delivery test and source mailbox for external delivery test.

- Internal OWA Availability Health

    ▪ Exchange 2007 - requires at least one mailbox

- External OWA Availability Health - requires test account with mailbox

- Internal Mailbox Delivery Health - one or more test mailboxes on each mailbox database

Recommendation

It is recommended that you create test mailboxes for the tests that are only used for UC Diagnostics. Use the scripts provided to create these test mailboxes.

Creating Exchange 2007 test mailboxes

Creating Exchange 2010 or Exchange 2013 test mailboxes

About test mailboxes for Internal Server Delivery Health Test

About test mailboxes for the External Message Delivery Health Test

Creating a test mailbox for External Message Delivery Health Test

Creating a test mailbox for the Internal Mailbox Delivery Health Test

Creating test mailboxes for the OWA Availability Health Test

Creating a test mailbox for the External OWA Availability Health Test

Creating Exchange 2007 test mailboxes

UC Diagnostics ships with a PowerShell script called *new-Exchange2007TestMailboxes* to simplify creating test mailboxes for Exchange 2007 servers. This script will create one test mailbox per store per server. The list of Exchange servers must be piped into the script.

The script must be run inside the Exchange 2007 Management Shell from a computer in the same forest as the Exchange servers. The script has the following syntax:

```
.\new-Exchange2007TestMailboxes.ps1
-OrganizationalUnit <OrganizationalUnitString>]
[-MailboxNameMask <MailboxNameMaskString>]
[-AuthorizedUser <AuthorizedUserName>]
[-NoPrompt]
```

where:

Table 86. Exchange 2007 test mailbox parameters.

Parameter	Description
Organizational Unit	Indicates the location in the Active Directory where the created user is associated with a mailbox.
	If this parameter is not specified, you are prompted to enter the name of an Organizational Unit.
Mailbox Name Mask	Indicates the pattern of mailbox names that the script generates.
	This parameter is optional. If it is not specified, the default mask is SOM_<ServerName>_<StorageGroupName>_<StoreName>.
Authorized User	Indicates the user account that will be granted access to the created mailboxes. This should be the account specified for the Diagnostic Services component during install unless alternate credentials are specified for the test.
	If this parameter is not specified, you are prompted to enter the user account name.
No Prompt	Allows you to suppress confirmation to create each test mailbox.
	This parameter is optional. If it is not specified, confirmation is required before creating each test mailbox.

To run scripts, the account must have the following permissions:

Table 87. Exchange 2007 permissions required to run scripts

Exchange version	Permissions
Exchange 2007	• Exchange Recipient Administrator role
	• Account Operator role for the applicable Active Directory containers

For example, to create test mailboxes on all servers with the default mailbox mask, use:

```
Get-mailboxserver|.\new-Exchange2007TestMailboxes.ps1
-OrganizationalUnit
"CN=Users,DC=mscs,DC=qc,DC=kan,DC=ca,DC=qsft"
-AuthorizedUser Administrator
```

Or, to create test mailboxes on the server AMER-MBX-01 with a non-default mailbox mask:

```
Get-mailboxserver amer-mbx-01|.\new-Exchange2007TestMailboxes.ps1
-OrganizationalUnit
"OU=TestAccounts,DC=mscs,DC=qc,DC=kan,DC=ca,DC=qsft"
-AuthorizedUser myAccount -MailboxNameMask
TestMailbox.<StorageGroupName>.<ServerName>.<StoreName>
```

Creating Exchange 2010 or Exchange 2013 test mailboxes

To simplify creating test mailboxes for Exchange 2010 or Exchange 2013 servers, UC Diagnostics ships with a PowerShell script called new-Exchange2010and2013TestMailboxes. This script creates one test mailbox per database per server, or one test mailbox per server, depending on the mask setting. The list of Exchange servers must be piped into the script.

If the test source mailbox is hosted on an Exchange 2010/2013 mailbox database, the Exchange organization must have at least one available Exchange CAS server that exists on the same site as the server that hosts the active mailbox database copy. Mailboxes must be named according to the server and database where they are located.

If you are creating a test mailbox for the Exchange 2010 OWA Health test, ensure all database copies for the mailbox database are in the same site as your CAS server. Because the PowerShell cmdlet used in the test requires a test mailbox for each site, this guarantees you always have a test mailbox in the site, even when databases fail over/switch over among member servers of the Database Availability Group (DAG).

Exchange 2010/2013 mailbox creation script syntax

You must run the script inside the Exchange 2010 or Exchange 2013 Management Shell from a computer in the same forest as the Exchange servers. The script has the following syntax:

```
.\new-Exchange2010and2013TestMailboxes.ps1

-OrganizationalUnit <OrganizationalUnitString>]
[-MailboxNameMask <MailboxNameMaskString>]
[-AuthorizedUser <AuthorizedUserName>]
[-NoPrompt]
```

Table 88. Exchange 2010/2013 test mailbox parameters.

Parameter	Description
Organizational Unit	Indicates the location in the Active Directory where the created user is associated with a mailbox. If this parameter is not specified, you are prompted to enter the name of an Organizational Unit.
Mailbox Name Mask	Indicates the pattern of mailbox names that the script generates. This must match the setting in the Internal Server Delivery Health test.
	This parameter is optional. If it is not specified, the default mask is SOM_<ServerName>_<DatabaseName>.
	<DatabaseName> is optional.
Authorized User	Indicates the user account that is granted access to the created mailboxes. This must be the account specified for the Diagnostic Services component during install unless alternate credentials are specified for the test.
No Prompt	Allows you to suppress confirmation to create each test mailbox.
	This parameter is optional. If it is not specified, confirmation is required before creating each test mailbox.

To run this script, the account must have the following permissions:

- Exchange Recipient Administrator role.
- Account Operator role for the applicable Active Directory containers.

The list of Exchange servers must be piped into the script.

For example, to create one test mailbox for every mailbox server in the Exchange organization, use the following script:

```
Get-mailboxserver|.\new-Exchange2010and2013TestMailboxes.ps1
-OrganizationalUnit
"OU=TestAccounts,DC=mscs,DC=qc,DC=kan,DC=ca,DC=qsft"
-MailboxNameMask TestMailbox.<ServerName>
-AuthorizedUser myAccount
```

Or, to create one test mailbox on every mailbox database on the server AMER-MBX-01, use the following script:

```
Get-mailboxserver amer-mbx-01|.\new-Exchange2010and2013TestMailboxes.ps1
-OrganizationalUnit

"OU=TestAccounts,DC=mscs,DC=qc,DC=kan,DC=ca,DC=qsft"
-MailboxNameMask TestMailbox.<ServerName>.<DatabaseName>
-AuthorizedUser myAccount
```

About test mailboxes for Internal Server Delivery Health Test

This test involves the exchange of messages between each pair of servers in your network. You must create at least one test mailbox on each server that is included in the test.

By creating one mailbox per storage group/store (Exchange 2007) or per database (Exchange 2010), you can ensure that the complete test runs even if there is a problem with one of the stores or databases.

Mailboxes for the Internal Server Delivery Health test on Exchange 2007 servers must be named according to the server, storage group, and store where they are located. Mailboxes for the Internal Server Delivery Health test on Exchange 2010 servers must be named according to the server and database where they are located. For more information, see Exchange Internal Server Delivery Health Test on page 48.

If the test source mailbox is hosted on an Exchange 2010 mailbox database for the BlackBerry Message Delivery Health test or for the Exchange Internal and External Message Delivery Health tests, the Exchange organization must have at least, one available Exchange 2010 CAS server on the same site as the active mailbox database copy.

The Internal Server Delivery health test is not supported for Exchange 2013. Use the Internal Mailbox Delivery health test to monitor the sending and receiving of messages between mailboxes of all Exchange versions.

About test mailboxes for the External Message Delivery Health Test

The Exchange External Message Delivery health test allows you to monitor the ability to send a message to an external target and to measure delivery and round-trip time.

For this test, you must enter the names of:

- The source mailbox to send a message to an SMTP address and receive replies from that address.

- The destination email address where test messages is sent.

The destination mailbox can be in another Exchange organization or it can be in any of the free web-based email services.

To test round-trip delivery, the destination mailbox must be configured to automatically forward the message back to the originating mailbox, thus enabling the Round-Trip Delivery counter in the test. For the test to recognize the returning message, the original subject line must be inserted in the subject or body of the returning message.

If the test source mailbox is hosted on an Exchange 2010/2013 mailbox database, the Exchange organization must have at least one available Exchange 2010/2013 CAS server that exists on the same site as the server that hosts the active mailbox database copy.

Creating a test mailbox for External Message Delivery Health Test

The External Message Delivery Health tests do not have any restrictions on the name of the mailbox.

The Exchange External Message Delivery Health Test allows you to monitor the ability to send a message to an external target, and to measure delivery and round trip time.

For this test, you must enter the names of:

- The source mailbox to send a message to an SMTP address and receive replies from that address.

- The destination email address where test messages is sent.

The destination mailbox can be in another Exchange organization or in any free web-based email service.

To test round-trip delivery, the destination mailbox must be configured to automatically forward the message back to the originating mailbox, thus enabling the Round-Trip Delivery counter in the test. For the test to recognize the returning message, the original subject line must be inserted in the subject or body of the returning message.

For External Message Delivery Health tests, if the test source mailbox is hosted on an Exchange 2010/2013 mailbox database, the Exchange organization must have at least one available Exchange CAS server that exists on the same site as the active mailbox database copy.

To create test mailboxes for Exchange 2010/2013, see Creating Exchange 2010 or Exchange 2013 test mailboxes on page 81.

To create test mailboxes for Exchange 2007, see Creating Exchange 2007 test mailboxes on page 80.

Creating a test mailbox for the Internal Mailbox Delivery Health Test

You can create user mailboxes or dedicated test mailboxes for source and target mailbox pairs to allow both DAG and non-DAG database mailboxes. You can create one or more test mailboxes on each mailbox database.

For information about creating test mailboxes for Exchange 2010 or 2013, see Creating Exchange 2010 or Exchange 2013 test mailboxes on page 81. For information about creating test mailboxes for Exchange 2007, see Creating Exchange 2007 test mailboxes on page 80.

Creating test mailboxes for the OWA Availability Health Test

The OWA Availability Health uses a Microsoft PowerShell cmdlet called test-OwaConnectivity to test OWA availability. For this cmdlet to run, you must create at least one test mailbox using the Microsoft PowerShell cmdlet called `new-TestCasConnectivityUser`. For more information about this cmdlet, go to www.microsoft.com.

You must create one or more test mailboxes on a Mailbox server to perform this test. It is recommended that you set the accounts created for test mailboxes to have "password never expires". This setting prevents logon failures due to a password expiring.

Creating Exchange 2007 test mailboxes for OWA Availability

UC Diagnostics uses a PowerShell script to simplify creating test mailboxes for Exchange 2007 servers. You must create mailboxes for the Exchange 2007 OWA Availability Health test using the PowerShell cmdlet called new-CASConnectivityMailbox.

To create test mailboxes for the Internal OWA Availability test

1 Login to one of your Exchange 2007 Mailbox servers as a Domain Administrator.

2 Open the Exchange Management PowerShell Console.

3 Change the directory to the Exchange Server Scripts folder (for example, C:\Program Files\Microsoft\Exchange Server\Scripts)

4 Execute the following command:

    get-mailboxServer|.\new-TestCasConnectivityUser.ps1

5 When prompted for the Organizational Unit (OU), enter the Distinguished Name (DN).

   The OU is specified as a DN since multiple OUs of the same name can exist in your organization. For example:

```
OU=Users,DC=mscs,DC=qc,DC=kan,DC=ca,DC=qsft
```

Creating Exchange 2010 Test Mailboxes for OWA Availability

UC Diagnostics uses a PowerShell script to simplify creating test mailboxes for Exchange 2010 servers.Mailboxes for the Exchange 2010 OWA Availability Health test must be created using the PowerShell cmdlet called new-CASConnectivityMailbox.

Ensure all database copies of the mailbox database are in the same site as your CAS server. The PowerShell cmdlet used in the test requires a test mailbox for each site. This guarantees you always have a test mailbox in the site, even when databases fail over/switch over among member servers of the Database Availability Group (DAG).

To create test mailboxes for the Internal OWA Availability test

1   Login to one of your Exchange 2010 Mailbox servers as a Domain Administrator.

2   Open the Exchange Management PowerShell Console.

3   Change the directory to the Exchange Server Scripts folder (for example, C:\Program Files\Microsoft\Exchange Server\Scripts)

4   Execute the following command:

```
get-mailboxServer|.\new-TestCasConnectivityUser.ps1
```

To specify the OU in which the test mailboxes are created, include the "-ou" parameter in the above command. This avoids a potential error message returned by the script if the "Users" OU exists anywhere in your Active Directory. For example, enter:

```
get-mailboxServer|.\new-TestCasConnectivityUser.ps1 -ou
"OU=Users,DC=mscs,DC=qc,DC=kan,DC=ca,DC=qsft"
```

Creating a test mailbox for the External OWA Availability Health Test

This test verifies that users associated with the alternate credentials can logon to their mailboxes through an external OWA URL.

Since this test uses mailboxes associated with alternate credentials, you must explicitly choose the alternate credentials on the Test Settings page when you create this test.

Account Prerequisites

The account associated with alternate credentials must have a mailbox on Exchange 2007 or 2010. The alternate credentials must have View-Only Organization Management privileges for Exchange 2010.

Adding health sets for Exchange System health tests

You can include additional health sets that you want to monitor for the specific Exchange System Health tests that you want to run.

To add health sets

1   Click **<Add Health Sets>** located under one the following Health Sets sections in the listview of the Exchange system health test that you select:

- CustomerTouchPoints
- ServiceComponents
- ServerComponents
- DependencyAvailability

2   Enter one health set per line you want to add and click **OK**.

For more information about health sets, see Exchange System Health Test on page 67.

Configuring Exchange impersonation for the Modern Message Delivery health test

The Exchange Modern Message Delivery Health test uses Exchange Web Services (EWS) to connect to the test source and target mailboxes. The test credentials that are used must have "Exchange Impersonation" permissions to all the test mailboxes.

Configuring impersonation for all users

You can configure Exchange impersonation for all users in an organization.

To configure a service account to impersonate all users in an organization

1   Open the Exchange Management Shell.

2   Run the New-ManagementRoleAssignment cmdlet to add the permission to impersonate to the specified user.

The following example shows how to configure Exchange Impersonation to enable a service account to impersonate all other users in an organization.

```
New-ManagementRoleAssignment –Name:impersonationAssignmentName –
Role:ApplicationImpersonation –User:serviceAccount
```

Configuring impersonation for specific users or groups

You can configured Exchange impersonation for specific users or groups.

To configure a service account to impersonate specific users or groups of users

1   Open the Exchange Management Shell.

2   Run the New-ManagementScope cmdlet to create a scope to which the impersonation role can be assigned. If an existing scope exists, you can skip this step.

The following example shows how to create a management scope for a specific group.

```
New-ManagementScope –Name:scopeName –
RecipientRestrictionFilter:recipientFilter
```

3 Run the New-ManagementRoleAssignment cmdlet to add the permission to impersonate the members of the specified scope.

The following example shows how to configure Exchange Impersonation to enable a service account to impersonate all users in a scope.

```
New-ManagementRoleAssignment –Name:impersonationAssignmentName –
Role:ApplicationImpersonation –User:serviceAccount –
CustomRecipientWriteScope:scopeName
```

Registering UC Diagnostics with the Microsoft Azure portal

If you are connecting to Office 365 and are using OAuth 2.0 modern authentication to connect through PowerShell and EWS, you must register the UC Diagnostics application with the Microsoft Azure portal site. Depending on the region from which you are accessing the Microsoft Azure portal site, the user interface can differ.

You can configure OAuth 2.0 authentication to be used for the Exchange Online Mailbox Logon health test and for the Exchange Online Message Delivery health test.

UC Diagnostics uses client credential flows (Application permissions). You must have global administrator permissions to register the UC Diagnostics application with Azure Active Directory,

To register UC Diagnostics with Azure Active Directory

1 In the Azure Active Directory Admin Center, click **Azure Active Directory**.

2 Under Manage, select **App registrations**.

3 Select **Owned applications** and click **New registrations**.

4 Enter the application name in Name (such as UC Diagnostics) and click **Accounts in any organizational directory (Any Azure AD directory - Multitenant)**.

5 Click **Register**.

6 Select **Overview** and copy down the values that display for **Application (client) ID** and **Directory (tenant) ID**.

You will need this information to configure the UC Diagnostics Exchange Online Mailbox Logon Health and Exchange Online Message Delivery Health tests when using OAuth modern authentication.

7 Under Manage, select **API permissions** and click **Add a permission**.

8 Under Microsoft APIs scroll down to the Supported legacy APIs heading and click **Exchange**.

9 Click **Delegated permissions** and select the **EWS.AccessAsUser** check box under EWS.

10 Click **Add permissions**.

11 Under Configured Permissions, click **Add a permission**.

12 Select **Exchange** and click **Application permissions**.

13 Select the **full_access_as_app** check box and click **Update permissions**.

14 Click **Grant admin consent for <Your Directory Name>**. To perform this step, you must have administrator permissions.

After admin consent is granted, the status is green.

15 Under Manage, select **Authentication** and click **Yes** in the Advanced settings section.

16 Click **Save**.

17 Under Manage, select **Certificates & secrets** and click **New client secret**.

18 Enter a description in Description, select a time period for Expires, and click **Add**.

19 Copy down the **client secret value** that is displayed.

You will need this information to configure the UC Diagnostics Exchange Online Mailbox Logon Health and Exchange Online Message Delivery Health tests when using OAuth modern authentication.

Health tests available from the Lync/Skype for Business Environment

- About the Lync/Skype for Business health tests
- Lync/Skype Server Health Test
- Lync/Skype Synthetic Transaction Health Tests
    - Lync/Skype Instant Messaging Health Test
    - Lync/Skype Instant Messaging Conference Health Test
    - Lync/Skype Peer-to-Peer Audio/Video Call Health Test
    - Lync/Skype Audio/Video Conferencing Health Test
    - Lync/Skype Presence Status Health Test
    - Lync/Skype Logon Registration Health Test
    - Lync/Skype Address Book Service Health Test
    - Lync/Skype Persistent Chat Message Health Test
- Active Directory Account Lockout Health Test
- Skype for Business Online DNS Connectivity Health Test
- Office 365 Subscription Health Test
- OCS Server Health Test
- Creating a test user for the Lync/Skype Environment

About the Lync/Skype for Business health tests

The following health tests are available when you right-click the Exchange organization node:

Table 1. Available health tests for Lync/Skype for Business environment

Organization/Environment	Health Tests
Lync/Skype for Business	• Lync/Skype Server Health Test • Lync/Skype Instant Messaging Health Test • Lync/Skype Instant Messaging Conference Health Test • Lync/Skype Peer-to-Peer Audio/Video Call Health Test • Lync/Skype Audio/Video Conferencing Health Test • Lync/Skype Presence Status Health Test • Lync/Skype Logon Registration Health Test • Lync/Skype Address Book Service Health Test • Lync/Skype Persistent Chat Message Health Test • Active Directory Account Lockout Health Test
Office 365	• Office 365 Subscription Health Test • Skype for Business Online DNS Connectivity Health Test
Office Communications Server (OCS)	• OCS Server Health Test

You can also create a Generic Server Health Test to monitor your generic servers. To create a Generic Server Health Test, see Creating and configuring health tests on page 27.

Lync/Skype Server Health Test

The Lync/Skype Server Health Test allows you to monitor the basic health of all your Lync or Skype for Business servers. This test allows you to monitor the following types of information:

- Network availability
- Operating system disk space usage
- Any Performance Counter
- Any Windows service
- Any Event Log entry

Best Practice

It is recommended that you configure two server health tests - one test without monitoring event logs with an interval of 30 minutes and the second test for monitoring event logs that run only once a day.

Lync or Skype Server Health Test Prerequisites

The following tables show the test target servers, required configuration to run the test, and the permissions required by the test credentials.

Table 2. Lync or Skype server health test targets.

Server version	Server type
All	All servers
	NOTE: The Lync/Skype Server Health test does not monitor federated partners.

Table 3. Lync or Skype server health test required configuration.

Lync or Skype server version	Required Configuration
All	• Enable WMI on each Lync or Skype server • Enable remote access to any database

Table 4. Lync or Skype server health test credential required permissions.

Lync or Skype server version	Permissions Required for Test Credentials
All	• Member of Local Administrators group on each Lync or Skype server to have: Read access to operating system drive to retrieve disk space Read access to Windows system directory to access Event Logs Read access to Service Control Manager Read access to Registry to access Performance Counters and Event Logs

Lync/Skype Synthetic Transaction Health Tests

In addition to the basic server health test, you can use additional health tests to monitor activities on your Lync 2010, Lync 2013, and Skype for Business 2015 servers such as instant messaging, conferences, peer-to-peer audio/video calls, logon registration, and address book service. The test targets for these health tests are Lync 2010, Lync 2013, and Skype for Business 2015 pools.

- Lync/Skype Instant Messaging Health Test
- Lync/Skype Instant Messaging Conference Health Test
- Lync/Skype Peer-to-Peer Audio/Video Call Health Test
- Lync/Skype Audio/Video Conferencing Health Test
- Lync/Skype Presence Status Health Test
- Lync/Skype Logon Registration Health Test
- Lync/Skype Address Book Service Health Test
- Lync/Skype Persistent Chat Message Health Test

For some of the synthetic transaction health tests, you must create a test Lync or Skype user. For more information, see Creating a test user for the Lync/Skype Environment on page 98.

Lync/Skype Synthetic Transaction Health Test Prerequisites

The following software prerequisites and permissions are required for all the Lync and Skype for Business synthetic tests.

Lync/Skype Test Software Prerequisites

To run the health tests on Lync 2010, Lync 2013, or Skype for Business 2015, ensure the following software prerequisites are met:

- You must have PowerShell 2.0 or later installed on the UC Diagnostics computer.

- You must enable Remote PowerShell on each Lync or Skype for Business server.

Permissions Required for Lync/Skype Test Credentials

The test credentials that are used to run the health tests on the Lync 2010, Lync 2013, and Skype for Business 2015 servers must have the following permissions:

- Member of Local Administrators group -
  required to permit PowerShell cmdlets to access Lync or Skype server

- Member of CsHelpDesk, CSAdministrator, or CSServerAdministrator security group -
  required to permit PowerShell cmdlets to run discovery and pool tests.

Creating a test user for the Lync/Skype Environment

Lync/Skype Instant Messaging Health Test

This test allows you to monitor the operation of instant messaging between two test users in a pool.

Table 5. Counters for instant messaging (IM) health test counters.

Category	Counter
Instant Messaging Transaction	• Transaction latency in seconds • Transaction status • Transaction details

Lync/Skype Instant Messaging Conference Health Test

This test allows you to monitor the operation of instant messaging conferencing between two test users in a pool.

Table 6. Counters for instant messaging (IM) conference health test counters.

Category	Counter
Instant Messaging Conferencing Transaction	• Transaction latency in seconds • Transaction status • Transaction details

Lync/Skype Peer-to-Peer Audio/Video Call Health Test

This test allows you to monitor the operation of peer-to-peer audio/video conversation between two test users in a pool.

Table 7. Counters for peer-to-peer audio/video call health test counters.

Category	Counter
Peer-To-Peer Audio/Video Call Transaction	• Transaction latency in seconds • Transaction status • Transaction details

Lync/Skype Audio/Video Conferencing Health Test

This test allows you to monitor the operation of audio/video conferencing between two test users in a pool.

Table 8. Counters for peer-to-peer audio/video conference health test counters.

Category	Counter
Audio/Video Conferencing Transaction	• Transaction latency in seconds • Transaction status • Transaction details

Lync/Skype Presence Status Health Test

This test allows you to monitor the exchange of presence information between two test users in a pool.

Table 9. Counters for presence status health test counters.

Category	Counter
Presence Status Transaction	• Transaction latency in seconds • Transaction status • Transaction details

Lync/Skype Logon Registration Health Test

This test allows you to monitor the operation of logon registration to a pool.

Table 10. Counters for logon registration health test counters.

Category	Counter
Logon Registration Transaction	• Transaction latency in seconds • Transaction status • Transaction details

Lync/Skype Address Book Service Health Test

This test allows you to monitor the ability to connect to an Address Book Download Web Service from a pool.

Table 11. Counters for address book service health test counters.

Category	Counter
Address Book Service Transaction	• Transaction latency in seconds • Transaction status • Transaction details

Lync/Skype Persistent Chat Message Health Test

This test verifies whether two users can exchange messages using the Persistent Chat service. The test logs two users on to Lync Server 2013 or to Skype for Business 2015, connects the users to a persistent chat room, exchanges a pair of messages, exits the chat room and logs off the two users.

This test will fail if you have not created a chat room or if the two test users have not been assigned a Persistent Chat policy that provides access to the Persistent Chat service.

The test is not available for Lync 2010.

Table 12. Persistent chat message health test required configuration.

Lync/Skype server version	Required Configuration
All	The test uses the PowerShell Test-CsPersistentChatMessage –TargetPoolFqdn <target fqdn> cmdlet. Before the cmdlet can work, you must use Setup parameter to enable it. • Run the Test-CsPersistentChatMessage cmdlet with the Setup parameter from a computer that has access to the Lync/Skype server topology. **NOTE:** When you use the Setup parameter, you must also use the TestUser1SipAddress and the TestUser2SipAddress parameters.

For example, suppose you are running the Test-CsPersistentChatMessage cmdlet with the Setup parameter for a pool named LyncEnt-pool.smov2.qc.kan.ca.qsft. First you must create two test users in the pool. If you are running the test against more than one Lync 2013 registrar pool, you must create same test users for each pool.

For more information about creating Lync/Skype test users, see

The following example shows the syntax for the cmdlet:

```
Test-CsPersistentChatMessage -TargetFqdn LyncEnt-pool.smov2.qc.kan.ca.qsft –Setup
$true -TestUser1SipAddress "sip:testuser1@smov2.qc.kan.ca.qsft"
-TestUser2SipAddress "sip:testuser2@smov2.qc.kan.ca.qsft"
```

Table 13. Counters for persistent chat message health test counters.

Category	Counter
Persistent Chat Message Transaction	• Transaction latency in seconds • Transaction status • Transaction details

Skype for Business Online DNS Connectivity Health Test

The Skype for Business Online DNS Connectivity Health test helps you verify the correctness of your DNS configuration and identify any issues. Skype for Business Online requires four DNS records. The domain name is the name of the Session Initiation Protocol (SIP) of your organization.

In China, Skype for Business Online is operated by 21Vianet and the required DNS configuration has different destination domain names. When you configure the health test, you must select the appropriate service:

- Office 365
- Office 365 operated by 21Vianet

Table 14. Skype for Business Online DNS connectivity health test counters

DNS Record Type	Service	Domain Name	Protocol	Port	Purpose
SRV (Service)	_sip	*sipdir.online.lync.com*	_tls	443	Used by Skype for Business to coordinate the flow of information between Lync clients.
SRV (Service)	_sipfederation	*sipfed.online.lync.com*	_tcp	5061	Allows your Office 365 domain to share instant messaging (IM) features with external clients by enabling SIP federation.
CNAME (Alias)	sip	*sipdir.online.lync.com*			Used by the Lync client to help find the Skype for Business Online service and sign in.
CNAME (Alias)	lyncdiscover	*webdir.online.lync.com*			Used by the Lync mobile client to help find the Skype for Business Online service and sign in.

Table 15. Skype for Business Online operated by 21 Vianet DNS connectivity health test counters

DNS Record Type	Service	Domain Name	Protocol	Port	Purpose
SRV (Service)	_sip	*sipdir.online.partner.lync.cn*	_tls	443	Used by Skype for Business to coordinate the flow of information between Lync clients.
SRV (Service)	_sipfederation	*sipfed.online.partner.lync.cn*	_tcp	5061	Allows your Office 365 domain to share instant messaging (IM) features with external clients by enabling SIP federation.
CNAME (Alias)	sip	*sipdir.online.partner.lync.cn*			Used by the Lync client to help find the Skype for Business Online service and sign in.
CNAME (Alias)	lyncdiscover	*webdir.online.partner.lync.cn*			Used by the Lync mobile client to help find the Skype for Business Online service and sign in.

Table 16. Skype for Business Online DNS connectivity health test targets.

Platform	Target Type
Office 365	Skype for Business Online

Table 17. Skype for Business Online DNS connectivity health test required software.

Platform	Software Required on the UC Diagnostics computer
Office 365	• Windows PowerShell 5.0 or later • Microsoft Online Service Sign-in Assistant • Microsoft Azure Active Directory Module for Windows PowerShell • Microsoft Exchange Online PowerShell Module

Office 365 Subscription Health Test

The Office 365 Subscription Health test provides an overview of your Office 365 licensing plans. Licensing plans define the Office 365 services that are available to users. The test shows license activity such as the number of licenses that are currently assigned to users (used) and how many licenses are due for renewal.

About the Office 365 subscription lifecycle

During the first 30 days after an Office 365 subscription ends, the Office 365 tenant account is in a period known as the expired state. During the expired period, users can still access data. After 30 days, the tenant account enters the disabled state for 90 days. During this period, users cannot access data. An Office 365 administrator can log in, backup data, or reactivate the subscription.

At the end of the disabled state, 120 days after the subscription has ended, the account enters the deprovisioning state. During the deprovisioning state, the data from user accounts and also email data and documents, is permanently deleted.

Table 18. Office 365 Subscription health test counters.

Category	Counter
Total licenses	Total number of purchased licenses in the licensing plan.
Number of licenses used	Number of licenses that have been assigned to users in the specified licensing plan.
Number of licenses used (%)	Percentage of licenses that have been assigned to users in the specified licensing plan.
Number of licenses that must be renewed	Number of licenses in the licensing plan that have not been renewed and that will expire after the 30-day grace period.
Next lifecycle date	Next date on which a a subscription lifecycle event occurs. Lifecycle events can include states such as active, expired, disabled, or deprovisioned.
Next lifecycle date (days)	Date on which the next subscription lifecycle event will occur that is less than the specified number of days. You can set thresholds for warning and error notifications.

Table 19. Office 365 Subscription health test targets.

Platform	Target Type
Office 365	All services

The following software is required.

Table 20. Office 365 subscription health test required software.

Platform	Software Required on the UC Diagnostics computer
Office 365	• Windows PowerShell 5.0 or later
	• Microsoft Online Service Sign-in Assistant
	• Microsoft Azure Active Directory Module for Windows PowerShell
	• Microsoft Exchange Online PowerShell Module

Table 21. Office 365 Subscription health test credential required permissions.

Platform	Permissions Required for Test Credentials
Office 365	Valid Office 365 credential that was used to connect to Office 365.

If the password of the Office 365 credential is changed, you must change the password on Office 365 connection properties.

OCS Server Health Test

The OCS Server Health Test allows you to monitor the basic health of all your OCS 2007 and OCS 2007 R2 servers. This test allows you to monitor the following types of information:

- Network availability
- Operating system disk space usage
- Any Performance Counter
- Any Windows service
- Any Event Log entry

OCS Server Health Test Prerequisites

The following tables show the test target servers, required configuration to run the test, and the permissions required by the test credentials.

Table 22. OCS server health test targets.

OCS server version	Server type
All	All servers
	The OCS Server Health test does not monitor federated partners.

Table 23. OCS server health test required configuration.

OCS server version	Required Configuration
All	• Enable WMI on each OCS server
	• Enable remote access to any back-end databases

Table 24. OCS server health test credential required permissions.

OCS server version	Permissions Required for Test Credentials
All	• Member of the Local Administrators group on each OCS server • db_datareader rights for any back-end databases For SQL server prerequisites, see the *Unified Communications Diagnostics Deployment Guide*. You can become a member of RTCUniversalServerAdmin to update the Back-End databases to provide the db_datareader user role for the rtc, rtcconfig, and rtcdyn tables. As an alternative, you can: 1 Create a new Security Group (such as UC OCS Diagnostic Users). 2 Map UC OCS Diagnostic Users into the Back-End Database and provide a User Mapping to the rtc, rtcconfig, and rtcdyn databases with the public and db_datareader role. 3 Add UC OCS Diagnostic Users to the RTCUniversalReadOnlyAdmins group. 4 Add UC OCS Diagnostic Users to the Power Users and Performance Monitor Users security group on each OCS server through a GPO or some other mechanism.

Creating a test user for the Lync/Skype Environment

Several of the Lync/Skype synthetic transaction health tests require test users. You must create test users for each registrar pool against which you want to run health tests.

These test users are created using a Microsoft PowerShell cmdlet called `New-CsHealthMonitoringConfiguration`. You execute the PowerShell cmdlet in the Lync Server Management Shell on the Lync server or the Skype for Business Server Management Shell on the Skype server. For more information about this cmdlet, go to www.microsoft.com.

The script has the following syntax:

```
New-CsHealthMonitoringConfiguration
-Identify <XdsGlobalRelativeIdentity>
-FirstTestUserSipUri <String>
-SecondTestUserSipUri <String>
[-Confirm [<SwitchParameter>]]
[-FirstTestSamAccountName <String>]
[-Force <SwitchParameter>]
[-InMemory <SwitchParameter>]
[-SecondTestSamAccountName <String>]
[-WhatIf [<SwitchParameter>]]
```

where:

Table 25. Lync/Skype test user parameters.

Parameter	Description
Identify	Identifies the location in the Active Directory where the created user is associated with a mailbox. If this parameter is not specified, you are prompted to enter the name of an Organizational Unit.

Table 25. Lync/Skype test user parameters.

Parameter	Description
FirstTestUserSipUri or SecondTestUserSipUri	Identifies the mailbox names that the script generates.
FirstTestSamAccountName or SecondTestSamAccountName	Identifies an account name to be associated with the test mailboxes. This parameter is optional.
Confirm	Selects whether to prompt for confirmation before executing the command.
Force	Selects whether to suppress the display of any non-fatal error message that may occur when executing the command.
InMemory	Creates an object reference without actually committing the object as a permanent change. If you assign the output of this cmdlet (called with this parameter) to a variable, you can make changes to the properties of the object reference and then commit those changes by calling this cmdlet's matching Set- cmdlet.
WhatIf	Describes what would happen if you executed the command, without actually executing the command.

An example use of the cmdlet follows:

```
New-CsHealthMonitoringConfiguration
-Identity LyncEnt-pool.smov2.qc.kan.ca.qsft
-FirstTestUserSipUri "sip:testuser1@smov2.qc.kan.ca.qsft"
-SecondTestUserSipUri "sip:testuser2@smov2.qc.kan.ca.qsft"
```

Test users are required to run the following Lync/Skype synthetic transaction health tests:

- Instant Messaging Health Test
- Instant Messaging Conference Health Test
- Peer to Peer Audio/Video Call Health Test
- Audio/Video Conferencing Health Test
- Presence Status Health Test
- Log On Registration Health Test
- Address Book Service Health Test
- Persistent Chat Message Health Test

To configure test users for Lync/Skype Health Tests

1. Login to one of your Lync or Skype servers as a member of group RTCUniversalServerAdmins.

2. Open the Lync Server Management Shell or the Skype for Business Server Management Shell.

3. Execute following command for each of the registrar pools you want to run UC Diagnostics tests against:

```
New-CsHealthMonitoringConfiguration
-Identity poolName.mycomany.com
-FirstTestUserSipUri "sip:user1@mycompany.com"
-SecondTestUserSipUri "sip:user2@mycompany.com"
```

Resolving Problems with Native Tools

Unified Communications Diagnostics allows you access to native management tools to help you troubleshoot and resolve problems with your Exchange, Skype for Business, Office 365, OCS, Lync, and BlackBerry environments.

Several tools are available that can be used for most environments.

- Native tools for most servers
- Native tools for Exchange
- Native tools for Lync/Skype for Business
- Native tools for Office 365
- Native tools for OCS
- Native tools for Lync/Skype for Business

Native tools for most servers

The following table identifies the common management tools that are available for most servers, including Exchange, BlackBerry, OCS, Lync, and Skype for Business:

Table 1. Common native tools accessible through UC Diagnostics.

Tool	Description
Computer Management	Allows you to manage a single local or remote computer. The Computer Management console combines several administration utilities you can use to do the following: • monitor system events • create and manage shared resources • view a list of users connected to a local or remote computer • set properties for storage devices • view device configurations and add new device drivers • manage applications and services
Event Viewer	Allows you to gather information about hardware, software, system problems, and to monitor Windows security events. Event Viewer records events in the application, security, and system.
Services	Allows you to start, stop, and configure Windows services.
Active Directory Users and Computers	Allows you to administer user accounts, computer accounts, groups, and organizational units (OUs).

To launch a tool

- Right-click a server and select **Resolve | Launch <tool name>**.

Native tools for Exchange

The following table identifies the specific management tools available for your Exchange servers:

Table 2. Native tools for Exchange accessible through UC Diagnostics.

Tool	Description
Exchange 2013 Admin Center	Allows you to access the Exchange 2013 Admin Center. For more information, see http://technet.microsoft.com/en-us/library/jj150562(v=exchg.150).aspx. **NOTE:** This is only accessible from the Exchange 2013 server.
Exchange Management Console	Allows you to manage your Exchange 2007/2010 servers organization.

To launch a tool

- Right-click a server and select **Resolve | Launch <tool name>**.

Native tools for Lync/Skype for Business

The following table identifies the specific management tools available for your Lync/Skype for Business servers:

Table 3. Native tools for Lync/Skype for Business accessible through UC Diagnostics

Tool	Description
Lync/Skype Server Control Panel	Allows you to add and configure your Lync/Skype environment.

To launch a tool

- Right-click a server and select **Resolve | Launch <tool name>**.

Native tools for Office 365

The following table identifies the portals that you can access to manage your Office 365 environment:

Table 4. Native tools for Office 365 accessible through UC Diagnostics

Tool	Description
Office 365 Admin Center	Allows an Office 365 administrator to manage user accounts and settings for Office 365. Provides access to your tenant Exchange Online and Skype for Business Online configuration.

To launch a tool

- Right-click the node and select **Resolve | Launch <tool name>**.

Native tools for OCS

The following table identifies the management tools available for your OCS 2007 or OCS 2007 R2 servers:

Table 5. Native tools for OCS accessible through UC Diagnostics

Tool	Description
OCS Administrator Console	Allows you to configure your OCS environment. **NOTE:** You cannot launch the OCS Administrator Console from an Edge server directly. You can access the OCS Administrator Console through the Computer Management native tool.
CWA Administration Console	Allows you to configure Communication Web Access (CWA) server for your OCS 2007 R2 organization. **NOTE:** The CWA Administration Console is not available from an OCS 2007 environment.
Group Chat Administrator Console	Allows you to configure Group Chat settings for your OCS 2007 R2 organization. **NOTE:** The Group Chat Administrator Console is not available from an OCS 2007 environment.

To launch a tool

- Right-click a server and select **Resolve | Launch <tool name>**.

Native tools for BlackBerry

The following table identifies the specific management tools available for your BlackBerry servers:

Table 6. Native tools for BlackBerry accessible through UC Diagnostics

Tool	Description
BlackBerry Manager	Allows you to manage and configure your BlackBerry devices to receive messages.
BlackBerry Server Configuration	Allows you to inspect and modify BlackBerry configurations.
BlackBerry Administration Service	Allows you to manage BlackBerry Servers, users and roles from the web.

To launch a tool

- Right-click a server and select **Resolve | Launch <tool name>**.

Launching the Diagnostic Console from the Management Console

You can use the Diagnostics Console plug-ins to diagnose your servers. The Diagnostics Console allows you to further diagnose and resolve issues for individual servers within your organization.

To launch the Diagnostic Console plug-in from the Management Console

- Right-click a server and select **Diagnose | Launch Diagnostic Console**.

You can access diagnostic consoles for all versions of Exchange, for BlackBerry, for OCS 2007 and 2007 R2, and for Lync 2013 and Skype for Business 2015.

- Diagnosing Exchange 2007 with the Diagnostic Console (Plug In)
- Diagnosing Exchange 2010 with the Diagnostic Console (Plug In)
- Diagnosing Exchange 2013 with the Diagnostic Console (Plug In)
- Diagnosing Exchange 2016 with the Diagnostic Console (Plug In)
- Diagnosing BlackBerry with the Diagnostic Console (Plug In)
- Diagnosing OCS with the Diagnostic Console (Plug In)
- Diagnosing Lync 2013 or Skype for Business 2015 with the Diagnostic Console (Plug In)

Launching UC Analytics from the Management Console

Another product in the Unified Communications Command Suite, UC Analytics provides dynamic interactive analytics to unlock the business intelligence trapped in your most widely-used corporate communication assets. Predefined and customized insights provide a simple way to:

- Understand and measure Exchange customer, partner, and competitor communication.

- Understand and measure messaging within your organization, for on-premise Exchange, and for hybrid and native Office 365 (Exchange Online)

- View statistics for your legacy (Exchange 2007 and Exchange 2010) public folders and replicas and for new (Exchange 2013 and Exchange 2016) public folders.

- View Exchange ActiveSync activity for mobile devices and users.

- Compare Skype for Business/Lync voice, conference, and peer-to-peer session activity for your employees.

- Identify Skype for Business/Lync servers, pools, departments, users, and devices that are experiencing poor quality calls and sessions.

- Compare Cisco peer-to-peer call and conference call activity for your employees.

UC Analytics unlocks the business intelligence in your corporate messaging system to enable better business decisions. If you have installed the UC Analytics web site, you can launch the Analytics web site from the Management Console.

To launch UC Analytics from the Management Console

- Right-click the UC Analytics node and enter the URL for the Analytics web site.

  For example, http://<*ServerName*>/Analytics/

Diagnosing Problems using the Diagnostic Console

Introducing the Diagnostic Console

The Diagnostic Console provides you with a real-time representation of the messaging system processes and components within a server. You can diagnose and resolve issues using the Diagnostic Console, which contains the following:

- Home Pages that highlight targeted areas of server activity.

- Graphical flows that illustrate the rate at which data is moving between server components. Colorful buttons, gauges, spinners, and containers display the value of key statistics and metrics.

- Visual warnings if the performance metrics exceed acceptable thresholds, which you can adjust. The buttons, gauges, and other visual objects, collectively referred to as components, change color to show you the source of the problem.

- Warning messages that are displayed well before the traffic levels of a server become critical.

- A range of reports and graphs that provide you with detailed information about a server. You can view this information on the screen or you can print it.

When you connect to the Diagnostic Console, the Home Page displays a high-level summary of your Exchange, BlackBerry, or OCS front-end server.

The Home Page contains the various panels, message flows, and drilldowns to help you perform an extensive analysis of components on your server. To view detailed information on specific components, right-click a component, message flow, and drilldown, and select What's This, Metrics, or Properties.

While the Management Console can run tests when it is closed, the Diagnostic Console cannot perform any actions when it is closed.

If you are using the Diagnostic Console as a monitoring tool, you must disconnect from, then reconnect to the Diagnostic Console daily.

For information about the software prerequisites, required permissions, and required configuration for using the diagnostic console, see the *Unified Communications Diagnostics Deployment Guide.*

Performance Considerations

The Diagnostic Console retrieves a large amount of data from a server at frequent intervals, which can affect the server's performance. Also, using the Diagnostic Console for an extended period of time can consume critical system resources, affecting the stability of UC Diagnostics.

It is recommended that the Diagnostic Console view a maximum of 10 servers at any one time.

Launching the Diagnostic Console from the Management Console

You can use the Diagnostic Console plug-in to diagnose your servers. The Diagnostic Console allows you to further diagnose and resolve issues within individual servers in your organization.

To launch the Diagnostic Console plug-in from the Management Console

• Right-click a server and select **Diagnose | Launch Diagnostic Console**.

Launching and Connecting to the Diagnostic Console

To directly launch the diagnostic console without starting the management console, use the following steps.

To launch and connect to the Diagnostic Console

1 Select **Start | Programs | Quest | Spotlight | UC Diagnostics Console**.

2 Select **File | Connect**.

3 Click the **Tools** button, then select **Create New Connection** to create a plug-in connection to the server.

4 Select a connection type, enter a connection name, and click **OK**.

5 Enter the address of target computer, and click **OK**.

6 In the Welcome to UC Diagnostics page, select **File | Connect**.

7 Select the plug-in connection you created, and click **Connect**.

For special information about connecting to an OCS environment, see .

Diagnosing Exchange 2007 with the Diagnostic Console (Plug In)

- Introducing the Exchange 2007 Diagnostic Console
- Understanding the Exchange 2007 Diagnostic Console
- Panels
- Message Flows
- Drilldowns
- Metrics

Introducing the Exchange 2007 Diagnostic Console

You can diagnose and resolve issues using the Exchange 2007 Diagnostic Console. You can view a real-time representation of the messaging system processes and components within specific connected Exchange 2007 servers.

The Exchange 2007 Diagnostic Console contains the following:

- Home pages that highlight targeted areas of the Exchange 2007 server activity.
- Graphical flows that illustrate the rate at which data is moving between server components. Colorful buttons, gauges, queues, spinners, and containers display the value of key statistics and metrics.
- Visual warnings if the performance metrics exceed acceptable thresholds, which you can adjust. The buttons, gauges, queues, and other visual objects, collectively referred to as components, change color to show you the source of the problem.
- Warning messages that are displayed well before the traffic levels of a server become critical.
- A range of reports and graphs that provide you with detailed information about a server. You can view this information on the screen or you can print it.

Understanding the Exchange 2007 Diagnostic Console

The Exchange Diagnostic Console provides you with a real-time representation of the messaging system processes and components within Exchange. When you connect to the Exchange 2007 Diagnostic Console, the home page displays a high level summary of your Exchange 2007 server. You can diagnose and resolve issues using the Exchange Diagnostic Console.

The home page contains the various panels, message flows, and drilldowns to help you perform an extensive analysis of the major components on your Exchange 2007 server.

To view detailed information on specific components, right-click a component, message flow, and drilldown, and select What's This, Metrics, or Properties.

Exchange Diagnostic Console Recommendations

The Diagnostic Console retrieves a large amount of data from a server frequently, which can place excessive stress on a server, affecting the server's performance. Also, using the Diagnostic Console for an extended period of time can consume critical system resources, affecting the stability of UC Diagnostics as a whole.

Quest recommends the following:

- Allow the Diagnostic Console view a maximum number of 10 servers at any one time.

- If you install the Diagnostic Console on a computer that contains Spotlight products and you want to launch the Diagnostic Console from the UC Diagnostics Management Console, the Diagnostic Console and the Spotlight products must be installed on the C: drive. Otherwise, the Diagnostic Console fails to launch from the Management Console. As a workaround, create a shortcut on your desktop to C:\Program Files\Quest\Spotlight\Console\Spotlight.exe to manually open connections.

- If you are using the Diagnostic Console as a monitoring tool, you must disconnect from and reconnect to the Diagnostic Console daily. Though the Management Console can run tests when closed, the Diagnostic Console cannot perform any actions when it is closed.

For information about the Exchange software prerequisites, Exchange required configuration, and the permissions needed by the credentials to access Exchange, see the *Unified Communications Diagnostics Deployment Guide*.

Panels

The Exchange 2007 Diagnostic Console contains the following panels:

- AD/DNS Panel
- Server Role Status Panel
- Transport-In Panel
- Transport Panel
- Transport-Out Panel
- Clients Panel
- Information Store Panel
- OS/ Subsystem Panel

AD/DNS Panel

The components of the Directory Services panel indicate how Exchange 2007 interacts with directory services. This information includes:

Table 1. Exchange 2007 AD/DNS panel.

Component	Description
AD	Shows the status of the Active Directory (AD) servers used by this Exchange 2007 server
DNS	Shows the status about the Domain Name System (DNS) servers in use by this Exchange 2007 server

Server Role Status Panel

This panel shows the Exchange 2007 roles that are installed. This information includes:

Table 2. Exchange 2007 server role status panel.

Component	Description
MBX	Shows whether the Mailbox role is installed on this Exchange 2007 server. The Mailbox role is responsible for hosting mailbox and public folder data. It also provides MAPI access for Outlook clients.
UM	Shows whether the Unified Messaging role is installed on this Exchange 2007 server. The Unified Messaging role enables you to access their mailbox, address book, and calendar using telephone and voice. Note that IP-PBX or VoIP gateway must be installed to use the functionality of the Unified Messaging role.
CAS	Shows whether the Client Access role is installed on this Exchange 2007 server. The Client Access role provides mailbox server protocol access apart from MAPI. It allows you access to the mailboxes using Outlook Web Access (OWA), POP3/IMAP4, and ActiveSync.
EDG	Shows whether the Edge Transport role is installed on this Exchange 2007 server. The Edge Transport role provides mail quarantine and SMTP services to enhance security. It is the first hop of incoming mail and the last hop of outgoing mail. Note that it does not require AD access so that it can function with limited access to the corporate network (for added security).
HUB	Shows whether the Hub Transport role is installed on this Exchange 2007 server. The Hub Transport role handles mail flow by routing messages to either another Hub Transport server, an Edge server, or a Mailbox server. This role uses AD site info to determine the mail flow.

Transport-In Panel

The Transport-In panel groups components that represent current inbound connections to this Exchange 2007 server. This information includes:

Table 3. Exchange 2007 transport-in panel.

Component	Description
Connections	Shows the total number of inbound SMTP connections established by other SMTP hosts to this Exchange server. The number of connections represents the sum of all SMTP inbound connections from all remote domains to SMTP Receive Connectors on this Exchange 2007 server.

Table 3. Exchange 2007 transport-in panel.

Component	Description
Connectors	Shows the number of SMTP Receive connectors on this Exchange 2007 server that can accept mail from other SMTP servers.
Submission Queue	Shows the number of items in the Submission Queue. The submission queue holds messages before they are consumed by the Categorizer which determines what to do with the messages based on information about the intended recipients.
	After the submission queue, the Categorizer then routes the message to either an Edge Server role, another Hub server in a different AD Site, a mailbox on an Exchange server, or the Unreachable Queue.

Transport Panel

The Transport panel groups components that identify the status of the various transport queues on this Exchange 2007 server. This information includes:

Table 4. Exchange 2007 transport panel.

Component	Description
Unreachable Queue	Shows the number of messages in the transport unreachable queue on this Exchange 2007 server. The Unreachable Queue contains any messages that cannot be routed to their final destination.
Poison Queue	Shows the number of potentially harmful messages on this Exchange 2007 server. Messages that contain content that might be damaging to the Exchange Server system are by default delivered to this Poison Queue and suspended. If messages in this queue are deemed not harmful, message delivery can be resumed, and the message enters the Submission Queue.
Mailbox Delivery Queue	Represents the number of items in the Transport Mailbox Delivery Queue on this Exchange server. The mailbox delivery queue holds messages that are being delivered to mailbox recipients whose mailbox data is stored on a Mailbox server role located in the same site as this Transport server. The next hop for a message in this queue is the distinguished name of the destination mailbox store.
LDAP Search Time (ms)	Shows LDAP Search Time (in milliseconds) for the transport to send an LDAP search request to Active Directory, and receive a response on this Exchange 2007 server. Exchange 2007 uses Active Directory (AD) as a repository for mailbox and mail routing configuration data. Exchange 2007 servers issue LDAP queries against Active Directory to retrieve message routing data.

Transport-Out Panel

The Transport-Out panel groups components that represent current outbound activity from the Exchange 2007 server. This information includes:

Table 5. Exchange 2007 transport-out panel.

Component	Description
Connections	Shows the current number of outbound SMTP connections to other SMTP hosts. The number of connections represents the sum of all SMTP outbound connections from SMTP Send Connectors on this Exchange 2007 server to all remote SMTP domains.

Table 5. Exchange 2007 transport-out panel.

Component	Description
Connectors	Shows the number of SMTP Send connectors on this Exchange 2007 server that can service connections to other SMTP servers.
Remote Delivery Queue	Shows the number of messages in the transport that are queued for delivery to a remote server using SMTP. The Exchange 2007 Hub and Edge roles can have multiple remote delivery queues. Each queue contains messages with recipients that share the same remote server destination. On a Hub role server, the destination servers are within the same Exchange Organization as this Exchange server, but in a different AD Site. For the Edge role, the destination servers are external to the Organization, and handle message delivery for external SMTP domains.

Clients Panel

The Clients panel groups components that represent current client connections and associated latency to this Exchange 2007 server. This information includes:

Table 6. Exchange 2007 clients panel.

Component	Description
MAPI	Indicates the number of MAPI user connections to this Exchange 2007 server. The Mailbox role provides MAPI access for Microsoft Outlook clients, and enables these types of connections.
OWA	Indicates the number of current unique OWA users logged on to this Exchange 2007 server. The Client Access role provides OWA to allow you to access his or her mailbox from a web browser and have full access to all the information in the mailbox including task lists, calendar information, mail items, public folders, UNC shares (\\servername\share) and SharePoint documents. This value is decremented when a you log off your OWA session or the session times out.
ActiveSync	Shows the number of current secure HTTP connections (HTTPS) that are established from Windows Mobile-based or Exchange ActiveSync-enabled mobile devices and this Exchange 2007 server. ActiveSync is a push orientated protocol. Data such as user messages, schedules, contact information and tasks are synchronized over the HTTPS connection.
Outlook Anywhere	Shows the number of unique users currently connected to this Exchange 2007 server via RPC/HTTP. In Microsoft Exchange Server 2007, the Outlook Anywhere feature, formerly known as RPC over HTTP, lets clients that use Microsoft Office Outlook to connect to their Exchange servers from outside the corporate network or over the Internet using the RPC over HTTP Windows networking component.
POP3	Shows the number of POP3 connections to this Exchange 2007 server. The Client Access role provides POP3 access to mailbox data for clients that rely on this protocol.
IMAP4	Shows the number of IMAP4 connections to this Exchange 2007 server. The Client Access role provides IMAP4 access to mailbox data for clients that rely on this protocol.
Latency (ms) (for MAPI)	Shows the average latency for MAPI clients connected with Outlook to this Exchange 2007 server providing the Mailbox role.
Latency (ms) (for OWA)	Shows the average latency for OWA clients on the Exchange 2007 server.
Latency (ms) (for ActiveSync)	Shows the average latency for ActiveSync clients on the Exchange 2007 server.
Latency (ms) (for POP3)	Shows the average latency for POP3 clients on the Exchange 2007 server.
Latency (ms) (for IMAP4)	Shows the average latency for IMAP4 clients on the Exchange 2007 server.

Information Store Panel

The Information Store panel displays key operational metrics for the information store on this Exchange server. This information includes:

Table 7. Exchange 2007 information store panel.

Component	Description
Average message delivery time(sec)	Indicates the average time in seconds between the submission of a message to the mailbox store and the delivery to all local recipients (recipients on the same server) for the last ten messages.
Clients with RPC (Remote Procedure Calls) latency > 2 sec	Indicates the number of client reported Remote Procedure Calls (RPCs) with a latency greater than two seconds. The most commonly used RPC protocol is MAPI, and a high RPC latency can cause MAPI clients such as Microsoft Outlook to hang and stop responding when users send email, receive email, or use calendar functionality such as creating or viewing appointments.
Average mailbox database size	Indicates the average size of the mailbox database.
Total Logons	Indicates the total number of logons to the information store on this Exchange 2007 server. This includes end-user client connections and system processes that are currently logged-on to any storage group in the local information store. There can be multiple logons per connection for most client applications. As a result, it is possible to see the number of client logons exceed the number of mailboxes on a server.
Average client RPC latency (ms)	Shows the average time (in milliseconds) that it takes the server to respond to RPC connected clients. The average is for the past 1024 packets. The most commonly used RPC protocol is MAPI. A high RPC latency can cause MAPI clients such as Microsoft Outlook to hang and stop responding when users send email, receive email, or use any type of calendar functionality such as creating or viewing appointments.
Mailbox Stores	Shows the percentage of disk space consumed by the mailbox stores on this server. This also shows how much of the server disk consumption is attributable to mailbox store consumption versus other data.
Public Folders	Shows the percentage of public store disk space consumption on this server. This allows you to assess how much of the server disk consumption is attributable to public store data versus other data.
Transaction Logs	Shows the total percentage of disk space consumed by the transaction logs on this server. It can be used to quickly assess how much server disk consumption is attributable to transaction log data versus other data on the Exchange server.
Send Queue	Shows the number of messages in the send queue of the information store. This queue holds all outgoing messages from the information store.
Receive Queue	Shows the number of messages in the receive queue of the information store. These messages are waiting to be processed by the information store.
Storage Groups	Shows the number of storage groups installed on the Exchange 2007 server.
Store Memory	Shows the total physical memory of the store process.
Mailbox Count	Shows the total number of mailboxes that reside in all mailbox stores and public folders.

OS/ Subsystem Panel

The OS/ Subsystem panel displays components that represent the health of important subsystem features. This information includes:

Table 8. Exchange 2007 OS/ subsystem panel.

Component	Description
Exchange Services	Indicates the sum of CPU utilization for all of the Exchange 2007 services running on this server.
System Disk	Shows the percentage of disk usage for the Windows system disk on this Exchange 2007 server.
CPU Usage	Shows the amount of CPU used on this Exchange 2007 server.
System Memory	Shows the amount of physical memory (RAM) Windows is using. Physical memory usage can normally remain close to the total amount of physical memory installed on the system unless the amount of physical memory exceeds the amount of virtual memory that Windows is using. Windows normally keeps some physical memory available for immediate use.
Ping Time	Indicates the amount of time it takes the computer running the Diagnostic Console to ping the target server.
Top CPU Consumer	Identifies the process that is consuming the most CPU on this Exchange 2007 server.
Top Memory Consumer	Identifies the process that is consuming the most memory on this Exchange 2007 server.

Message Flows

The Exchange 2007 Diagnostic Console contains the following message flows that show the amount of information being sent to various components in your Exchange 2007 environment.

Table 9. Exchange 2007 message flows panel.

Message flow	Description
Msgs Submitted/sec	Indicates the rate of messages being submitted per second to this Exchange 2007 transport queues.
Msgs Received/sec	Indicates the rate of messages received by SMTP Receive connector on this Exchange 2007 server.
MAPI Msgs Submitted/sec	Indicates the rate that messages are submitted to the Information Store on the Exchange server by MAPI clients (connected with Outlook).
OWA Msgs Received/sec	Indicates the rate that bytes are received by Exchange server from OWA clients.
ActiveSync Bytes Received/sec	Indicates the rate that bytes are received by Exchange this server from ActiveSync mobile devices.
POP3/IMAP4 Bytes Received/sec	Indicates the number of bytes per second received from POP3 and IMAP4 clients.
Msgs Sent/sec	Indicates the number of messages sent per second to the transport.
Msgs Delivered/sec	Indicates the rate of messages delivered to all recipients with mailboxes on this Exchange 2007 server.
Bytes Received/sec	Indicates the number of bytes received per second from all RPC clients on this Exchange 2007 server information store. RPC clients includes all internal Exchange system components.
Bytes Sent/sec	Indicates the number of bytes sent per second to all RPC clients from this Exchange 2007 server information store. RPC clients includes all internal Exchange system component.

Table 9. Exchange 2007 message flows panel.

Message flow	Description
Bytes Read/sec	Indicates the rate at which data is being read from the disk, network, and device subsystems of the Windows server running Exchange. The data is primarily being read from the disk subsystem.
Bytes Written/sec	Indicates the rate at which data is being written to the disk, network, and device subsystems of the Windows server running Exchange. The data is primarily being written to the disk subsystem.
Msgs Queued/sec	Indicates the number of messages queued for delivery per second on this Exchange 2007 server.
Msgs Sent/sec	Indicates the number of outbound messages sent per second by the SMTP send connectors on this transport server..

Drilldowns

Each drilldown page contains displays that provide you with specific information about the components of your system. Drilldowns mainly use two different types of displays — tables and charts. Drilldowns have the following features:

- They can be configured to show all or some of the metrics associated with components.

- You can access further information about displays in drilldowns by moving the mouse over the displays, or by clicking or right-clicking on them.

- You can copy the data shown in drilldowns to other applications or save it to a file.

- You can view a brief description of a drilldown by hovering your mouse over a component, such as a button, dataflow, status ball, or Toolbar button.

To view a drilldown

Right-click a component in a panel and select **Show Details.**

Table 10. Exchange 2007 drilldowns.

Drilldown	Associated charts/tabs
Active Directory Server Details	• Active Directory Servers — shows information about the Active Directory servers in use by this Exchange 2007 server. Exchange 2007 stores all configuration and recipient information in the Active Directory directory service database. All Exchange 2007 roles use Active Directory except the Edge role, which does not have access to Active Directory. The Edge role uses Active Directory Application Mode (ADAM) to store schema and configuration information. • Active Directory Server Details - Shows information about the currently selected Active Directory. Exchange 2007 stores all configuration and recipient information in the Active Directory directory service database. All Exchange 2007 roles use Active Directory except the Edge role which does not have access to Active Directory. The Edge role uses ADAM to store schema and configuration information.
DNS Servers	• DNS Servers - Shows information about the DNS servers in use by this Exchange 2007 server. The Exchange 2007 server uses the DNS server that is configured in the IP properties of the network adapter to locate domain controllers and global catalog servers, other Exchange servers, and remote domains. DNS lookup settings can be specified on the Hub Transport server, which override the settings on the network adapter to route messages.
Transport In/Transport/Transport Out	• Inbound Connections — shows the total number of inbound SMTP connections established by other SMTP hosts to this Exchange server • Outbound Connections — shows the current number of outbound SMTP connections to other SMTP hosts • Inbound Connectors — shows the number of SMTP Receive connectors on this Exchange 2007 server that are required to accept mail from other SMTP servers • Outbound Connectors — shows the number of SMTP Send connectors on this Exchange 2007 server that are required to handle connections to other SMTP servers • LDAP Search Time — shows LDAP Search Time (in ms) that is taken to send an LDAP search request and receive a response on this Exchange 2007 server • Transport Queues — shows the number of messages in the transport queues on this Exchange 2007 server
Clients	• MAPI — indicates the number of MAPI connections to this Exchange 2007 server. The Mailbox role provides MAPI access to Microsoft Outlook clients. • OWA — indicates the number of OWA connections to this Exchange 2007 server. The Client Access role provides OWA to allow a you to access to your mailbox information through a web browser. • ActiveSync — shows the number of ActiveSync connections to this Exchange 2007 server. The Client Access role uses ActiveSync to allow mailbox access from mobile devices. • POP3 — shows the number of POP3 connections to this Exchange 2007 server. The Client Access role provides POP3 access to mailbox data for clients that rely on this protocol. • IMAP4 — shows the number of IMAP4 connections to this Exchange 2007 server. The Client Access role provides IMAP4 access to mailbox data for clients that rely on this protocol.

Table 10. Exchange 2007 drilldowns.

Drilldown	Associated charts/tabs
Information Store	• Average Message Delivery Time — indicates the average time in seconds between the submission of a message to the mailbox store and the delivery to all local recipients (recipients on the same server) for the last 10 messages. • Total Logons — indicates the number of clients (including system processes) currently logged to any storage group in the information store. • Clients with RPC Latency > 2 sec – indicates the number of client reported RPCs (Remote Procedure Calls) with a latency greater than two seconds. • Average Client RPC Latency — shows the average time (in milliseconds) that it takes the server to respond to RPC connected clients. • Outlook Anywhere - indicates the number of unique users currently connected to this Exchange 2007 server via RPC/HTTP. The Outlook Anywhere feature, formerly known as RPC-over-HTTP, lets clients that use Microsoft Office Outlook to connect to their Exchange servers from outside the corporate network or over the Internet using the RP-over-HTTP Windows networking component.
Storage Groups	• Storage Groups table — shows the status of each storage group, the name of each storage group, the percentage of unused disk space for each transaction logs on the server, whether LCR is enabled on each storage group, copy status of any database replicas, whether or not circular logging is enabled, and the system path of each storage group. • Status — indicates the average time in seconds between the submission of a message to the mailbox store and the delivery to all local recipients (recipients on the same server) for the last ten messages, the number of clients (including system processes) currently logged to the selected Storage Group, and the number of incoming and outgoing messages. • Mailbox Stores — indicates the percentage of space taken up by this mailbox store or public folder on the disk on which it resides.
Exchange Services	• Exchange Services List — lists the Exchange services that are running on this Exchange 2007 server. Both required and optional services for the roles installed on this Exchange server are listed, along with their service status. • Service Details — shows the CPU and memory usage of the currently selected Exchange 2007 service.

Table 10. Exchange 2007 drilldowns.

Drilldown	Associated charts/tabs
Subsystem	• CPU Usage — indicates the processor CPU usage on this Exchange 2007 server. • System Memory — shows the amount of physical memory (RAM) Windows is using. • System Disk — shows the amount of used and free space on the Windows system disk on this Exchange 2007 server. • Ping Time — shows the ping time (in milliseconds) from the UC Diagnostics client to the Exchange 2007 server.
Processes	• Process Name — indicates the image name of the application itself. • CPU Usage — indicates the percentage of CPU time that the program is currently consuming. This is an instantaneous result. • Physical Memory — indicates the current size of the working set of the process. • Virtual Memory — indicates current memory allocated to this process that cannot be shared with other processes.

Metrics

A metric is an individual piece of information that UC Diagnostics has collected about the performance of a system, such as perfmon counters. The information may be a numeric value (a number or percentage), a string of text, or some other piece of data.

To view the perfmon counters

• Right-click a component and select **Metrics**.

The perfmon counter is visible in the Metric help section in the General tab.

Every time that the UC Diagnostics window is refreshed, UC Diagnostics retrieves the latest value of the metric, which can then be displayed in a drilldown or on the home page.

The Metric editor allows you to view and edit the properties of UC Diagnostics metrics, including their thresholds and severities. You can open the Metric editor for a component or a drilldown by right-clicking on the component and choosing Metrics from the invoked shortcut menu.

When you open the Metric editor, the General tab is open by default. Several metrics contain data source descriptions for the metric. The data source descriptions use the following list of functions.

Table 11. Exchange 2007 metrics.

Function	Description
max(x)	the maximum of a set of values in list x
max(x,y)	the maximum of x and y
min(x)	the minimum of a set of values in list x
count(x)	the number of values in list x
sum(x)	the sum of a set of values in list x
if(x,y,z)	if x is true, then return y, otherwise, return z
snull(x)	if x could not be collected, then return true
avg(x)	the average of values in list x

Diagnosing Exchange 2010 with the Diagnostic Console (Plug In)

Introducing the Exchange 2010 Diagnostic Console

The Exchange 2010 Diagnostic Console provides a real-time representation of the messaging system processes and components within specific connected Exchange 2010 servers. You can diagnose and resolve issues using the Exchange 2010 Diagnostic Console.

The Exchange 2010 Diagnostic Console contains the following:

- Home pages that highlight targeted areas of the Exchange 2010 server activity.

- Graphical flows that illustrate the rate at which data is moving between server components. Colorful buttons, gauges, queues, spinners, and containers display the value of key statistics and metrics.

- Visual warnings if the performance metrics exceed acceptable thresholds, which you can adjust. The buttons, gauges, queues, and other visual objects, collectively referred to as components, change color to show you the source of the problem.

- Warning messages that are displayed well before the traffic levels of a server become critical.

- A range of reports and graphs that provide you with detailed information about a server. You can view this information on the screen or you can print it.

Understanding the Exchange 2010 Diagnostic Console

When you connect to the Exchange 2010 Diagnostic Console, the home page displays a high level summary of your Exchange 2010 server.

The home page contains the various panels, message flows, and drilldowns to help you perform an extensive analysis of the major components on your Exchange 2010 server.

To view detailed information on specific components, right-click a component, message flow, or drilldown and select What's This, Metrics, or Properties.

Exchange Diagnostic Console Recommendations

The Exchange Diagnostic Console provides you with a real-time representation of the messaging system processes and components within Exchange.

The Diagnostic Console retrieves a large amount of data from a server frequently, which can place excessive stress on a server, affecting the server's performance. Also, using the Diagnostic Console for an extended period of time can consume critical system resources, affecting the stability of UC Diagnostics as a whole.

You can diagnose and resolve issues using the Exchange Diagnostic Console.

Quest recommends the following:

- Allow the Diagnostic Console view a maximum number of 10 servers at any one time.

- If you install the Diagnostic Console on a computer that contains Spotlight products and you want to launch the Diagnostic Console from the UC Diagnostics Management Console, the Diagnostic Console and the Spotlight products must be installed on the C: drive. Otherwise, the Diagnostic Console fails to launch from the Management Console. As a workaround, create a shortcut on your desktop to C:\Program Files\Quest\Spotlight\Console\Spotlight.exe to manually open connections.

- If you are using the Diagnostic Console as a monitoring tool, you must disconnect from and reconnect to the Diagnostic Console daily. Though the Management Console can run tests when closed, the Diagnostic Console cannot perform any actions when it is closed.

For information about the Exchange software prerequisites, Exchange required configuration, and the permissions needed by the credentials to access Exchange, see the *Unified Communications Diagnostics Deployment Guide*.

Panels

The Exchange 2010 Diagnostic Console contains the following panels:

- AD/DNS Panel
- Server Role Status Panel
- Transport-In Panel
- Transport Panel
- Transport-Out Panel
- Clientsl Pane
- Information Store Panel
- OS/Subsystem Panel

AD/DNS Panel

The components of the Active Directory Services panel indicate how Exchange 2010 interacts with Active Directory services. This information includes:

Table 1. Exchange 2010 AD/DNS panel.

Component	Description
AD	Shows the status of the Active Directory (AD) servers used by this Exchange 2010 server
DNS	Shows the status about the Domain Name System (DNS) servers in use by this Exchange 2010 server

Server Role Status Panel

This panel shows the Exchange 2010 roles that are installed. This information includes:

Table 2. Exchange 2010 server role status panel.

Component	Description
MBX	Shows whether the Mailbox role is installed on this Exchange 2010 server. The Mailbox role is responsible for hosting mailbox and public folder data. It also provides MAPI access for Outlook clients.
UM	Shows whether the Unified Messaging role is installed on this Exchange 2010 server. The Unified Messaging role enables you to access their mailbox, address book, and calendar using telephone and voice. The IP-PBX or VoIP gateway must be installed to use the functionality of the Unified Messaging role.
CAS	Shows whether the Client Access role is installed on this Exchange 2010 server. The Client Access role provides mailbox server protocol access apart from MAPI. It allows you access to the mailboxes using Outlook Web Access (OWA), POP3/IMAP4, and ActiveSync.
EDG	Shows whether the Edge Transport role is installed on this Exchange 2010 server. The Edge Transport role provides mail quarantine and SMTP services to enhance security. It is the first hop of incoming mail and the last hop of outgoing mail. Note that it does not require AD access so that it can function with limited access to the corporate network (for added security).
HUB	Shows whether the Hub Transport role is installed on this Exchange 2010 server. The Hub Transport role handles mail flow by routing messages to either another Hub Transport server, an Edge server, or a Mailbox server. This role uses AD site info to determine the mail flow.

Transport-In Panel

The Transport-In panel groups components that represent current inbound connections to this Exchange 2010 server. This information includes:

Table 3. Exchange 2010 transport-in panel.

component	Description
Connections	Shows the total number of inbound SMTP connections established by other SMTP hosts to this Exchange server. The number of connections represents the sum of all SMTP inbound connections from all remote domains to SMTP Receive Connectors on this Exchange 2010 server.
Connectors	Shows the number of SMTP Receive connectors on this Exchange 2010 server that can accept mail from other SMTP servers.

Table 3. Exchange 2010 transport-in panel.

component	Description
Submission Queue	Shows the number of items in the Submission Queue. The submission queue holds messages before they are consumed by the Categorizer which determines what to do with the messages based on information about the intended recipients. After the submission queue, the Categorizer then routes the message to either an Edge Server role, another Hub server in a different AD Site, a mailbox on an Exchange server, or the Unreachable Queue.

Transport Panel

The Transport panel groups components that identify the status of the various transport queues on this Exchange 2010 server. This information includes:

Table 4. Exchange 2010 transport panel.

Component	Description
Unreachable Queue	Shows the number of messages in the transport unreachable queue on this Exchange 2010 server. The Unreachable Queue contains any messages that cannot be routed to their final destination.
Poison Queue	Shows the number of potentially harmful messages on this Exchange 2010 server. Messages that contain content that might be damaging to the Exchange Server system are by default delivered to this Poison Queue and suspended. If messages in this queue are deemed not harmful, message delivery can be resumed, and the message enters the Submission Queue.
Mailbox Delivery Queue	Represents the number of items in the Transport Mailbox Delivery Queue on this Exchange server. The mailbox delivery queue holds messages that are being delivered to mailbox recipients whose mailbox data is stored on a Mailbox server role located in the same site as this Transport server. The next hop for a message in this queue is the distinguished name of the destination mailbox store.
LDAP Search Time (ms)	Shows LDAP Search Time (in milliseconds) for the transport to send an LDAP search request to Active Directory, and receive a response on this Exchange 2010 server. Exchange 2010 uses Active Directory (AD) as a repository for mailbox and mail routing configuration data. Exchange 2010 servers issue LDAP queries against Active Directory to retrieve message routing data.

Transport-Out Panel

The Transport-Out panel groups components that represent current outbound activity from the Exchange 2010 server. This information includes:

Table 5. Exchange 2010 transport-out panel.

Component	Description
Connections	Shows the current number of outbound SMTP connections to other SMTP hosts. The number of connections represents the sum of all SMTP outbound connections from SMTP Send Connectors on this Exchange 2010 server to all remote SMTP domains.
Connectors	Shows the number of SMTP Send connectors on this Exchange 2010 server that can service connections to other SMTP servers.

Table 5. Exchange 2010 transport-out panel.

Component	Description
Remote Delivery Queue	Shows the number of messages in the transport that are queued for delivery to a remote server using SMTP. The Exchange 2010 Hub and Edge roles can have multiple remote delivery queues. Each queue contains messages with recipients that share the same remote server destination.
	On a Hub role server, the destination servers are within the same Exchange Organization as this Exchange server, but in a different AD Site.
	For the Edge role, the destination servers are external to the Organization, and handle message delivery for external SMTP domains.

ClientsI Pane

The Clients panel groups components that represent current client connections and associated latency to this Exchange 2010 server. This information includes:

Table 6. Exchange 2010 clients panel.

Component	Description
MAPI	Indicates the number of MAPI user connections to this Exchange 2010 server. The Mailbox role provides MAPI access for Microsoft Outlook clients, and enables these types of connections.
OWA	Indicates the number of current unique OWA users logged on to this Exchange 2010 server. The Client Access role provides OWA to allow you to access his or her mailbox from a web browser and have full access to all the information in the mailbox including task lists, calendar information, mail items, public folders, UNC shares (\\servername\share) and SharePoint documents. This value is decremented when a you log off your OWA session or the session times out.
ActiveSync	Shows the number of current secure HTTP connections (HTTPS) that are established from Windows Mobile-based or Exchange ActiveSync-enabled mobile devices and this Exchange server. ActiveSync is a push orientated protocol. Data such as user messages, schedules, contact information and tasks are synchronized over the HTTPS connection.
Outlook Anywhere	Shows the number of unique users currently connected to this Exchange 2010 server via RPC/HTTP. The Outlook Anywhere feature, formerly known as RPC over HTTP, lets clients that use Microsoft Office Outlook to connect to their Exchange servers from outside the corporate network or over the Internet using the RPC over HTTP Windows networking component.
POP3	Shows the number of POP3 connections to this Exchange 2010 server. The Client Access role provides POP3 access to mailbox data for clients that rely on this protocol.
IMAP4	Shows the number of IMAP4 connections to this Exchange 2010 server. The Client Access role provides IMAP4 access to mailbox data for clients that rely on this protocol.
Latency (ms) (for MAPI)	Shows the average latency for MAPI clients connected with Outlook to this Exchange 2010 server providing the Mailbox role.
Latency (ms) (for OWA)	Shows the average latency for OWA clients on the Exchange 2010 server.
Latency (ms) (for ActiveSync)	Shows the average latency for ActiveSync clients on the Exchange 2010 server.
Latency (ms) (for POP3)	Shows the average latency for POP3 clients on the Exchange 2010 server.
Latency (ms) (for IMAP4)	Shows the average latency for IMAP4 clients on the Exchange 2010 server.

Information Store Panel

The Information Store panel displays key operational metrics for the information store on this Exchange 2010 server. This information includes:

Table 7. Exchange 2010 information store panel.

Component	Description
Average message delivery time(sec)	Indicates the average time in milliseconds between the submission of a message to the mailbox store and the delivery to all local recipients (recipients on the same server) for the last ten messages.
Clients with RPC (Remote Procedure Calls) latency > 2 sec	Indicates the number of client reported Remote Procedure Calls (RPCs) with a latency greater than two seconds. The most commonly used RPC protocol is MAPI, and a high RPC latency can cause MAPI clients such as Microsoft Outlook to hang and stop responding when users send email, receive email, or use calendar functionality such as creating or viewing appointments.
Average mailbox database size	Indicates the average size of the mailbox database.
Total Logons	Indicates the total number of logons to the information store on this Exchange 2010 server. This includes end-user client connections and system processes that are currently logged-on to any storage group in the local information store. There can be multiple logons per connection for most client applications. As a result, it is possible to see the number of client logons exceed the number of mailboxes on a server.
Average client RPC latency (ms)	Shows the average time (in milliseconds) that it takes the server to respond to RPC connected clients. The average is for the past 1024 packets. The most commonly used RPC protocol is MAPI. A high RPC latency can cause MAPI clients such as Microsoft Outlook to hang and stop responding when users send email, receive email, or use any type of calendar functionality such as creating or viewing appointments.
Mailbox Stores	Shows the percentage of disk space consumed by the mailbox stores on this server. This also shows how much of the server disk consumption is attributable to mailbox store consumption versus other data.
Public Folders	Shows the percentage of public store disk space consumption on this server. This allows you to assess how much of the server disk consumption is attributable to public store data versus other data.
Transaction Logs	Shows the total percentage of disk space consumed by the transaction logs on this server. It can be used to quickly assess how much server disk consumption is attributable to transaction log data versus other data on the Exchange server.
Send Queue	Shows the number of messages in the send queue of the information store. This queue holds all outgoing messages from the information store.
RPC Latency (ms)	Shows the database RPC latency of the Information store. The data is averaged over the past 1024 packets.
DAG Name	Shows the Database Accessibility Group (DAG) name. DAG allows you to replicate your database where your mail is stored across any number of servers.
Store Memory	Shows the total physical memory of the store process.
Mailbox Count	Shows the total number of mailboxes that reside in all mailbox stores and public folders.

OS/Subsystem Panel

The Subsystem panel displays components that represent the health of important subsystem features. This information includes:

Table 8. Exchange 2010 subsystem panel.

Component	Description
Exchange Services	Indicates the sum of CPU utilization for all of the Exchange 2010 services running on this server.
System Disk	Shows the percentage of disk usage for the Windows system disk on this Exchange 2010 server.
CPU Usage	Shows the amount of CPU used on this Exchange 2010 server.
System Memory	Shows the amount of physical memory (RAM) Windows is using. Physical memory usage can normally remain close to the total amount of physical memory installed on the system unless the amount of physical memory exceeds the amount of virtual memory that Windows is using. Windows normally keeps some physical memory available for immediate use.
Ping Time	Indicates the amount of time it takes the computer running the Diagnostic Console to ping the target server.
Top CPU Consumer	Identifies the process that is consuming the most CPU on this Exchange 2010 server.
Top Memory Consumer	Identifies the process that is consuming the most memory on this Exchange 2010 server.

Message Flows

The Exchange 2010 Diagnostic Console contains the following message flows that show the amount of information being sent to various components in your Exchange 2010 environment.

Table 9. Exchange 2010 message flows.

Message Flow	Description
Msgs Submitted/sec	Indicates the rate of messages being submitted per second to this Exchange 2010 transport queues.
Msgs Received/sec	Indicates the rate of messages received by SMTP Receive connector on this Exchange 2010 server.
MAPI Msgs Submitted/sec	Indicates the rate that messages are submitted to the Information Store on the Exchange server by MAPI clients (connected with Outlook).
OWA Msgs Received/sec	Indicates the rate that bytes are received by Exchange server from OWA clients.
ActiveSync Bytes Received/sec	Indicates the rate that bytes are received by Exchange this server from ActiveSync mobile devices.
POP3/IMAP4 Bytes Received/sec	Indicates the number of bytes per second received from POP3 and IMAP4 clients.
Msgs Sent/sec	Indicates the number of messages sent per second to the transport.
Msgs Delivered/sec	Indicates the rate of messages delivered to all recipients with mailboxes on this Exchange 2010 server.
Bytes Received/sec	Indicates the number of bytes received per second from all RPC clients on this Exchange 2010 server information store. RPC clients includes all internal Exchange system components.

Table 9. Exchange 2010 message flows.

Message Flow	Description
Bytes Sent/sec	Indicates the number of bytes sent per second to all RPC clients from this Exchange 2010 server information store. RPC clients includes all internal Exchange system component.
Bytes Read/sec	Indicates the rate at which data is being read from the disk, network, and device subsystems of the Windows server running Exchange. The data is primarily being read from the disk subsystem.
Bytes Written/sec	Indicates the rate at which data is being written to the disk, network, and device subsystems of the Windows server running Exchange. The data is primarily being written to the disk subsystem.
Msgs Queued/sec	Indicates the number of messages queued for delivery per second on this Exchange 2010 server.
Msgs Sent/sec	Indicates the number of outbound messages sent per second by the SMTP send connectors on this transport server.

Drilldowns

Each drilldown page contains displays that provide you with specific information about the components of your system. Drilldowns mainly use two different types of displays — tables and charts. Drilldowns have the following features:

- They can be configured to show all or some of the metrics associated with components.

- You can access further information about displays in drilldowns by moving the mouse over the displays, or by clicking or right-clicking on them.

- You can copy the data shown in drilldowns to other applications or save it to a file.

- You can view a brief description of a drilldown by hovering your mouse over a component, such as a button, dataflow, status ball, or Toolbar button.

To view a drilldown

Right-click a component in a panel and select **Show Details.**

Table 10. Exchange 2010 drilldowns.

Drilldown	Associated charts/tabs
Active Directory Servers	• Active Directory Servers — shows information about the Active Directory servers in use by this Exchange 2010 server. Exchange 2010 stores all configuration and recipient information in the Active Directory directory service database. All Exchange 2010 roles use Active Directory except the Edge role, which does not have access to Active Directory. The Edge role uses Active Directory Application Mode (ADAM) to store schema and configuration information.
	• Active Directory Servers Details — shows information about the currently selected Active Directory. Exchange 2010 stores all configuration and recipient information in the Active Directory directory service database. All Exchange 2010 roles use Active Directory except the Edge role which does not have access to Active Directory. The Edge role uses ADAM to store schema and configuration information.

Table 10. Exchange 2010 drilldowns.

Drilldown	Associated charts/tabs
DNS Servers	• DNS Servers — shows information about the DNS servers in use by this Exchange 2010 server. The Exchange 2010 server uses the DNS server that is configured in the IP properties of the network adapter to locate domain controllers and global catalog servers, other Exchange servers, and remote domains. DNS lookup settings can be specified on the Hub Transport server, which override the settings on the network adapter to route messages.
Transport In/Transport/Transport Out	• Inbound Connections — shows the total number of inbound SMTP connections established by other SMTP hosts to this Exchange server • Outbound Connections — shows the current number of outbound SMTP connections to other SMTP hosts • Inbound Connectors — shows the number of SMTP Receive connectors on this Exchange 2010 server that are required to accept mail from other SMTP servers • Outbound Connectors — shows the number of SMTP Send connectors on this Exchange 2010 server that are required to handle connections to other SMTP servers • LDAP Search Time — shows LDAP Search Time (in ms) that is taken to send an LDAP search request and receive a response on this Exchange 2010 server • Transport Queues — shows the number of messages in the transport queues on this Exchange 2010 server
Clients	• MAPI — indicates the number of MAPI connections to this Exchange 2010 server. The Mailbox role provides MAPI access to Microsoft Outlook clients. • OWA — indicates the number of OWA connections to this Exchange 2010 server. The Client Access role provides OWA to allow a you to access to your mailbox information through a web browser. • ActiveSync — shows the number of ActiveSync connections to this Exchange 2010 server. The Client Access role uses ActiveSync to allow mailbox access from mobile devices. • POP3 — shows the number of POP3 connections to this Exchange 2010 server. The Client Access role provides POP3 access to mailbox data for clients that rely on this protocol. • IMAP4 — shows the number of IMAP4 connections to this Exchange 2010 server. The Client Access role provides IMAP4 access to mailbox data for clients that rely on this protocol. • Outlook Anywhere — shows the number of unique users currently connected to this Exchange 2010 server via RPC/HTTP.
Information Store	• Average Message Delivery Time — indicates the average time in seconds between the submission of a message to the mailbox store and the delivery to all local recipients (recipients on the same server) for the last 10 messages. • Total Logons — indicates the number of clients (including system processes) currently logged to any storage group in the information store. • Clients with RPC Latency > 2 sec – indicates the number of client reported RPCs (Remote Procedure Calls) with a latency greater than two seconds. • Average Client RPC Latency — shows the average time (in milliseconds) that it takes the server to respond to RPC connected clients.

Table 10. Exchange 2010 drilldowns.

Drilldown	Associated charts/tabs
Exchange Mailbox Databases	• Transaction Log Free Space — shows the amount of free space on the transaction log disk with the least amount of free space on the server. There should be enough free disk space to accommodate foreseeable future growth in the transaction logs. If circular logging is turned off on the transaction logs, there should be enough free space to accommodate at least 25% of the current transaction log size. • Database Free Space — shows the amount of free space on the store disk with the least amount of free space on the server. There should be enough free disk space to accommodate foreseeable future growth in the mailbox store(s) and to defragment any store on this server. • Database Mount Status — shows the mount status of the mailbox stores on the server. Mailboxes contained in unmounted mailbox stores cannot receive incoming messages. • Exchange Mailbox Database List — shows information such as status, Database Name, Logons Currently Hosted, and Database Path for Exchange 2010 servers.
Exchange Services	• Exchange Services List — lists the Exchange services that are running on this Exchange 2010 server. Both required and optional services for the roles installed on this Exchange server are listed, along with their service status. • Service Details — shows the CPU and memory usage of the currently selected Exchange 2010 service.
Subsystem	• CPU Usage — indicates the processor CPU usage on this Exchange 2010 server. • System Memory — shows the amount of physical memory (RAM) Windows is using. • System Disk — shows the amount of used and free space on the Windows system disk on this Exchange 2010 server. • Ping Time — shows the ping time (in milliseconds) from the UC Diagnostics client to the Exchange 2010 server.
Processes	• Process Name — indicates the image name of the application itself. • CPU Usage — indicates the percentage of CPU time that the program is currently consuming. This is an instantaneous result. • Physical Memory — indicates the current size of the working set of the process. • Virtual Memory — indicates current memory allocated to this process that cannot be shared with other processes.

Metrics

A metric is an individual piece of information that UC Diagnostics has collected about the performance of a system, such as perfmon counters. The information may be a numeric value (a number or percentage), a string of text, or some other piece of data.

To view the perfmon counters

• Right-click a component and select **Metrics**.

The perfmon counter is visible in the Metric help section in the General tab.

Every time that the UC Diagnostics window is refreshed, UC Diagnostics retrieves the latest value of the metric, which can then be displayed in a drilldown or on the home page.

The Metric editor allows you to view and edit the properties of UC Diagnostics metrics, including their thresholds and severities. You can open the Metric editor for a component or a drilldown by right-clicking on the component and choosing Metrics from the invoked shortcut menu.

When you open the Metric editor, the General tab is open by default. Several metrics contain data source descriptions for the metric. The data source descriptions use the following list of functions.

Table 11. Exchange 2010 metrics.

Function	Description
max(x)	the maximum of a set of values in list x
max(x,y)	the maximum of x and y
min(x)	the minimum of a set of values in list x
count(x)	the number of values in list x
sum(x)	the sum of a set of values in list x
if(x,y,z)	if x is true, then return y, otherwise, return z
snull(x)	if x could not be collected, then return true
avg(x)	the average of values in list x

Diagnosing Exchange 2013 with the Diagnostic Console (Plug In)

- Introducing the Exchange 2013 Diagnostic Console
- Understanding the Exchange 2013 Diagnostic Console
- Panels
- Message Flows
- Drilldowns
- Metrics

Introducing the Exchange 2013 Diagnostic Console

The Exchange 2013 Diagnostic Console provides a real-time representation of the messaging system processes and components within specific connected Exchange 2013 servers. You can diagnose and resolve issues using the Exchange 2013 Diagnostic Console.

The Exchange 2013 Diagnostic Console contains the following:

- Home pages that highlight targeted areas of the Exchange 2013 server activity.
- Graphical flows that illustrate the rate at which data is moving between server components. Colorful buttons, gauges, queues, spinners, and containers display the value of key statistics and metrics.
- Visual warnings if the performance metrics exceed acceptable thresholds, which you can adjust. The buttons, gauges, queues, and other visual objects, collectively referred to as components, change color to show you the source of the problem.
- Warning messages that are displayed well before the traffic levels of a server become critical.
- A range of reports and graphs that provide you with detailed information about a server. You can view this information on the screen or you can print it.

Understanding the Exchange 2013 Diagnostic Console

When you connect to the Exchange 2013 Diagnostic Console, the home page displays a high level summary of your Exchange 2013 server.

The home page contains the various panels, message flows, and drilldowns to help you perform an extensive analysis of the major components on your Exchange 2013 server.

To view detailed information on specific components, right-click a component, message flow, and drilldown, and select What's This, Metrics, or Properties.

Exchange Diagnostic Console Recommendations

The Exchange Diagnostic Console provides you with a real-time representation of the messaging system processes and components within Exchange.

The Diagnostic Console retrieves a large amount of data from a server frequently, which can place excessive stress on a server, actually affecting the server's performance. Also, using the Diagnostic Console for an extended period of time can consume critical system resources, affecting the stability of UC Diagnostics as a whole.

Quest recommends the following:

- Allow the Diagnostic Console view a maximum number of 10 servers at any one time.

- If you are using the Diagnostic Console as a monitoring tool, you must disconnect from and reconnect to the Diagnostic Console daily. Though the Management Console can run tests when closed, the Diagnostic Console cannot perform any actions when it is closed.

- If you install the Diagnostic Console on a computer that contains Spotlight products and you want to launch the Diagnostic Console from the UC Diagnostics Management Console, the Diagnostic Console and the Spotlight products must be installed on the C: drive. Otherwise, the Diagnostic Console fails to launch from the Management Console. As a workaround, create a shortcut on your desktop to C:\Program Files\Quest\Spotlight\Console\Spotlight.exe to manually open connections.

For information about the Exchange software prerequisites, Exchange required configuration, and the permissions needed by the credentials to access Exchange, see the *Unified Communications Diagnostics Deployment Guide*.

Panels

The Exchange 2013 Diagnostic Console contains the following panels:

- AD/DNS Panel
- Server Roles Panel
- Clients Panel
- Client Access Server (CAS)
- Mailbox Server (MBX) Transport Panel
- Mailbox Server (MBX) Information Store Panel
- OS/ Subsystem Panel

AD/DNS Panel

The components of the Directory Services panel indicate how Exchange 2013 interacts with directory services. This information includes:

Table 1. Exchange 2013 AD/DNS panel.

Component	Description
AD	Shows the status of the Active Directory (AD) servers used by this Exchange 2013 server. It will check the following conditions (non-edge Exchange servers only): • If the domain controller is local to this Exchange 2013 server's AD site. • If the domain controller is synchronized with the rest of the forest. • The average LDAP Search Time (in msec) for all queries made against that domain controller. • The number of LDAP Search Timeouts for all queries made against that domain controller. • The ping time between the client (UC Diagnostics) and the domain controller. • If the domain controller is available on the network (from this client computer).
DNS	Shows the status about the Domain Name System (DNS) servers in use by this Exchange 2013 server. It will check the following conditions: • The ping time between the client (the Diagnostic Console) and the DNS server • If the DNS server can be reached on the network from this client

Server Roles Panel

The components of the Server Roles panel shows the Exchange 2013 roles that are installed. This information includes:

Table 2. Exchange 2013 server roles panel.

Component	Description
MBX	Shows whether the Mailbox role is installed on this Exchange 2013 server. The Mailbox role stores mailbox data, performs processing and rendering for client connections proxied by the Client Access server, and handles Unified Messaging requests. Mailbox servers can be organized into back-end clusters that use database availability groups (DAGs).
CAS	Shows whether the Client Access role is installed on this Exchange 2013 server. The Client Access role proxies connectivity for all clients, such as Microsoft Office Outlook, Outlook Web App, mobile devices, POP, and SMTP and also accepts mail from and delivers mail to other mail hosts on the Internet. Client access servers can be organized into Client Access server arrays.
EDG	Shows whether the Edge Transport role is installed on this Exchange 2013 server. Edge Transport servers handle the following functions: • Provide the rules that control mail flow and protect against spam as mail enters and leaves the organization. • Process all the external mail flow for the Exchange organization.

Clients Panel

The Clients panel groups components that represent current client connections to this Exchange 2013 server. This information includes:

Table 3. Exchange 2013 clients panel.

Component	Description
OWA	Indicates the number of current Outlook Web Access (OWA) users logged on to this Exchange 2013 server. The Client Access role provides OWA to allow you to access your mailbox from a web browser and have full access to all the information in the mailbox including task lists, calendar information, mail items, public folders, UNC shares and SharePoint documents. This value is decremented when users log out of their OWA session, or the session times out.
Outlook	Shows the number of users currently connected to this Exchange 2013 server through RPC over HTTP. In Microsoft Exchange Server 2013, the Outlook Anywhere feature, formerly known as RPC over HTTP, lets clients that use Microsoft Office Outlook to connect to their Exchange servers from outside the corporate network or over the Internet using the RPC over HTTP Windows networking component.
ActiveSync	Shows the number of current secure HTTP connections (HTTPS) that are established from Windows Mobile-based or Exchange ActiveSync-enabled mobile devices to this Exchange 2013 server. ActiveSync is a push-orientated protocol. Data such as user messages, schedules, contact information, and tasks are synchronized over the HTTPS connection.
Web Service	Shows the current number of connections with the World Wide Web Publishing Service (W3SVC) for this Exchange 2013 server. This information can help you determine if your server can handle the current user load.
IMAP4	Shows the number of IMAP4 connections to this Exchange 2013 server. The Client Access role provides IMAP4 access to mailbox data for clients that rely on this protocol. IMAP4 is an Internet messaging protocol that allows you to access mail on a server or download it to your computer. IMAP4 is designed for an environment where you can log on to the server from a variety of different workstations or across slow links. The IMAP4 protocol is disabled by default on Exchange 2013 server. If this Exchange server needs to support IMAP4 clients, start the IMAP4 service. Otherwise, leave it disabled for security reasons.
POP3	Shows the number of POP3 connections to this Exchange 2013 server. POP3 is an Internet messaging protocol that supports simple offline mail processing. POP3 allows you to download e-mail messages from the server and store them locally on a client computer. By default, POP3 is not enabled. If POP3 is required, start the service. If this Exchange server does not need to support POP3 clients, leave it disabled for security reasons.
UM Clients	Shows the number of voice mail calls that are currently connected to the Unified Messaging Server since the service was started.

Client Access Server (CAS)

The CAS panel groups components that represent current connections on the CAS server on this Exchange 2013 server. This information includes SMTP connection information. SMTP is the standard protocol for Internet Mail.

Exchange 2013 has an updated SMTP protocol and transport stack that does not depend on IIS. Exchange 2013 uses SMTP protocol for server-to-server message delivery within the same Active Directory site or Routing Group, between different Exchange Organizations, and when transferring mail to other email systems. This information includes:

Table 4. Exchange 2013 CAS panel.

Component	Description
Front-End Transport Service	Shows the CPU Usage for the Front-End Transport Service (in %).
	The Transportation Role is split into two parts in Exchange 2013: Front-End Transport Service (located in the Client Access Server) and Transport Service (located in the Mailbox Server).
SMTP Inbound Connections	Shows the total number of inbound SMTP connections established by other SMTP hosts to this Exchange server. The number of connections represents the sum of all SMTP inbound connections from all remote domains to SMTP Receive Connectors on this Exchange 2013 server.
	SMTP is the standard protocol for Internet Mail. Exchange 2013 has an updated SMTP protocol and transport stack that does not depend on IIS. Exchange 2013 uses SMTP protocol for server-to-server message delivery within the same Active Directory site or Routing Group, between different Exchange Organizations, and when transferring mail to other email systems.
HTTP/Proxy Outstanding Requests	Shows the quantity of concurrent outstanding proxy requests for the Microsoft Exchange HTTP Proxy access.
Avg. Authentication Latency (ms)	Shows the average time spent in authenticating CAS requests in the past 200 samples.
Avg. RPC Latency (sec)	Shows the average latency in seconds of RPC requests. Average is calculated over all RPCs since exrpc32 was loaded.
IIS Service	Shows the CPU Usage for World Wide Web Publishing Service (in %).
	Exchange Server depends on the Microsoft Internet Information Services (IIS) in order to connect using HTTP. To keep email communication flowing, the IIS Service must be running properly. If the IIS Service (W3SVC) is down, some Exchange 2013 specific functionality such as ECP, EWS, Autodiscover, ActiveSync, OWA, and PowerShell will be affected.
SMTP Outbound Connections	Shows the current number of outbound SMTP connections to other SMTP hosts. The number of connections represents the sum of all SMTP outbound connections from SMTP Send Connectors on this Exchange 2013 server to all remote SMTP domains.
	SMTP is the standard protocol for Internet Mail. Exchange 2013 has an updated SMTP protocol and transport stack that does not depend on IIS. Exchange 2013 uses SMTP protocol for server-to-server message delivery within the same Active Directory site or Routing Group, between different Exchange Organizations, and when transferring mail to other email systems.
Users at Max Concurrency	Shows the total quantity of the users that attain Maximum Connections Limitation.
Proxy Failure Rate	Shows the percentage of the connectivity related to the failures between the CAS servers and MBX servers in the past 200 samples.
LDAP Search Time (ms)	Shows the time to send an LDAP search request and receive a response (in milliseconds).
Inbound Connectors	Shows the number of SMTP Receive connectors on this Exchange 2013 server that can accept mail from other SMTP servers.
	SMTP Receive Connectors provide the ability for a Mailbox role to receive email from any other SMTP server on the Internet, other Exchange Server 2013 Mailbox server roles, or other Exchange Server 2013 organizations. Exchange 2013 Servers can have multiple SMTP Receive connectors with different parameters for availability or performance reasons.

Table 4. Exchange 2013 CAS panel.

Component	Description
Outbound Connectors	Shows the number of SMTP Send connectors on this Exchange 2013 server that can send connections to other SMTP servers.
	An SMTP Send connector is required for an Exchange Server 2013 to send any SMTP email to other SMTP server on the Internet or to any SMTP server within the same Exchange Server organization. More than one Exchange Mailbox server can use a Send Connector for routing purposes. The Send Connector properties in the Exchange Management Console show which Exchange Mailbox Servers in the same site can use this Send Connector through which to route mail.

Mailbox Server (MBX) Transport Panel

The Mailbox Server (MBX) Transport panel groups components that identify the status of the various transport queues on the mailbox server on this Exchange 2013 server. The Transportation Role is split into two parts in Exchange 2013: Mailbox Transport service and Front-End Transport service.

The Mailbox Transport service runs on all Exchange 2013 Mailbox servers and consists of two separate services:

- Mailbox Transport Delivery service receives the SMTP messages from the Transport service which is running on the local Exchange 2013 Mailbox server or other Exchange 2013 Mailbox servers.
- Mailbox Transport Submission service, which runs on the Exchange 2013 Mailbox server, that connects to a local mailbox database using RPC to retrieve messages.

Exchange 2013 has an updated SMTP protocol and transport stack that does not depend on IIS. Exchange 2013 uses SMTP protocol for server-to-server message delivery within the same Active Directory site or Routing Group, between different Exchange Organizations, and when transferring mail to other email systems.

Table 5. Exchange 2013 mailbox server transport panel

Component	Description
Inbound Connections	Shows the total number of inbound SMTP connections established by other SMTP hosts to this Exchange server. The number of connections represents the sum of all SMTP inbound connections from all remote domains to SMTP Receive Connectors on this Exchange 2013 server.
	SMTP is the standard protocol for Internet Mail. Exchange 2013 has an updated SMTP protocol and transport stack that does not depend on IIS. Exchange 2013 uses SMTP protocol for server-to-server message delivery within the same Active Directory site or Routing Group, between different Exchange Organizations, and when transferring mail to other email systems.
Outbound Connections	Shows the current number of outbound SMTP connections to other SMTP hosts. The number of connections represents the sum of all SMTP outbound connections from SMTP Send Connectors on this Exchange 2013 server to all remote SMTP domains.
	SMTP is the standard protocol for Internet Mail. Exchange 2013 has an updated SMTP protocol and transport stack that does not depend on IIS. Exchange 2013 uses SMTP protocol for server-to-server message delivery within the same Active Directory site or Routing Group, between different Exchange Organizations, and when transferring mail to other email systems.
EWS Response Time	Shows the average response time for the Exchange Web Services (EWS) which is running on the Exchange 2013 Mailbox Server.
	The Exchange Web Services (EWS) provides the functionality to enable Client Applications to communicate with the Exchange 2013 servers. It also provides the access to much of the same data, which is made available through the Microsoft Office Outlook.

Table 5. Exchange 2013 mailbox server transport panel

Component	Description
Transport Service	Shows the CPU usage for the Exchange Transport Service (in %).
	The Transport service runs on all Exchange 2013 Mailbox servers and is similar to the Hub Transport server role in previous Exchange versions. This service handles all the inside and outside SMTP mail flow for the entire Exchange 2013 organization. Each SMTP message must be categorized and content-inspected in the Transport service before it can be routed and delivered. After the messages are categorized, they are put in a delivery queue to await delivery to the destination.
	Unlike Exchange 2010 or earlier, the Transport service does not communicate with mailbox databases directly. That task is handled by the Mailbox Transport service. The Transport service routes SMTP messages between the Front-End Transport service which runs on all CAS servers, the Transport service, and the Mailbox Transport service
Transport Delivery Service	This shows the CPU usage for the Exchange Mailbox Transport Delivery service (in %).
	The Exchange Mailbox Transport Delivery service runs on all Exchange 2013 Mailbox servers. It is a separate service from the Mailbox Transport service.
	The Mailbox Transport Delivery service receives the SMTP messages from the Transport service on the local Exchange 2013 Mailbox servers or on the other Exchange 2013 Mailbox servers. The service uses an Exchange remote procedure call (RPC) to connect to a local mailbox database to deliver the messages. The Mailbox Transport Delivery service does not queue messages locally.
ActiveSync Pending	Shows the number of pending Sync commands on the Exchange 2013 Mailbox Server currently.
ActiveSync Request Time	Shows the average request time for the ActiveSync on this Exchange 2013 Mailbox Server.
	This Average Request Time is the average time that elapsed, in milliseconds, waiting for a request to be completed in this Mailbox Server.
Transport Submission Service	Shows the CPU usage for the Exchange Mailbox Transport Submission Service (in %).
	The Exchange Mailbox Transport Submission service runs on all Exchange 2013 Mailbox servers. It is a separate service from the Mailbox Transport service.
	The Mailbox Transport Submission service uses an Exchange remote procedure call (RPC) to connect to a local mailbox database to retrieve messages. The service submits the messages over SMTP to the Transport service that is running on the local Exchange 2013 Mailbox server or on the other Exchange 2013 Mailbox servers. The service has access to the same routing topology information as the Transport service. The Mailbox Transport Submission service does not queue messages locally.
Unreachable Queue	Shows the number of messages in the transport unreachable queue on this Exchange 2013 server. The Unreachable Queue contains any messages that cannot be routed to their final destination.
Poison Queue	Shows the number of potentially harmful messages on this Exchange 2013 server. Messages that contain content that might be damaging to the Exchange Server system are by default delivered to this Poison Queue and suspended. If messages in this queue are deemed not harmful, message delivery can be resumed, and the message enters the Submission Queue.

Table 5. Exchange 2013 mailbox server transport panel

Component	Description
Delivery Queue	Shows the number of items in the Transport Mailbox Delivery Queue on this Exchange server. The Mailbox Delivery Queue holds messages that are being delivered to mailbox recipients whose mailbox data is stored on a Mailbox Server Role located in the same site as this Transport server. The next hop for a message in this queue is the distinguished name of the destination mailbox store. A different mailbox delivery queue exists for each Mailbox server destination. Mailbox delivery queues are created as needed and automatically removed.
Submission Queue	Shows the number of items in the Submission queue. The Submission queue holds messages before they are consumed by the Categorizer which determines what to do with the messages based on information about the intended recipients. After the Submission queue, the Categorizer then routes the message to either a CAS Server role, another Mailbox server in a different AD Site, a mailbox on an Exchange server, or the Unreachable queue.

Mailbox Server (MBX) Information Store Panel

The Mailbox Server (MBX) Information Store Panel displays key operational metrics for the information store on this Exchange 2013 server. This information includes:

Table 6. Exchange 2013 mailbox server information store panel.

Component	Description
Public Folder	Shows the number of the public folder which are located in the Exchange 2013 Mailbox Server. In order to take advantage of the high availability and the storage technologies of the mailbox database, Microsoft Exchange 2013 Public Folders have been modernized. The specially designed mailboxes have been used to store both the public folder content and the hierarchy in the Public Folder architecture. There's no a public folder database any more. In Exchange 2013, the Public Folder replication uses continuous replication model. The content mailboxes and the high availability for the hierarchy are provided by database availability group (DAG).
Public Folder Mailbox	Shows the number of the public folder mailboxes which are located on the Exchange 2013 Mailbox Server. The Exchange 2013 Public folder mailboxes contain the information about the hierarchy for a public folder, and the actual content is contained in the Exchange 2013 public folder. When you create a public folder, the first public folder mailbox will become the master hierarchy mailbox. Public folder hierarchy mailbox subsequently created will become a secondary mailbox.
DAG	Shows the name of the Database Availability Group to which this Exchange 2013 server belongs. This is shown for informational purposes only. View the Mailbox Databases drilldown to see more information about the mailbox databases installed on this server.
Replication Service	Shows the Exchange 2013 Replication Service Status.

Table 6. Exchange 2013 mailbox server information store panel.

Component	Description
Store Worker Process	Shows the CPU Utilization of the Microsoft.Exchange.Store.Worker Service in Exchange 2013 Mailbox Server. In Exchange 2013, the information store is now called Managed Store, which has two processes: • Microsoft.Exchange.Store.Service.exe • Microsoft.Exchange.Store.Worker.exe Each database is running under its own process, which isolates the stores issues to a single database. Working with the Microsoft Exchange Replication service, Managed Store manages the mailbox databases and uses the Extensible Storage Engine (ESE) as the database engine. This architectural changes enable faster database failover and better physical disk failure handling.
Mailbox Counts	Shows the total number of mailboxes that reside in all mailbox stores. This is shown for informational purposes only.
Store Service Process	Shows the CPU Utilization of the Microsoft.Exchange.Store.Service Service in Exchange 2013 Mailbox Server. In Exchange 2013, the information store is now called Managed Store, which has two processes as below: • Microsoft.Exchange.Store.Service.exe • Microsoft.Exchange.Store.Worker.exe Each database is running under its own process, which isolates the stores issues to a single database. Working with the Microsoft Exchange Replication service, Managed Store manages the mailbox databases and uses the Extensible Storage Engine (ESE) as the database engine. This architectural changes enable faster database failover and better physical disk failure handling.
Mailbox Databases	Shows the percentage of disk space consumed by the mailbox stores on this server. This also shows how much of the server disk consumption is caused by mailbox store consumption versus other data.
Transaction Logs	Shows the total percentage of disk space consumed by the transaction logs on this server. It can be used to quickly assess how much server disk is consumed by transaction log data versus other data on the Exchange server.

OS/ Subsystem Panel

The Subsystem panel displays components that represent the health of important subsystem features. This information includes:

Table 7. Exchange 2013 subsystem panel.

Component	Description
CPU Usage	Shows the amount of CPU used on this Exchange 2013 server.
System Disk	Shows the percentage of disk usage for the Windows system disk on this Exchange 2013 server.
System Memory	Shows the amount of physical memory (RAM) Windows is using. Physical memory usage can normally remain close to the total amount of physical memory installed on the system unless the amount of physical memory exceeds the amount of virtual memory that Windows is using. Windows normally keeps some physical memory available for immediate use.
Ping Time	Shows the ping time (in milliseconds) from the client (UC Diagnostics) to the Exchange 2013 server.

Table 7. Exchange 2013 subsystem panel.

Component	Description
Top CPU Consumer	Identifies the process that is consuming the most CPU on this Exchange 2013 server.
Top Memory Consumer	Identifies the process that is consuming the most memory on this Exchange 2013 server.

Message Flows

The Exchange 2013 Diagnostic Console contains the following message flows that show the amount of information being sent to various components in your Exchange 2013 environment.

Table 8. Exchange 2013 message flows panel.

Message Flow	Description
HTTP Proxy Requests/sec	Shows the rate of the HTTP Proxy requests per second.
Inbound Msgs/Sec	Shows the number of messages (sent inbound into the forest) received by the SMTP server each second.
Msgs Sent/sec	Shows the number of messages sent by the SMTP Send connector per second.
Msgs Received/sec	Shows the rate of messages received by SMTP Receive connector on this Exchange 2013 server. The SMTP Receive connector is part of the Microsoft Exchange Transport service on Exchange 2013 holding Mailbox server roles. It controls message processing through a series of SMTP Receive agents performing anti-spam, antivirus, and other tasks before messages are submitted to the categorizer.
Messages Sent/sec	Shows the rate of messages delivered to the mailbox database using Exchange Remote Procedure Call (RPC).
Messages Submitted/sec	Shows the rate of retrieving messages from Mailbox database using Exchange Remote Procedure Call (RPC).
Bytes Written/sec	Shows the Process IO Write Bytes / Sec on the CAS Server through MSExchangeFrontendTransport.
Bytes Read/sec	Shows the Process IO Read Bytes / Sec on the CAS Server through MSExchangeFrontendTransport.
Bytes Read/sec	Shows the rate at which data is being read from the disk, network, and device subsystems of the Windows server running Exchange. The data is primarily read from the disk subsystem.
Bytes Written/sec	Shows the rate at which data is being written to the disk, network, and device subsystems of the Windows server running Exchange. The data is primarily written to the disk subsystem.

Drilldowns

Each drilldown page contains displays that provide you with specific information about the components of your system. Drilldowns mainly use two different types of displays — tables and charts. Drilldowns have the following features:

- They can be configured to show all or some of the metrics associated with components.
- You can access further information about displays in drilldowns by moving the mouse over the displays, or by clicking or right-clicking on them.

- You can copy the data shown in drilldowns to other applications or save it to a file.

- You can view a brief description of a drilldown by hovering your mouse over a component, such as a button, dataflow, status ball, or Toolbar button.

To view a drilldown

Right-click a component in a panel and select **Show Details.**

Table 9. Exchange 2013 drilldowns.

Drilldown	Associated Charts/Tabs
Active Directory Server	• Active Directory Servers - shows information about the Active Directory servers in use by this Exchange 2013 server. Exchange 2013 stores all configuration and recipient information in the Active Directory directory service database. • Active Directory Server Details - Shows information about selected Active Directory Server. Exchange 2013 stores all configuration and recipient information in the Active Directory directory service database.
DNS Servers	• DNS Servers - Shows information about the Domain Name System (DNS) Servers used by this Exchange 2013 server. The Exchange 2013 server uses the DNS server that is configured in the IP properties of the network adapter to locate domain controllers and global catalog servers, other Exchange servers, and remote domains. DNS lookup settings can be specified on the Hub Transport server, which override the settings on the network adapter to route messages.
Clients	You can drilldown to more detailed information for the following clients: • OWA • ActiveSync • IMAP4 • UM Clients • Outlook • Web Service • POP3 For more information, see Clients Panel on page 133.
Exchange Services	You can drilldown to more detailed information for the following services: • Front-End Transport Service • Transport Submission Service • IIS Service • Mailbox Transport Service - • Transport Delivery Service • Store Service For more information, see Mailbox Server (MBX) Transport Panel on page 135.
Client Access Server (CAS)	You can drilldown to more detailed information for the following components: • SMTP Inbound Connections • HTTP/Proxy Outstanding Requests • Avg. Authentication Latency • Avg. RPC Latency • SMTP Outbound Connections • Users at Max Concurrency • Proxy Failure Rate • LDAP Search Time For more information, see Client Access Server (CAS) on page 133.

Table 9. Exchange 2013 drilldowns.

Drilldown	Associated Charts/Tabs
Mailbox Server (MBX) Transport	You can drilldown to more detailed information for the following components: • Inbound Connections • Outbound Connections • ActiveSync Pending • ActiveSync Request Time • Unreachable Queue • EWS Response Time • Poison Queue • Delivery Queue • Submission Queue For more information, see Mailbox Server (MBX) Transport Panel on page 135.
Mailbox Server (MBX) Information Store	• Public Folder List - shows information about the public folders on this Exchange 2013 server. • Public folder Mailbox List - shows the information of the public folder mailboxes. • Exchange Database Information - shows information about the databases on this Exchange 2013 server, such as Transaction Log Free Space, Database Free Space, and Database Mount Status.
Subsystem	You can drilldown to more detailed information for the following components: • CPU Usage • System Disk • System Memory • Ping Time For more information, see OS/ Subsystem Panel on page 138.
Processes	• Process Name — indicates the image name of the application itself. • CPU Usage — indicates the percentage of CPU time that the program is currently consuming. This is an instantaneous result. • Physical Memory — indicates the current size of the working set of the process. • Virtual Memory — indicates current memory allocated to this process that cannot be shared with other processes.

Metrics

A metric is an individual piece of information that UC Diagnostics has collected about the performance of a system, such as perfmon counters. The information may be a numeric value (a number or percentage), a string of text, or some other piece of data.

To view the perfmon counters

• Right-click a component and select **Metrics**.

The perfmon counter is visible in the Metric help section in the General tab.

Every time that the UC Diagnostics window is refreshed, UC Diagnostics retrieves the latest value of the metric, which can then be displayed in a drilldown or on the home page.

The Metric editor allows you to view and edit the properties of UC Diagnostics metrics, including their thresholds and severities. You can open the Metric editor for a component or a drilldown by right-clicking on the component and choosing Metrics from the invoked shortcut menu.

When you open the Metric editor, the General tab is open by default. Several metrics contain data source descriptions for the metric. The data source descriptions use the following list of functions.

Table 10. Exchange 2013 metrics.

Function	Description
max(x)	the maximum of a set of values in list x
max(x,y)	the maximum of x and y
min(x)	the minimum of a set of values in list x
count(x)	the number of values in list x
sum(x)	the sum of a set of values in list x
if(x,y,z)	if x is true, then return y, otherwise, return z
snull(x)	if x could not be collected, then return true
avg(x)	the average of values in list x

Diagnosing Exchange 2016 with the Diagnostic Console (Plug In)

- Introducing the Exchange 2016 Diagnostic Console
- Understanding the Exchange 2016 Diagnostic Console
- Panels
- Message Flows
- Drilldowns
- Metrics

Introducing the Exchange 2016 Diagnostic Console

The Exchange 2016 Diagnostic Console provides a real-time representation of the messaging system processes and components within specific connected Exchange 2016 servers. You can diagnose and resolve issues using the Exchange 2016 Diagnostic Console.

The Exchange 2016 Diagnostic Console contains the following:

- Home pages that highlight targeted areas of the Exchange 2016 server activity.
- Graphical flows that illustrate the rate at which data is moving between server components. Colorful buttons, gauges, queues, spinners, and containers display the value of key statistics and metrics.
- Visual warnings if the performance metrics exceed acceptable thresholds, which you can adjust. The buttons, gauges, queues, and other visual objects, collectively referred to as components, change color to show you the source of the problem.
- Warning messages that are displayed well before the traffic levels of a server become critical.
- A range of reports and graphs that provide you with detailed information about a server. You can view this information on the screen or you can print it.

Understanding the Exchange 2016 Diagnostic Console

When you connect to the Exchange 2016 Diagnostic Console, the home page displays a high level summary of your Exchange 2016 server.

The home page contains the various panels, message flows, and drilldowns to help you perform an extensive analysis of the major components on your Exchange 2016 server.

To view detailed information on specific components, right-click a component, message flow, and drilldown, and select What's This, Metrics, or Properties.

Exchange Diagnostic Console Recommendations

The Exchange Diagnostic Console provides you with a real-time representation of the messaging system processes and components within Exchange.

The Diagnostic Console retrieves a large amount of data from a server frequently, which can place excessive stress on a server, actually affecting the server's performance. Also, using the Diagnostic Console for an extended period of time can consume critical system resources, affecting the stability of UC Diagnostics as a whole.

Quest recommends the following:

- Allow the Diagnostic Console view a maximum number of 10 servers at any one time.

- If you are using the Diagnostic Console as a monitoring tool, you must disconnect from and reconnect to the Diagnostic Console daily. Though the Management Console can run tests when closed, the Diagnostic Console cannot perform any actions when it is closed.

- If you install the Diagnostic Console on a computer that contains Spotlight products and you want to launch the Diagnostic Console from the UC Diagnostics Management Console, the Diagnostic Console and the Spotlight products must be installed on the C: drive. Otherwise, the Diagnostic Console fails to launch from the Management Console. As a workaround, create a shortcut on your desktop to C:\Program Files\Quest\Spotlight\Console\Spotlight.exe to manually open connections.

For information about the Exchange software prerequisites, Exchange required configuration, and the permissions needed by the credentials to access Exchange, see the *Unified Communications Diagnostics Deployment Guide*.

Panels

The Exchange 2016 Diagnostic Console contains the following panels:

- AD/DNS Panel
- Server Roles Panel
- Clients Panel
- Client Access Services Panel
- Transport Panel
- Information Store Panel
- OS/ Subsystem Panel

AD/DNS Panel

The components of the Directory Services panel indicate how Exchange 2016 interacts with directory services. This information includes:

Table 1. Exchange 2016 AD/DNS panel.

Component	Description
AD	Shows the status of the Active Directory (AD) servers used by this Exchange 2016 server and checks the following conditions (non-edge Exchange servers only): • If the domain controller is local to this Exchange 2016 server's AD site. • If the domain controller is synchronized with the rest of the forest. • The average LDAP Search Time (in msec) for all queries made against that domain controller. • The number of LDAP Search Timeouts for all queries made against that domain controller. • The ping time between the client (UC Diagnostics) and the domain controller. • If the domain controller is available on the network (from this client computer).
DNS	Shows the status about the Domain Name System (DNS) servers in use by this Exchange 2016 server and checks the following conditions: • The ping time between the client (the Diagnostic Console) and the DNS server • If the DNS server can be reached on the network from this client

Server Roles Panel

The components of the Server Roles panel shows the Exchange 2016 roles that are installed. This information includes:

Table 2. Exchange 2016 server roles panel.

Component	Description
MBX	Shows whether the Mailbox role is installed on this Exchange 2016 server. Mailbox servers contain following components: • Mailbox databases that process, display, and store the mailbox data. • Client access services that handle all the client connections to the Exchange server. • Transport services that are used to transfer and route the email messages. • Unified Messaging (UM) services that deliver voice mail and related telephony services to mailboxes Mailbox servers can be organized into back-end clusters that use database availability groups (DAGs).
EDG	Shows whether the Edge Transport role is installed on this Exchange 2016 server. Edge Transport servers handle the following functions: • Provide the rules that control mail flow and protect against spam as mail enters and leaves the organization. • Process all the external mail flow for the Exchange organization.

Clients Panel

The Clients panel groups components that represent current client connections to this Exchange 2016 server. This information includes:

Table 3. Exchange 2016 clients panel.

Component	Description
Outlook	Shows the number of users currently connected to this Exchange 2016 server through RPC over HTTP. In Microsoft Exchange Server 2016, the Outlook Anywhere feature, formerly known as RPC over HTTP, lets clients that use Microsoft Office Outlook to connect to their Exchange servers from outside the corporate network or over the Internet using the RPC over HTTP Windows networking component.
ActiveSync	Shows the number of current secure HTTP connections (HTTPS) that are established from Windows Mobile-based or Exchange ActiveSync-enabled mobile devices to this Exchange 2016 server. ActiveSync is a push-orientated protocol. Data such as user messages, schedules, contact information, and tasks are synchronized over the HTTPS connection.
Web Service	Shows the current number of connections with the World Wide Web Publishing Service (W3SVC) for this Exchange 2016 server. This information can help you determine if your server can handle the current user load.
IMAP4	Shows the number of IMAP4 connections to this Exchange 2016 server. The Client Access services provide IMAP4 access to mailbox data for clients that rely on this protocol.
	IMAP4 is an Internet messaging protocol that allows you to access mail on a server or download it to your computer. IMAP4 is designed for an environment where you can log on to the server from a variety of different workstations or across slow links.
	The IMAP4 protocol is disabled by default on Exchange 2016 server. If this Exchange server needs to support IMAP4 clients, start the IMAP4 service. Otherwise, leave it disabled for security reasons.
POP3	Shows the number of POP3 connections to this Exchange 2016 server.
	POP3 is an Internet messaging protocol that supports simple offline mail processing. POP3 allows you to download e-mail messages from the server and store them locally on a client computer.
	By default, POP3 is not enabled. If POP3 is required, start the service. If this Exchange server does not need to support POP3 clients, leave it disabled for security reasons.
UM Clients	Shows the number of voice mail calls that are currently connected to the Unified Messaging Server since the service was started.

Client Access Services Panel

Exchange 2016 has an SMTP protocol and transport stack that does not depend on IIS. Exchange 2016 uses SMTP protocol for server-to-server message delivery within the same Active Directory site or Routing Group, between different Exchange Organizations, and when transferring mail to other email systems. This information includes:

Table 4. Exchange 2016 Client Access services panel.

Component	Description
Front-End Transport Service	Shows the CPU Usage for the Front-End Transport Service (in %).
	The Transportation Role is split into two parts in Exchange 2016: Front-End Transport Service (part of the Client Access services) and Transport Service (part of the Backend services).

Table 4. Exchange 2016 Client Access services panel.

Component	Description
SMTP Inbound Connections	Shows the total number of inbound (recieved) SMTP connections established by other SMTP hosts to this Exchange server. The number of connections represents the sum of all SMTP inbound connections from all remote domains to SMTP Receive Connectors on this Exchange 2016 server.
	If the server is an Edge server, the value comes from perfmon. If the server is not an Edge server, value comes from server properties.
	Exchange 2016 uses SMTP protocol for server-to-server message delivery within the same Active Directory site or Routing Group, between different Exchange organizations, and when transferring mail to other email systems.
HTTP/Proxy Outstanding Requests	Shows the quantity of concurrent outstanding proxy requests for the Microsoft Exchange HTTP Proxy access.
Avg. Authentication Latency (ms)	Shows the average time spent in authenticating client access requests in the past 200 samples.
Avg. RPC Latency (sec)	Shows the average latency in seconds of RPC requests. Average is calculated over all RPCs since exrpc32 was loaded.
IIS Service	Shows the CPU Usage for World Wide Web Publishing Service (in %).
	Exchange Server depends on the Microsoft Internet Information Services (IIS) to connect using HTTP. To keep email communication flowing, the IIS Service must be running properly. If the IIS Service (W3SVC) is down, some Exchange 2016 specific functionality such as ECP, EWS, Autodiscover, ActiveSync, and PowerShell will be affected.
SMTP Outbound Connections	Shows the current number of outbound (sent) SMTP connections to other SMTP hosts. The number of connections represents the sum of all SMTP outbound connections from SMTP Send Connectors on this Exchange 2016 server to all remote SMTP domains.
	If the server is an Edge server, the value comes from perfmon. If the server is not an Edge server, value comes from server properties.
	Exchange 2016 uses SMTP protocol for server-to-server message delivery within the same Active Directory site or Routing Group, between different Exchange organizations, and when transferring mail to other email systems.
Users at Max Concurrency	Shows the total quantity of the users that attain Maximum Connections Limitation.
Proxy Failure Rate	Shows the percentage of the connectivity related to the failures between the Client Access (frontend) services and the Backend services on the destination Exchange 2016 server in the past 200 samples.
LDAP Search Time (ms)	Shows the time to send an LDAP search request and receive a response (in milliseconds).
Inbound Connectors	Shows the number of SMTP Receive connectors on this Exchange 2016 server that can accept mail from other SMTP servers.
	SMTP Receive Connectors provide the ability for Backend services to receive email from any other SMTP server on the Internet, from other Exchange Server 2016 Backend services, or other Exchange Server 2016 organizations. Exchange 2016 Servers can have multiple SMTP Receive connectors with different parameters for availability or performance reasons.
Outbound Connectors	Shows the number of SMTP Send connectors on this Exchange 2016 server that can send connections to other SMTP servers.
	An SMTP Send connector is required for an Exchange Server 2016 to send any SMTP email to other SMTP server on the Internet or to any SMTP server within the same Exchange Server organization. More than one Exchange server can use a Send Connector for routing purposes. The Send Connector properties in the Exchange Management Console show which Exchange servers in the same site can use this Send Connector through which to route mail.

Transport Panel

The Transport panel groups components that identify the status of the various transport queues on this Exchange 2016 server. The Transportation Role is split into two parts in Exchange 2016: Mailbox Transport service and Front-End Transport service.

The Transport service runs on all Exchange 2016 Mailbox servers and consists of two separate services:

- Mailbox Transport Delivery service receives the SMTP messages from the Transport service which is running on the local Exchange 2016 server or other Exchange 2016 servers.
- Transport Submission service, which runs on the Exchange 2016 server, that connects to a local mailbox database using RPC to retrieve messages.

Exchange 2016 has an updated SMTP protocol and transport stack that does not depend on IIS. Exchange 2016 uses SMTP protocol for server-to-server message delivery within the same Active Directory site or Routing Group, between different Exchange Organizations, and when transferring mail to other email systems.

Table 5. Exchange 2016 Transport panel

Component	Description
Inbound Connections	Shows the total number of inbound SMTP connections established by other SMTP hosts to this Exchange server. The number of connections represents the sum of all SMTP inbound connections from all remote domains to SMTP Receive Connectors on this Exchange 2016 server.
	SMTP is the standard protocol for Internet Mail. Exchange 2016 has an updated SMTP protocol and transport stack that does not depend on IIS. Exchange 2016 uses SMTP protocol for server-to-server message delivery within the same Active Directory site or Routing Group, between different Exchange Organizations, and when transferring mail to other email systems.
Outbound Connections	Shows the current number of outbound SMTP connections to other SMTP hosts. The number of connections represents the sum of all SMTP outbound connections from SMTP Send Connectors on this Exchange 2016 server to all remote SMTP domains.
	SMTP is the standard protocol for Internet Mail. Exchange 2016 has an updated SMTP protocol and transport stack that does not depend on IIS. Exchange 2016 uses SMTP protocol for server-to-server message delivery within the same Active Directory site or Routing Group, between different Exchange Organizations, and when transferring mail to other email systems.
EWS Response Time	Shows the average response time for the Exchange Web Services (EWS) which is running on the Exchange 2016 Mailbox Server.
	The Exchange Web Services (EWS) provides the functionality to enable Client Applications to communicate with the Exchange 2016 servers. It also provides the access to much of the same data, which is made available through the Microsoft Office Outlook.
Transport Service	Shows the CPU usage for the Exchange Transport Service (in %).
	The Transport service runs on all Exchange 2016 Mailbox servers and is similar to the Hub Transport server role in previous Exchange versions. This service handles all the inside and outside SMTP mail flow for the entire Exchange 2016 organization. Each SMTP message must be categorized and content-inspected in the Transport service before it can be routed and delivered. After the messages are categorized, they are put in a delivery queue to await delivery to the destination.
	Unlike Exchange 2010 or earlier, the Transport service does not communicate with mailbox databases directly. That task is handled by the Mailbox Transport service. The Transport service routes SMTP messages between the Front-End Transport service, the Transport service, and the Mailbox Transport service

Table 5. Exchange 2016 Transport panel

Component	Description
Transport Delivery Service	This shows the CPU usage for the Exchange Mailbox Transport Delivery service (in %).
	The Exchange Mailbox Transport Delivery service runs on all Exchange 2016 Mailbox servers. It is a separate service from the Mailbox Transport service.
	The Mailbox Transport Delivery service receives the SMTP messages from the Transport service on the local Exchange 2016 Mailbox servers or on the other Exchange 2016 Mailbox servers. The service uses an Exchange remote procedure call (RPC) to connect to a local mailbox database to deliver the messages. The Mailbox Transport Delivery service does not queue messages locally.
ActiveSync Pending	Shows the number of pending Sync commands on the Exchange 2016 Mailbox Server currently.
ActiveSync Request Time	Shows the average request time for the ActiveSync on this Exchange 2016 Mailbox Server.
	This Average Request Time is the average time that elapsed, in milliseconds, waiting for a request to be completed in this Mailbox Server.
Transport Submission Service	Shows the CPU usage for the Exchange Mailbox Transport Submission Service (in %).
	The Exchange Mailbox Transport Submission service runs on all Exchange 2016 Mailbox servers. It is a separate service from the Mailbox Transport service.
	The Mailbox Transport Submission service uses an Exchange remote procedure call (RPC) to connect to a local mailbox database to retrieve messages. The service submits the messages over SMTP to the Transport service that is running on the local Exchange 2016 Mailbox server or on the other Exchange 2016 Mailbox servers. The service has access to the same routing topology information as the Transport service. The Mailbox Transport Submission service does not queue messages locally.
Unreachable Queue	Shows the number of messages in the transport unreachable queue on this Exchange 2016 server. The Unreachable Queue contains any messages that cannot be routed to their final destination.
Poison Queue	Shows the number of potentially harmful messages on this Exchange 2016 server. Messages that contain content that might be damaging to the Exchange Server system are by default delivered to this Poison Queue and suspended. If messages in this queue are deemed not harmful, message delivery can be resumed, and the message enters the Submission Queue.
Delivery Queue	Shows the number of items in the Transport Mailbox Delivery Queue on this Exchange server. The Mailbox Delivery Queue holds messages that are being delivered to mailbox recipients whose mailbox data is stored on a Mailbox Server Role located in the same site as this Transport server. The next hop for a message in this queue is the distinguished name of the destination mailbox store.
	A different mailbox delivery queue exists for each Mailbox server destination. Mailbox delivery queues are created as needed and automatically removed.
Submission Queue	Shows the number of items in the Submission queue. The Submission queue holds messages before they are consumed by the Categorizer which determines what to do with the messages based on information about the intended recipients. After the Submission queue, the Categorizer routes the message to a Mailbox server in a different AD site, a mailbox on an Exchange server, or the Unreachable queue.

Information Store Panel

The Information Store Panel displays key operational metrics for the information store on this Exchange 2016 server. This information includes:

Table 6. Exchange 2016 Information Store panel.

Component	Description
Public Folder	Shows the number of the public folder which are located in the Exchange 2016 Mailbox Server.
	In order to take advantage of the high availability and the storage technologies of the mailbox database, Microsoft Exchange 2016 Public Folders have been modernized. The specially designed mailboxes have been used to store both the public folder content and the hierarchy in the Public Folder architecture. There's no a public folder database any more.
	In Exchange 2016, the Public Folder replication uses continuous replication model.
	The content mailboxes and the high availability for the hierarchy are provided by database availability group (DAG).
Public Folder Mailbox	Shows the number of the public folder mailboxes which are located on the Exchange 2016 Mailbox Server.
	The Exchange 2016 public folder mailboxes contain the information about the hierarchy for a public folder, and the actual content is contained in the Exchange 2016 public folder. When you create a public folder, the first public folder mailbox will become the master hierarchy mailbox. Public folder hierarchy mailbox subsequently created will become a secondary mailbox.
DAG	Shows the name of the Database Availability Group to which this Exchange 2016 server belongs. This is shown for informational purposes only. View the Mailbox Databases drilldown to see more information about the mailbox databases installed on this server.
Replication Service	Shows the Exchange 2016 Replication Service Status.
Store Worker Process	Shows the CPU Utilization of the Microsoft.Exchange.Store.Worker Service in Exchange 2016 Mailbox Server.
	In Exchange 2016, the information store is now called Managed Store, which has two processes:
	• Microsoft.Exchange.Store.Service.exe
	• Microsoft.Exchange.Store.Worker.exe
	Each database is running under its own process, which isolates the stores issues to a single database. Working with the Microsoft Exchange Replication service, Managed Store manages the mailbox databases and uses the Extensible Storage Engine (ESE) as the database engine. This architectural changes enable faster database failover and better physical disk failure handling.
Mailbox Counts	Shows the total number of mailboxes that reside in all mailbox stores. This is shown for informational purposes only.

Table 6. Exchange 2016 Information Store panel.

Component	Description
Store Service Process	Shows the CPU Utilization of the Microsoft.Exchange.Store.Service Service in Exchange 2016 Mailbox Server.
	In Exchange 2016, the information store is now called Managed Store, which has two processes as below:
	• Microsoft.Exchange.Store.Service.exe
	• Microsoft.Exchange.Store.Worker.exe
	Each database is running under its own process, which isolates the stores issues to a single database. Working with the Microsoft Exchange Replication service, Managed Store manages the mailbox databases and uses the Extensible Storage Engine (ESE) as the database engine. This architectural changes enable faster database failover and better physical disk failure handling.
Mailbox Databases	Shows the percentage of disk space consumed by the mailbox stores on this server. This also shows how much of the server disk consumption is caused by mailbox store consumption versus other data.
Transaction Logs	Shows the total percentage of disk space consumed by the transaction logs on this server. It can be used to quickly assess how much server disk is consumed by transaction log data versus other data on the Exchange server.

OS/ Subsystem Panel

The Subsystem panel displays components that represent the health of important subsystem features. This information includes:

Table 7. Exchange 2016 subsystem panel.

Component	Description
CPU Usage	Shows the amount of CPU used on this Exchange 2016 server.
System Disk	Shows the percentage of disk usage for the Windows system disk on this Exchange 2016 server.
System Memory	Shows the amount of physical memory (RAM) Windows is using. Physical memory usage can normally remain close to the total amount of physical memory installed on the system unless the amount of physical memory exceeds the amount of virtual memory that Windows is using. Windows normally keeps some physical memory available for immediate use.
Ping Time	Shows the ping time (in milliseconds) from the client (UC Diagnostics) to the Exchange 2016 server.
Top CPU Consumer	Identifies the process that is consuming the most CPU on this Exchange 2016 server.
Top Memory Consumer	Identifies the process that is consuming the most memory on this Exchange 2016 server.

Message Flows

The Exchange 2016 Diagnostic Console contains the following message flows that show the amount of information being sent to various components in your Exchange 2016 environment.

Table 8. Exchange 2016 message flows panel.

Message Flow	Description
HTTP Proxy Requests/sec	Shows the rate of the HTTP Proxy requests per second.
Inbound Msgs/Sec	Shows the number of messages (sent inbound into the forest) received by the SMTP server each second.
Msgs Sent/sec	Shows the number of messages sent by the SMTP Send connector per second.
Msgs Received/sec	Shows the rate of messages received by SMTP Receive connector on this Exchange 2016 server. The SMTP Receive connector is part of the Microsoft Exchange Transport service on Exchange 2016 holding Mailbox server roles. It controls message processing through a series of SMTP Receive agents performing anti-spam, antivirus, and other tasks before messages are submitted to the categorizer.
Messages Sent/sec	Shows the rate of messages delivered to the mailbox database using Exchange Remote Procedure Call (RPC).
Messages Submitted/sec	Shows the rate of retrieving messages from Mailbox database using Exchange Remote Procedure Call (RPC).
Bytes Written/sec	Shows the Process IO Write Bytes / Sec through the MSExchangeFrontendTransport service.
Bytes Read/sec	Shows the Process IO Read Bytes / Sec through the MSExchangeFrontendTransport service.
Bytes Read/sec	Shows the rate at which data is being read from the disk, network, and device subsystems of the Windows server running Exchange. The data is primarily read from the disk subsystem.
Bytes Written/sec	Shows the rate at which data is being written to the disk, network, and device subsystems of the Windows server running Exchange. The data is primarily written to the disk subsystem.

Drilldowns

Each drilldown page contains displays that provide you with specific information about the components of your system. Drilldowns mainly use two different types of displays — tables and charts. Drilldowns have the following features:

- They can be configured to show all or some of the metrics associated with components.

- You can access further information about displays in drilldowns by moving the mouse over the displays, or by clicking or right-clicking on them.

- You can copy the data shown in drilldowns to other applications or save it to a file.

- You can view a brief description of a drilldown by hovering your mouse over a component, such as a button, dataflow, status ball, or Toolbar button.

To view a drilldown

Right-click a component in a panel and select **Show Details.**

Table 9. Exchange 2016 drilldowns.

Drilldown	Associated Charts/Tabs
Active Directory Server	• Active Directory Servers - shows information about the Active Directory servers in use by this Exchange 2016 server. Exchange 2016 stores all configuration and recipient information in the Active Directory directory service database. • Active Directory Server Details - Shows information about selected Active Directory Server. Exchange 2016 stores all configuration and recipient information in the Active Directory directory service database.
DNS Servers	• DNS Servers - Shows information about the Domain Name System (DNS) Servers used by this Exchange 2016 server. The Exchange 2016 server uses the DNS server that is configured in the IP properties of the network adapter to locate domain controllers and global catalog servers, other Exchange servers, and remote domains. DNS lookup settings can be specified on the Hub Transport server, which override the settings on the network adapter to route messages.
Clients	You can drilldown to more detailed information for the following clients: • ActiveSync • IMAP4 • UM Clients • Outlook • Web Service • POP3 For more information, see Clients Panel on page 146.
Exchange Services	You can drilldown to more detailed information for the following services: • Front-End Transport Service • Transport Submission Service • IIS Service • Mailbox Transport Service • Transport Delivery Service • Store Service For more information, see Transport Panel on page 148.
Client Access Services	You can drilldown to more detailed information for the following components: • SMTP Inbound Connections • HTTP/Proxy Outstanding Requests • Avg. Authentication Latency • Avg. RPC Latency • SMTP Outbound Connections • Users at Max Concurrency • Proxy Failure Rate • LDAP Search Time For more information, see Client Access Services Panel on page 146.

Table 9. Exchange 2016 drilldowns.

Drilldown	Associated Charts/Tabs
Transport	You can drilldown to more detailed information for the following components: • Inbound Connections • Outbound Connections • ActiveSync Pending • ActiveSync Request Time • Unreachable Queue • EWS Response Time • Poison Queue • Delivery Queue • Submission Queue For more information, see Transport Panel on page 148.
Information Store	• Public Folder List - shows information about the public folders on this Exchange 2016 server. • Public folder Mailbox List - shows the information of the public folder mailboxes. • Exchange Database Information - shows information about the databases on this Exchange 2016 server, such as Transaction Log Free Space, Database Free Space, and Database Mount Status.
Subsystem	You can drilldown to more detailed information for the following components: • CPU Usage • System Disk • System Memory • Ping Time For more information, see OS/ Subsystem Panel on page 151.
Processes	• Process Name — indicates the image name of the application itself. • CPU Usage — indicates the percentage of CPU time that the program is currently consuming. This is an instantaneous result. • Physical Memory — indicates the current size of the working set of the process. • Virtual Memory — indicates current memory allocated to this process that cannot be shared with other processes.

Metrics

A metric is an individual piece of information that UC Diagnostics has collected about the performance of a system, such as perfmon counters. The information may be a numeric value (a number or percentage), a string of text, or some other piece of data.

To view the perfmon counters

•   Right-click a component and select **Metrics**.

The perfmon counter is visible in the Metric help section in the General tab.

Every time that the UC Diagnostics window is refreshed, UC Diagnostics retrieves the latest value of the metric, which can then be displayed in a drilldown or on the home page.

The Metric editor allows you to view and edit the properties of UC Diagnostics metrics, including their thresholds and severities. You can open the Metric editor for a component or a drilldown by right-clicking on the component and choosing Metrics from the invoked shortcut menu.

When you open the Metric editor, the General tab is open by default. Several metrics contain data source descriptions for the metric. The data source descriptions use the following list of functions.

Table 10. Exchange 2016 metrics.

Function	Description
max(x)	the maximum of a set of values in list x
max(x,y)	the maximum of x and y
min(x)	the minimum of a set of values in list x
count(x)	the number of values in list x
sum(x)	the sum of a set of values in list x
if(x,y,z)	if x is true, then return y, otherwise, return z
snull(x)	if x could not be collected, then return true
avg(x)	the average of values in list x

Diagnosing BlackBerry with the Diagnostic Console (Plug In)

- Introducing the BlackBerry Diagnostic Console

- Understanding the Diagnostic Console

- BlackBerry Panels

- BlackBerry Message Flows

- BlackBerry Drilldowns

- Metrics

Introducing the BlackBerry Diagnostic Console

The Diagnostic Console provides you with a real-time representation of the messaging system processes and components within a Blackberry server. You can diagnose and resolve issues using the Diagnostic Console.

The Diagnostic Console contains the following:

- Home Pages that highlight targeted areas of the Blackberry server activity.

- Graphical flows that illustrate the rate at which data is moving between server components. Colorful buttons, gauges, spinners, and containers display the value of key statistics and metrics.

- Visual warnings if the performance metrics exceed acceptable thresholds, which you can adjust. The buttons, gauges, and other visual objects, collectively referred to as components, change color to show you the source of the problem.

- Warning messages that are displayed well before the traffic levels of a server become critical.

- A range of reports and graphs that provide you with detailed information about a server. You can view this information on the screen or you can print it.

Understanding the Diagnostic Console

When you connect to the Diagnostic Console, the Home Page displays a high-level summary of your Blackberry server.

The Home Page contains the various panels, message flows, and drilldowns to help you perform an extensive analysis of the major components on your Blackberry server.

To view detailed information on an Exchange server, right-click a component, message flow, and drilldown, and select What's This, Metrics, or Properties.

Specifying SQL Authentication Information

Before connecting to the BlackBerry Diagnostic Console, you can specify SQL Database Authentication information and a private SNMP Community:

1   Right-click a UC Diagnostics BlackBerry Server plug-in connection, and select **Properties**.

2   Select the **Details** tab.

3   Select the **BlackBerry Configuration Database Authentication** check box, and enter a username and password.

4   Select the **Non-Public SNMP Community** check box, and enter a name for the SNMP Community.

5   Click **OK**.

If a private SNMP community is set on the server, the SNMP community name must be entered.

BlackBerry Diagnostic Console Recommendations

The BlackBerry Diagnostic Console provides a real-time representation of the messaging system processes and components within your BlackBerry server. The Diagnostic Console retrieves a large amount of data from a server frequently, which can place excessive stress on a server, actually affecting the server's performance. Also, using the Diagnostic Console for an extended period of time can consume critical system resources, affecting the stability of UC Diagnostics as a whole.

Quest recommends the following:

*   Allow the Diagnostic Console to view a maximum number of 10 servers at any one time.

*   If you are installing the Diagnostic Console on a computer containing Spotlight products and you want to launch the Diagnostic Console from the UC Diagnostics Management Console, then the Diagnostic Console and the Spotlight products should be installed on the C: drive. Else, the Diagnostic Console will fail to launch from the Management Console. As a workaround, create a shortcut on your desktop to C:\Program Files\Quest\Spotlight\Console\Spotlight.exe to manually open connections.

*   If you are using the Diagnostic Console as a monitoring tool, you must disconnect from and reconnect to the Diagnostic Console daily. Though the Management Console can run tests when closed, the Diagnostic Console cannot perform any actions when it is closed.

For information about the required configuration on the BlackBerry Enterprise server and the permissions that are required by the diagnostic console credentials, see the *Unified Communications Diagnostics Deployment Guide*.

BlackBerry Panels

The BlackBerry Server Home Page displays a high-level operational summary of the BlackBerry server and is comprised of the following panels:

*   BlackBerry Service Health Panel

*   BlackBerry SRP Panel

*   BlackBerry System Panel

*   BlackBerry Server Panel

*   BlackBerry Users Panel

*   BlackBerry OS/ Subsystem Panel

BlackBerry Service Health Panel

The Service Health panel displays the CPU and memory usage status of the BlackBerry services described in the following table:

Table 1. BlackBerry server health panel.

Service	Description
BlackBerry Attachment Service	Converts supported attachments into a format that users can view on their BlackBerry handheld devices.
BlackBerry Dispatcher Service	Compresses and encrypts all BlackBerry data and routes the data through the BlackBerry router to and from the wireless network.
BlackBerry Messaging Agents Service	Connects to BlackBerry to provide wireless enterprise activation, and delivers messages to and from the user's mailboxes on the BlackBerry server.
BlackBerry Policy Service	Performs administrative services over the wireless network, such as sending IT policies and IT commands.
BlackBerry Router Service	Connects to the wireless network to route data to and from BlackBerry handheld devices.
BlackBerry Synchronization Service	Synchronizes organizer data between BlackBerry handheld devices and the messaging server over the wireless network.

BlackBerry SRP Panel

This panel indicates whether or not the BlackBerry server is connected to the Server Relay Protocol. This point-to-point protocol runs on top of TCP/IP, and defines transactions between the BlackBerry services and the Relay Server.

Table 2. BlackBerry service relay protocol (SRP) panel.

Component	Description
Reconnections	Indicates the number of times the BlackBerry Dispatcher Service has successfully reconnected to SRP since it was started.
Failed Connections	Indicates the number of times the BlackBerry Dispatcher Service has tried, but failed to connect to SRP since it was started.
SRP Time Not Connected (sec)	Indicates the total time, (in seconds), that the BlackBerry Dispatcher Service has not been connected to SRP since startup.
SRP Last Connect	Indicates the following: • Time of Last SRP Error — indicates the time of the last SRP error. • Last SRP Error — displays the error message of the last failed SRP connection attempt.

BlackBerry System Panel

The System panel identifies the BlackBerry server version, the server UID, the Microsoft Windows version, the AD site, and uptime on this BlackBerry server.

Table 3. BlackBerry system panel.

Component (Example)	Description
BES Version 4.1.3.16	Indicates that the BlackBerry server is running version 4.1.3.16.
SRPID: T95475585	Indicates that the SRPID of the BlackBerry server is T95475585.

Table 3. BlackBerry system panel.

Component (Example)	Description
Windows Server 2007 SP 2	Indicates that the version of Windows running on this server is Windows Server 2007 Service Pack 2.
Database	Identifies the server on which the BlackBerry Configuration Database for this BlackBerry server is located.
Uptime: 13d 01:16	Indicates how long the computer hosting the BlackBerry server has been running.

BlackBerry Server Panel

The Server panel shows server-specific information such as licenses in use, messaging statistics, and critical events on this BlackBerry server.

Table 4. BlackBerry server panel.

Component	Description
Pending Messages	Indicates the number of messages pending delivery to handheld devices serviced by this BlackBerry server.
Expired Messages	Indicates the number of messages which expired before delivery to handheld devices serviced by this BlackBerry server.
Error Messages	Indicates the number of messages that were undeliverable due to error.
MORE Requests	Indicates the number of MORE requests issued from devices.
Global Filtered	Indicates the number of messages to which the BlackBerry Server applied global filters and did not forward to handhelds. Filters are rules applied to messages as they arrive in your Exchange mailbox, and determine whether to redirect the message to your BlackBerry device.
User Filtered	Indicates the number of messages to which the BlackBerry Server applied user-defined filters and did not forward to handhelds. Filters are rules applied to messages as they arrive in your Exchange mailbox, and determine whether to redirect the message to your BlackBerry device
OTAC Users	Indicates the number of users enabled for Over the Air Calendar (OTAC) access. OTAC support allows wireless calendar synchronization for handheld devices.
WER Users	Indicates the number of users enabled for Wireless Email Reconciliation (WER). WER enables you to move or change the status of email messages on the handheld and synchronize these changes to your desktop wirelessly, and vice versa.
	WER is not supported on handhelds running OS versions less than 2.6.
Failed Initializations	Indicates the number of users which failed to initialize correctly.
Critical Events	Indicates the number of critical events which have not been addressed on the BlackBerry server.
Licenses in Use	Indicates the total number of user licenses currently in use on the BlackBerry Server. A Client Access License (CAL) is a license that allows the specified number of users to use the BlackBerry Server.
Messaging Agents	Indicates the number of Messaging Agents running on the BlackBerry Server. BlackBerry Messaging Agents run on demand. Thus, if there are no active users on a particular Messaging Agent, the Messaging Agent will not be running.
Service Connections	Indicates the number of services currently connected to the BlackBerry Router
Device Connections	Indicates the number of devices currently connected to the BlackBerry Router.

BlackBerry Users Panel

The Users panel contains components that indicate the number of users serviced by this BlackBerry server, the number of dormant users, messaging statistics, user latency, and the most recent user error.

Table 5. BlackBerry users panel.

Components	Description
Total Users	Indicates the number of users serviced by this BlackBerry server
Dormant Users	Indicates the number of users whose last contact with the BlackBerry server occurred over 30 days ago
Messages Sent	Indicates the number of messages sent by handheld devices serviced by this BlackBerry server
Messages Received	Indicates the number of messages received by handheld devices serviced by this BlackBerry server
Calendar Sent	Indicates the number of calendar events sent by handheld devices serviced by this BlackBerry server
Calendar Received	Indicates the number of calendar events received by handheld devices serviced by this BlackBerry server
Average Latency	Indicates the average latency of the last 10 messages sent to the handheld devices for all users
Last Error	Indicates the time of the most recent error that occurred for users

BlackBerry OS/ Subsystem Panel

The OS/ Subsystem panel displays the status of the components that represent the health of critical subsystem features.

Table 6. BlackBerry OS / subsystem panel.

Components	Description
CPU Usage	Shows the total amount of CPU usage on this BlackBerry server
Top CPU Consumer	Identifies the process that is consuming the most CPU on this BlackBerry server
Top Memory Consumer	Identifies the process that is consuming the most memory on this BlackBerry server
Network Output Queue	Indicates the network output queue length for all network adapters on this BlackBerry server
Network Bytes per Sec	Indicates the number of bytes sent and received per second by the network adapters on this BlackBerry server
Processor Queue	Indicates the processor queue length on this BlackBerry server
System Memory	Indicates the amount of RAM that is currently being consumed on this BlackBerry server
System Disk	Indicates the amount of free and used disk space on this BlackBerry server

BlackBerry Message Flows

The Diagnostic Console contains the following message flows that show the amount of information being sent to various components in your Blackberry environment.

Table 7. BlackBerry Message Flows

Message Flow	Description
Msgs Received/min	Indicates the number of messages received by handhelds per minute. This value reflects server activity since the last time the BlackBerry Server restarted.
Msgs Sent/min	Indicates the number of messages sent by handhelds per minute. This value reflects server activity since the last time the BlackBerry Server restarted.
Bytes Read/sec	Indicates the rate at which data is being read from the disk on the BlackBerry Server
Bytes Written/sec	Indicates the rate at which data is being written to the disk on the BlackBerry Server

BlackBerry Drilldowns

Each drilldown page contains displays that provide you with specific information about the components of your system. Drilldowns mainly use two different types of displays – tables and charts. Drilldowns have the following features:

- They can be configured to show all or some of the metrics associated with components.

- You can access further information about displays in drilldowns by moving the mouse over the displays, or by clicking or right-clicking them.

- You can copy the data shown in drilldowns to other applications or save it to a file.

- You can view a brief description of a drilldown by hovering your mouse over a component, such as a button, dataflow, status ball, or Toolbar button.

To view a drilldown

Right-click a component in a panel and select **Show Details.**

Table 8. BlackBerry drilldowns.

Drilldown	Associated Charts/Tabs
Service Health	• BlackBerry Attachment Service • BlackBerry Dispatcher Service • BlackBerry Messaging Agents Service • BlackBerry Policy Service • BlackBerry Router Service • BlackBerry Synchronization Service For a description of these charts, For more information, see BlackBerry Service Health Panel on page 158.
SRP	• SRP Status – indicates whether or not the BlackBerry Server is connected to RIM's Server Relay Protocol (SRP) server using port 3101 For a description on the other charts, For more information, see BlackBerry SRP Panel on page 158.

Table 8. BlackBerry drilldowns.

Drilldown	Associated Charts/Tabs
Server	• Message and Users – Shows messages and user information. Message charts includes: Pending, Expired, Error, MORE, Global Filtered, and User Filtered. User charts include: OTAC, WER, and Failed Initializations. • Licenses and Connections – Shows license and connection information. License charts include information on licenses currently in use. Connection charts include: Message Agents, Service Connections, and Device Connections. For a description on these charts, For more information, see BlackBerry Server Panel on page 159.
Users	• User Configuration – shows configuration data for the users hosted by this BlackBerry Server • User Devices – shows users' handheld device information on this BlackBerry Server • User Statistics – shows statistical information related to the users on this BlackBerry Server
OS/Subsystem	• CPU Usage • System Disk • Network Bytes per Sec • System Memory • Network Output Queue • Processor Queue Length For a description of these charts, For more information, see BlackBerry OS/Subsystem Panel on page 160.
Processes	• Process Name • CPU Usage • Physical Memory • Virtual Memory

Metrics

A metric is an individual piece of information that UC Diagnostics has collected about the performance of a system, such as perfmon counters. The information may be a numeric value (a number or percentage), a string of text, or some other piece of data.

To view the perfmon counters

• Right-click a component and select **Metrics**.

The perfmon counter is visible in the Metric help section in the General tab.

Every time that the UC Diagnostics window is refreshed, UC Diagnostics retrieves the latest value of the metric, which can then be displayed in a drilldown or on the home page.

The Metric editor allows you to view and edit the properties of UC Diagnostics metrics, including their thresholds and severities. You can open the Metric editor for a component or a drilldown by right-clicking on the component and choosing Metrics from the invoked shortcut menu.

When you open the Metric editor, the General tab is open by default. Several metrics contain data source descriptions for the metric. The data source descriptions use the following list of functions.

Table 9. Server metrics.

function	Description
max(x)	the maximum of a set of values in list x
max(x,y)	the maximum of x and y
min(x)	the minimum of a set of values in list x
count(x)	the number of values in list x
sum(x)	the sum of a set of values in list x
if(x,y,z)	if x is true, then return y, otherwise, return z
snull(x)	if x could not be collected, then return true
avg(x)	the average of values in list x

15

Diagnosing OCS with the Diagnostic Console (Plug In)

- Introducing the OCS Diagnostic Console
- Understanding the OCS Diagnostic Console
- Panels
- OCS Message Flows
- OCS Drilldowns
- Metrics

Introducing the OCS Diagnostic Console

The Diagnostic Console provides you with a real-time representation of the messaging system processes and components within OCS (Office Communications Server). The Diagnostic Console can perform real-time monitoring on Front-End and Conferencing servers only.

The Diagnostic Console retrieves a large amount of data from a server frequently, which can place excessive stress on a server, affecting the server's performance. Also, using the Diagnostic Console for an extended period of time can consume critical system resources, affecting the stability of UC Diagnostics. It is recommended that the Diagnostic Console view a maximum of 10 servers at any one time.

The Diagnostic Console contains the following:

- Home pages that highlight targeted areas of the OCS server activity.
- Graphical flows that illustrate the rate at which data is moving between server components. Colorful buttons, gauges, queues, spinners, and containers display the value of key statistics and metrics.
- Visual warnings if the performance metrics exceed acceptable thresholds, which you can adjust. The buttons, gauges, queues, and other visual objects, collectively referred to as components, change color to show you the source of the problem.
- Warning messages that are displayed well before the traffic levels of a server become critical.
- A range of reports and graphs that provide you with detailed information about a server. You can view this information on the screen or you can print it.

If you are using the Diagnostic Console as a monitoring tool, you must disconnect from, then reconnect to the Diagnostic Console daily. Though the Management Console can run tests when it is closed, the Diagnostic Console cannot perform any actions when it is closed.

For information about software prerequisites and the permissions required to run the diagnostic console on OCS, see the *Unified Communications Diagnostics Deployment Guide*.

When Connecting to OCS

You may see your service account in the security log of the OCS environment that is being monitored. If you are using the OCS Diagnostic Console, you connect to the OCS server using the user credentials of the user who is currently logged in. Kerberos logs events in the event log during authentication.

Before you launch and connect to the OCS Diagnostic Console, read OCS related information on Active Directory. You need read access to the following:

- Perfmon on the target server
- Event Logs on the target server
- Back-End database tables (rtc and rtcdyn) for the pool where the target server is located
- Back-End database stored procedures (rtc and rtcconfig) for the pool where the target server is located

To get read access on OCS

1   Create a new domain security group named "OCS Diagnostic Users".

2   Connect to the OCS Back-End server using SQL client tools.

3   Assign to the "OCS Diagnostic Users" group the database roles of "db_datareader" and "public", for the rtc, rtcconfig, and rtcdyn databases.

4   Add the "OCS Diagnostic Users" group to the TRCUniversalReadOnlyAdmins domain security group.

    This provides read access to the OCS data in Active Directory.

5   Add the "OCS Diagnostic Users" group to the Power Users and Performance Monitor Users local security groups on each OCS server.

Understanding the OCS Diagnostic Console

When you connect to the Diagnostic Console, the home page displays a high level summary of your OCS server.

The home page contains the various panels, message flows, and drilldowns to help you perform an extensive analysis of the major components on your OCS server.

To view detailed information on your specific components, right-click a component, message flow, and drilldown, and select What's This, Metrics, or Properties.

Panels

OCS Message Flows

OCS Drilldowns

Metrics

Panels

The Diagnostic Console contains the following panels:

- Server Information Panel
- Clients/Network Panel
- Server Load Panel

- Server Roles Panel
- OS/Subsystem Panel

Server Information Panel

The Server Information panel, located below the toolbar, displays information about the OCS environment you are currently viewing. This information includes:.

Table 1. OCS server information panel.

Component	Description
OCS Version	Indicates the OCS version to which you are connected - either OCS 2007 or OCS 2007 R2.
Server FQDN	Indicates the Fully Qualified Domain Name of the server being monitored.
Operating System	Indicates the operating system running on the server being monitored.
OCS Pool	Indicates the name of the pool to which the server being monitored belongs.
Back-End Database	Indicates the server (and possible instance) hosting the Back-End database for the pool.
Server Certificate (CRT) Status Ball	Validates the identification of the remote server.
AS Status Ball	Indicates if the Application Sharing (AS) server is present and registered in the environment. Use the drilldown to monitor the performance and requests of the AS Server. The AS Status Ball is active only if you are connected to an OCS 2007 R2 server.
QMS Status Ball	Indicates that there is a Quality of Monitoring Experience (QMS) server configured in the environment. Use the drilldown to see what server(s) is (are) hosting the role.
CDR Status Ball	Indicates there is a Call Details Report (CDR) Server Role configured in the environment. Use the drilldown to see what server(s) is (are) hosting the role.
CWA Status Ball	Indicates there is a Communicator Web Access (CWA) Server Role configured in the environment. Use the drilldown to see what server(s) is (are) hosting the role

Clients/Network Panel

The Clients/Network panel displays information about the connections and messages waiting to be sent from your OCS environment. This panel includes:

Table 2. OCS clients/network panel.

Component	Description
Secure Connections	Indicates the number of active secure connections (clients) that have been made to this server. Connections are secured using Transport Layer Security (TLS).
Registered Endpoints	Indicates the number of connected endpoints registered.
AD Search Latency (ms)	Indicates the average latency related to queries (in ms) sent to the Active Directory.
Outstanding RPC Calls	Indicates the number of RPC calls waiting to be sent.
Network Output Queue	Indicates the number of network packets waiting to be sent.
Authentication Queue	Indicates the number of authentication requests waiting to be handled.

Table 2. OCS clients/network panel.

Component	Description
Theoretical Bandwidth	Indicates the level of network traffic graphed against a "theoretical" maximum bandwidth. The maximum bandwidth is calculated by totaling the capacity of all network devices reported by the operating system. If you are running on an Ethernet network, the actual maximum is approximately 50% of the theoretical bandwidth because of the methods involved in sending data. Having the actual bandwidth equal the theoretical bandwidth is only possible using full duplex Ethernet. Token passing network topologies, such as Token ring and FDDI, enable a theoretical maximum bandwidth much closer to the actual bandwidth.
Ping Time	Indicates the amount of time it takes the computer running the Diagnostic Console to ping the target server.

Server Load Panel

The Server Load panel displays information flow controlled connections, SIP and C3P messages, and database. This panel includes:

Table 3. OCS server load panel.

Component	Description
Flow Controlled Connections	Indicates the number of connections currently operating in a flow-controlled manner. When a connection is flow-controlled, it can only have one outstanding transaction.
Average Holding Time(s)	Indicates the average time an incoming message waits before being processed.
SIP Messages Outstanding	Indicates the total number of SIP Messages currently being processed by the server.
Message Processing Time(s)	Indicates the average amount of time to process incoming messages.
Conf. Allocation Latency (ms)	Indicates the average time to allocate a new conference.
Outstanding C3P Transactions	Indicates the number of outstanding C3P transactions waiting to be processed.
Database Queue Latency (ms)	Indicates the average amount of time a database request waits in the processing queue for the database to become available.
Database Sproc Latency (ms)	Indicates the average amount of time to execute a stored procedure (Sproc) on the Back-End database.

Server Roles Panel

The Server Roles panel displays information about the amount of CPU being used by your Front-End server and conferencing servers. This panel includes:

Table 4. OCS server roles panel.

Component	Description
Front-End (RTCSrv)	Indicates the amount of CPU usage from the OCS Front-End service.
Front-End (RTCHost)	Indicates the amount of CPU usage from the OCS Front-End host process.
IM Conferencing	Indicates the amount of CPU usage from the OCS IM Conferencing server. It also indicates the number of Allocated Conferences.
PSTN Conferencing	Indicates the amount of CPU usage from the OCS PSTN Conferencing server. It also indicates the number of Allocated Conferences.
Web Conferencing	Indicates the amount of CPU usage from the OCS Web Conferencing server. It also indicates the number of Allocated Conferences.

Table 4. OCS server roles panel.

Component	Description
A/V Conferencing	Indicates the amount of CPU usage from the OCS A/V Conferencing server. It also indicates the number of Allocated Conferences.

OS/Subsystem Panel

The OS/Subsystem panel displays information about the amount of CPU being used by all processes. It also indicates the amount of System Memory and System Disk being used, and reports on any errors. This panel includes:

Table 5. OCS OS subsystem panel.

Component	Description
CPU Usage	Indicates the amount of CPU used by all processes.
Top CPU Consumer	Indicates the top CPU consumer.
Top Memory Consumer	Indicates the top consumer of memory.
System Memory	Indicates the amount of system memory used by all processes.
Processor Queue	Indicates the number of threads waiting to execute.
System Disk	Indicates the amount of system disk space being used.
Event Log Errors	Indicates the number of OCS-related errors in the Event Log.
Last AB Update	Indicates the date stamp of the most recent file in the Address Book share location.

OCS Message Flows

The OCS Diagnostic Console contains the following message flows that show the amount of information being sent to various components in your OCS environment.

Table 6. OCS message flows panel.

Message Flow	Description
Unavailable/Sec	Indicates the amount of errors per second
SIP In/Sec	Indicates the amount of incoming SIP messages/second
SIP Out/Sec	Indicates the amount of outgoing SIP messages/second
Authentications/Sec	Indicates the number of authentications created per second
Authentication Errors/Sec	Indicates the number of authentication errors per second
Com Failures/Sec	Indicates the number of communication failures per second
Req Drop/Sec	Indicates the number of requests dropped per second
Resp Drop/Sec	Indicates the number of responses dropped per second
C3P Rec/Sec	Indicates the number of C3P messages received per second
C3P Sent/Sec	Indicates the number of C3P messages sent per second
Archiving/Sec	Indicates the number of messages sent to the MSMQ per second
User Replication Updates/Sec	Indicates the number of user replicator updates occurring per second

OCS Drilldowns

Each drilldown page contains displays that provide you with specific information about the components of your system. Drilldowns mainly use two different types of displays – tables and charts. Drilldowns have the following features:

- They can be configured to show all or some of the metrics associated with components.

- You can access further information about displays in drilldowns by moving the mouse over the displays, or by clicking or right-clicking on them.

- You can copy the data shown in drilldowns to other applications or save it to a file.

- You can view a brief description of a drilldown by hovering your mouse over a component, such as a button, dataflow, status ball, or Toolbar button.

To view a drilldown

- Right-click a component in a panel and select **Show Details**.

Table 7. OCS drilldowns.

Drilldown	Associated Charts/Tabs
Clients/Network	• Network — indicates the number of packets waiting to be sent through the network. • TCP/IP — indicates the TCP segments, UDP datagrams, IP Fragments, and IP Datagrams that are transferred. • NBT — indicates the computers that have an active connection to the system being diagnosed. • Authentication — indicates how many Authentications/sec and Authentication Errors/sec are occurring. • AD Search Latency — indicates the average amount of time to perform an LDAP search against the first Global Catalog found in the domain. • Outstanding RPC Calls — indicates the number of RPC calls waiting to be sent between Front-End servers. • Connected Endpoints — allows you to enter a search filter to limit the number of endpoints returned.
Server Load	• Flow Controlled — indicates the number of flow controlled connections per connections source, average holding time of connections, how many connections have been dropped, and average delay of connections. • SIP — indicates the number of incoming and outgoing SIP messages, messages outstanding, dropped, or held, and memory usage of the SIP Proxy. • C3P — indicates the average time to allocate a new conference and the number of C3P transactions being processed. • Database — indicates the average amount of time a database request or database stored procedure waits before it is sent to the database.
Server Roles	• Roles — indicates the amount of CPU usage per Front-End server, and number of allocated conferences by type. • IM Conferences — indicates the number of connected users, the number of incoming and outgoing messages, and overall health per IM conference. • Telephony (PSTN) Conferences — handles the C3P messages that flow between Focus and the ACP. • Web Conferences — indicates the number of participants, number of slides, and number of errors in the Web Conference. • A/V Conferences — indicates the number of users, number of audio/video messages being sent and received, the average time it takes to process Audio packets, and the number of buffers sent to users.

Table 7. OCS drilldowns.

Drilldown	Associated Charts/Tabs
OS Subsystem	• CPU — indicates the CPU usage by all processes. • Memory — indicates the amount of memory used by all users. • Top CPU/Memory Consumers — indicates the top consumers of CPU and memory. • Logical Disk – indicates the number of read and write requests, disk queue, and transfer time. • User Replicator/Address Book — indicates the user replicator updates and the contents of the Address Book file share. • Archiving — indicates various characteristics of the Archiving server such as CPU and memory usage, database queue latencies, database queue depth, and MSMQ messages.

Metrics

A metric is an individual piece of information that UC Diagnostics has collected about the performance of a system, such as perfmon counters. The information may be a numeric value (a number or percentage), a string of text, or some other piece of data.

Each time the UC Diagnostics window is refreshed, UC Diagnostics retrieves the latest value of the metric, which can be displayed in a drilldown or on the home page.

The Metric editor allows you to view and edit the properties of UC Diagnostics metrics, including their thresholds and severities. You can open the Metric editor for a component or a drilldown by right-clicking on the component and choosing Metrics from the invoked shortcut menu.

When you open the Metric editor, the General tab is open by default. Several metrics contain data source descriptions for the metric. The data source descriptions use the following list of functions.

Table 8. OCS metrics.

Function	Description
max(x)	the maximum of a set of values in list x
max(x,y)	the maximum of x and y
min(x)	the minimum of a set of values in list x
count(x)	the number of values in list x
sum(x)	the sum of a set of values in list x
if(x,y,z)	if x is true, then return y, otherwise, return z
snull(x)	if x could not be collected, then return true
avg(x)	the average of values in list x

To view the perfmon counters

• Right-click a component and select **Metrics**.

The perfmon counter is visible in the Metric help section in the General tab.

Diagnosing Lync 2013 or Skype for Business 2015 with the Diagnostic Console (Plug In)

- Introducing the Lync/Skype Diagnostic Console
- Understanding the Lync/Skype Diagnostic Console
- Panels
- Lync/Skype Message Flows
- Lync/Skype Drilldowns
- Metrics

Introducing the Lync/Skype Diagnostic Console

The Diagnostic Console provides you with a real-time representation of the messaging system processes and components within Lync 2013/Skype for Business 2015. The Diagnostic Console can perform real-time monitoring on Front-End and Conferencing servers only.

The Diagnostic Console retrieves a large amount of data from a server frequently, which can place excessive stress on a server, affecting the server's performance. Also, using the Diagnostic Console for an extended period of time can consume critical system resources, affecting the stability of UC Diagnostics. It is recommended that the Diagnostic Console view a maximum of 10 servers at any one time.

The Diagnostic Console contains the following:

- Home pages that highlight targeted areas of the Lync/Skype server activity.
- Graphical flows that illustrate the rate at which data is moving between server components. Colorful buttons, gauges, queues, spinners, and containers display the value of key statistics and metrics.
- Visual warnings if the performance metrics exceed acceptable thresholds, which you can adjust. The buttons, gauges, queues, and other visual objects, collectively referred to as components, change color to show you the source of the problem.
- Warning messages that are displayed well before the traffic levels of a server become critical.
- A range of reports and graphs that provide you with detailed information about a server. You can view this information on the screen or you can print it.

If you are using the Diagnostic Console as a monitoring tool, you must disconnect from, then reconnect to the Diagnostic Console daily. Though the Management Console can run tests when it is closed, the Diagnostic Console cannot perform any actions when it is closed.

For information about software prerequisites and the permissions required to run the diagnostic console on Lync or Skype for Business, see the *Unified Communications Diagnostics Deployment Guide*.

When Connecting to Lync/Skype

You may see your service account in the security log of the Lync/Skype environment that is being monitored. If you are using the Lync Diagnostic Console, you connect to the Lync/Skype server using the user credentials of the user who is currently logged in. Kerberos logs events in the event log during authentication.

Before you launch and connect to the Lync/Skype Diagnostic Console, you must be able to read the Lync or Skype related information in Active Directory. You need read access to the following:

- Perfmon on the target server

Required permissions on Lync/Skype servers

The following permissions are required on each server.

Table 1. Lync/Skype diagnostic console permissions.

Lync/Skype role	Permissions required on Lync/Skype servers
All	Member of Local Administrators group
	Member of at least one of the following security groups
	• CSHelpDesk
	• CSServerAdministrator
	• CSViewOnlyAdministrator

Understanding the Lync/Skype Diagnostic Console

When you connect to the Diagnostic Console, the home page displays a high level summary of your Lync/Skype server. The home page contains the various panels, message flows, and drilldowns to help you perform an extensive analysis of the major components on your Lync 2013/Skype for Business 2015 server.

> Panels
>
> Lync/Skype Message Flows
>
> Lync/Skype Drilldowns
>
> Metrics

To view detailed information on your specific components, right-click a component, message flow, and drilldown, and select What's This, Metrics, or Properties.

Panels

The Diagnostic Console contains the following panels:

- General Information Panel
- AD/DNS Panel
- Roles Panel
- Connections Panel
- Web Components
- SIP Stack
- Lync/Skype Server Health Panel
- OS/Subsystem Panel

General Information Panel

The General Information panel displays information about the Lync/Skype environment you are currently viewing.

Table 2. Lync/Skype general information panel.

Component	Description
Windows Version	Indicates the operating system and service packs that are installed on the server being monitored.
Lync/Skype Pool FQDN	Indicates the Fully Qualified Domain Name (FQDN) of the pool to which the server being monitored belongs.
Back-End Database	Indicates the server that is hosting the back-end database for the pool.
Lync/Skype Version	Indicates the Lync/Skype version that is installed on the server to which you are connected.
Uptime	Indicates the number of days that the server has been running.
CU Version	Indicates the latest installed Lync 2013 or Skype for Business 2015 cumulative update version.

AD/DNS Panel

The AD/DNS panel provides information about the Active Directory and Domain Name System servers used by this Lync/Skype server.

Table 3. Lync/Skype AD/DNS panel.

Component	Description
AD	Determines the status of the Active Directory (AD) servers used by this Lync/Skype server by checking the following conditions: • the average amount of time (in mlliseconds) it takes to perform LDAP searches against the first Global Catalog found in the domain. • the ping time between the client and the domain controller. • whether the domain controller is available on the network from this client computer.

Table 3. Lync/Skype AD/DNS panel.

Component	Description
DNS	Determines the status of the Domain Name System (DNS) servers in use by this Lync/Skype server by checking the following conditions: • the ping time between the client (Diagnostic Console) and the DNS server. • whether the DNS server can be reached on the network from this client.

Roles Panel

The Roles panel provides information about the server roles installed and active on this server. The server role balls display information about the status of each server role and the amount of CPU being used.

Table 4. Lync/Skype roles panel.

Component	Description
FE (Front-end)	Indicates whether the front-end server role is present and registered in the Lync/Skype environment. Front-end is a server role that provides many basic functions. It is the core Lync/Skype server role.
DIR (Director)	Indicates whether the director server role is present and registered in the environment. Directors can authenticate the Lync/Skype user requests, but Directors do not host user accounts and do not provide presence or conferencing services. The Director is the most useful way to enhance the security in deployments in which external user accesses are enabled.
MED (Mediation)	Indicates whether the mediation server role is present and registered in the Lync/Skype environment. A mediation server is necessary to implement dial-in conferencing and Enterprise Voice. It can translate signaling and media between the Lync/Skype Server Enterprise Voice infrastructure and the PSTN gateway, the IP-PBX, or the SIP trunk.
CHAT	Indicates whether the persistent chat server role is present and registered in the environment.

Connections Panel

The Connections panel shows the current connection status on a Lync/Skype server.

Table 5. Lync/Skype connections panel.

Component	Description
Total Clients	The total number of active registered endpoints connected to this server.
IM Conference	Shows the number of instant messaging conferences on this server that are using the Instant Messaging Conferencing Unit (ImMcu).
AV Conference	Shows the number of active audio/video conferences on this server that are using the Audio Video Server (AVMCU) service.
AS Conference	Shows the number of active application sharing conferences on this server that are using the Application Sharing Server (ASMCU) service.
Enterprise Inbound Calls	The number of inbound enterprise voice calls currently in progress.
Enterprise Outbound Calls	The number of outbound enterprise voice calls currently in progress.

Table 5. Lync/Skype connections panel.

Component	Description
PCHAT Rooms	Shows the number of persistent chat sessions with active users on this server.
Mobile Clients	The number of currently active sessions with active presence subscriptions. You can drilldown to display more details about connections that are using Mcx (Mobility Service) or UCWA (Unified Communications Web API).

Web Components

The clients primarily talk SIP to the Lync/Skype server, or UCWA in the case of mobile which involves a web component, as does the client interaction with the address book.

This panel allows you to view how the server is processing incoming mobile messages. You can use this panel to determine if the server is too busy and is unable to process user requests in timely fashion.

Table 6. Lync/Skype web components panel.

Component	Description
AB Health State	Indicates the state of the Address Book file requests and search requests to the Lync 2013 or Skype for Business 2015 server. Click the component to display a drilldown that shows the status of the failed/succeeded Address Book file download requests rate and the Address Book Web Query failures rate.
AB Processing Time (ms)	Shows the average processing time for a successful Address Book file request (in milliseconds). Click the component to display a drilldown that shows the Address Book average processing time (ms) and the Address Book Web Query average processing time (ms).
Web Req Queue	Indicates number of current application requests. This value can grow if the application is overloaded due to a large number of requests. The number can also represent requests that are waiting on other services to respond or software errors that result in no response.
HTTP Proxy Requests	Shows the number of HTTP proxy requests that are pending for completion.

SIP Stack

The clients primarily talk SIP to the Lync/Skype server, or UCWA in the case of mobile which involves a web component, as does the client interaction with the address book.

This panel allows you to view how the server is processing SIP messages. You can use this panel to determine if the server is too busy and is unable to process user requests in timely fashion.

Table 7. Lync/Skype SIP stack panel.

Component	Description
Msg Hold Time (s)	The average time that the server held the incoming SIP messages currently being processed. A healthy system should have a hold time of less than 3 seconds.
Msg Processing Time (s)	The average time (in seconds) it takes to process an incoming SIP message.
Msg Timed Out	The number of incoming SIP messages currently being held by the server for processing for more than the maximum tracking interval.
Outgoing Queue Delay	The average time (in seconds) for messages delayed in the outgoing (send) queues. The server will drop client connections if it is throttled and messages stay in the outgoing queue for more than 20 seconds. Use this indicator to determine if the destination of the connection is overloaded or if network bandwidth to the destination is insufficient.

Lync/Skype Server Health Panel

The Server Health panel displays information about Lync/Skype and IIS services, and shows the availability and status of various services on the server. This panel includes:

Table 8. Lync/Skype server health panel.

Component	Description
Lync/Skype Services	Indicates the status of the Lync/Skype services that are set as required on this server. It will set an alarm if any of the required services are not currently running.
	The spinner shows the CPU percentage that is used by the Lync/Skype services running on this server.
IIS Service	Shows the status of Internet Information Services (IIS) on the this server (running, stopped, or service is not installed).
	The spinner shows the CPU percentage that is used by IIS running on this server.
MCU Health State	Indicates the current health of application sharing conferences, audio/video (A/V) conferences, data conferences, and instant messaging (IM) conferences.
CMS Replication	Indicates whether the Central Management Store (CMS) replication for this server is up-to-date.
MCU Allocation Latency (ms)	This indicates the average time (in milliseconds) that it takes to complete a full MCU allocation request. If the value is high, it might be a temporary situation if the MCU factory or MCU or back-end is busy and does not respond immediately.
Database Queue Latency (ms)	Indicates the average time (in milliseconds) that a request is held in the request queue that is going to the back-end database. If the topology is healthy, this value averages less than 5000 ms. Occasional spikes are acceptable.
Create Conference Latency (ms)	This indicates the average time (in milliseconds) that it takes to complete a create conference call. If the value is high, it might be a temporary situation if the MCU or back-end is busy and does not respond immediately
Storage Service Database	Shows the current percentage of space that is used by the Storage Service database.

OS/Subsystem Panel

The OS/Subsystem panel displays information about the amount of CPU being used by all processes. It also indicates the amount of System Memory and System Disk being used, and reports on any errors. This panel includes:

Table 9. Lync/Skype OS/subsystem panel.

Component	Description
CPU Usage	Indicates the amount of CPU used by all processes on the monitored server.
System Disk	Indicates the percentage of system disk space being used, showing the amount of used space and the amount of free space.
Top CPU Consumer	Indicates the top consumer of processing resources.
Top Memory Consumer	Indicates the top consumer of memory.
System Memory	Indicates the amount of system memory that is used by all processes on the monitored server.
Ping Time	Indicates the amount of time it takes the computer running the diagnostic console to ping the target server.

Table 9. Lync/Skype OS/subsystem panel.

Component	Description
Network Output Queue	Shows the number of packets waiting to be sent from the target server. The network output queue can help alert you to problems the server is experiencing with network connectivity.
Theoretical Bandwidth	Indicates the level of network traffic graphed against a "theoretical" maximum bandwidth. The maximum bandwidth is calculated by totaling the capacity of all network devices reported by the operating system. If you are running on an Ethernet network, the actual maximum is approximately 50% of the theoretical bandwidth because of the methods involved in sending data. Having the actual bandwidth equal the theoretical bandwidth is only possible using full duplex Ethernet. Token passing network topologies, such as Token ring and FDDI, enable a theoretical maximum bandwidth much closer to the actual bandwidth.

Lync/Skype Message Flows

The Lync/Skype Diagnostic Console contains the following message flows that show the amount of information being sent to various components in your Lync/Skype environment.

Table 10. Lync/Skype message flows.

Message Flow	Description
UCWA App Req Rec/Sec	Shows the number of UCWA application creation requests received per second.
Web Push Notification Req/Sec	The per second rate of sent push notifications by the MCX mobility service.
SIP Msgs In/Sec	Shows the per-second rate of the incoming messages on the SIP protocol processing layer of the server.
SIP Msgs Out/Sec	Shows the per-second rate of the outgoing messages on the SIP protocol processing layer of the server.
Bytes Sent/Sec (between Connections and OS/Subsystem)	Shows the number of bytes sent from the ASMCU service and the application sharing transport (per second).
Bytes Received/Sec (between Connections and OS/Subsystem)	Shows the number of bytes received by the ASMCU service and the application sharing transport (per second).
DB Query / Sec	Indicates the number of Address Book database queries per second.
HTTP Proxy Req / Sec	Shows the number of HTTP proxy requests per second.
Req Drop / Sec	Indicates the number of incoming requests dropped (per second) because they could not be processed (due to insufficient routing information, bad headers, server resource allocation failure, and so on).
Resp Drop / Sec	Indicates the number of incoming responses dropped (per second) because they could not be processed (due to insufficient routing information, bad headers, server resource allocation failure, and so on).
Bytes Read/Sec (between Server Health and OS/Subsystem)	Shows the rate at which data is being read from the disk, network, and device subsystems of the Windows server that is hosting the server. The data is read primarily from the disk subsystem.
Bytes Written/Sec (between Server Health and OS/Subsystem)	Shows the rate at which data is being written to the disk, network, and device subsystems of the Windows server that is hosting the server. The data is written primarily to the disk subsystem.

Lync/Skype Drilldowns

Each drilldown page contains displays that provide you with specific information about the components of your system. Drilldowns mainly use two different types of displays – tables and charts. Drilldowns have the following features:

- They can be configured to show all or some of the metrics associated with components.

- You can access further information about displays in drilldowns by moving the mouse over the displays, or by clicking or right-clicking on them.

- You can copy the data shown in drilldowns to other applications or save it to a file.

- You can view a brief description of a drilldown by hovering your mouse over a component, such as a button, dataflow, status ball, or Toolbar button.

To view a drilldown

- Right-click a component in a panel and select **Show Details**.

Table 11. Lync/Skype drilldowns.

Drilldown	Associated Charts/Tabs
AD	Shows the status of the Active Directory servers available to the Lync Server 2013 or the Skype for Business 2015 server including: • The ping time between the client (Diagnostic Console) and the domain controller. • If this Active Directory Server is GC. • If this Active Directory server is available on the network.
DNS	Shows the status of the DNS (Domain Name System) servers used by this the Lync Server 2013 or the Skype for Business 2015 server including: • The ping time between the client (Diagnostic Console) and the DNS Server. • If the DNS server can be reached on the network from this client.
Connections	Shows the number of active connections for conferences, calls, and chat rooms: • Total Clients: Indicates the total number of active registered endpoints connected to this Lync 2013/Skype for Business 2015 Server. • IM Conferences: Indicates the number of active Instant Messaging (IM) conferences on this Lync 2013/Skype for Business 2015 Server. • A/V Conferences: Indicates the number of active audio or video conferences on this A/V Conferencing Server. • AS Conferences: Indicates the number of active application sharing conferences on this Lync 2013/Skype for Business 2015 Server. • Enterprise Inbound/Outbound Calls: Indicates the number of enterprise voice inbound/outbound calls in progress. • Persistent Chat Rooms: Indicates the total number of persistent chat rooms with active users on this Lync 2013/Skype for Business 2015 Server.

Table 11. Lync/Skype drilldowns.

Drilldown	Associated Charts/Tabs
Mobile Clients	Shows detailed information for mobile clients including: • The number of currently active sessions. • The current number of active sessions in the Mobile Communication Service (Mcx) that have active presence subscriptions (number of always-connected mobile users). • The number of active applications. • The number of active user instances. **NOTE:** If the difference between Active Sessions with Active Presence and Active Sessions is small over time, this means that most mobile device users have an always-connected device such as an Android mobile device under Mcx. If the Active Session count is much higher than Active Session with Active Presence count, this indicates that more users are using a background endpoint device, such as Windows Phone under Mcx.
AB Health State	Shows graphs that contain the following information: • Address Book failed file download requests (per second). • Address Book succeeded file download requests (per second) • Address Book failed web search requests (per second).
AB Processing Time	Shows graphs that contain the following information: • Average processing time for a successful Address Book file download request (in milliseconds) • Average processing time for a successful Address Book web search request (in milliseconds)
Web Req Queue	You can drill down to see requests awaiting completion - The total number of requests currently being processed by application.
Lync/Skype Services	If you drilldown on the Lync/Skype Services spinner, you can view the key services status, memory consumption, and CPU consumption for the following server roles: • Front-end • Persistent Chat • Mediation • Director You can see the status of the services on each server. If one or more of the required services are not running, the server will set an alarm.
IIS Services	Shows the detailed information about individual IIS services, such as the World Wide Web Publishing Server. You can view each service status, memory consumption, and CPU consumption.
MCU Health State	Individual graphs show the current health of the different types of conferences: • IMMCU - instant messaging (IM) conferences • ASMCU - application sharing conferences • AVMCU - audio/video (A/V) conferences • DATAMCU - data conferences
CMS Replication	Indicates if the current status of the Central Management Store (CMS) replication for this server is up to date by showing the following details: • The full qualified domain name of the CMS replica server. • Whether the Central Management Store Replica is up to date with the Central Management Store Master. • The latest date and time when the CMS master received a status package from the CMS replica. • The latest date and time when the CMS master generated a data package to the CMS replica and the version of Lync/Skype server.

Table 11. Lync/Skype drilldowns.

Drilldown	Associated Charts/Tabs
Database Queue Latency (ms)	In the drilldown you can see that database latency is determined by the following values: • Queue latency - The amount of time (in milliseconds) that it takes for a request to leave the front-end server queue toward the back-end database. A healthy Lync/Skype Server and SQL Server connection should show a value of less than 5000 msec. • Sproc latency (DBStore)- The amount of time (in milliseconds) that it takes to execute a sproc call for the database access component of Lync/Skype Server User Services Module. • Sproc latency (REGDBStore)- - The amount of time (in milliseconds) that it takes to execute a sproc call for the local registrar component of Lync/Skype Server Registrar Module.
OS/Subsystem	Individual graphs provide information about: • Percentage of CPU that is used by the operating system. • The amount of used and free space on the system disk. • The amount of system memory that is used and free (MB). • The time it takes to send a ping request from the diagnostic console to the Lync/Skype server.
Top CPU Consumer Top Memory Consumer	Shows all the processes on the server and how much CPU that each process is using, how much physical memory (MB) that each process is using, and the amount of virtual memory allocated to each process.
Network Output Queue	Represents the number of packets that are waiting to be sent through the network from the target server. Graphs are provided that show: • The total number of packets sent and received. • The total amount of kilobytes of data sent and received. • The number of packets handled by each network card. • The number of inbound and outbound errors and retries.
Theoretical Bandwidth	Shows details about the amount of kilobytes sent (per second), kilobytes received (per second), and the total number of kilobytes processed (per second).

Metrics

A metric is an individual piece of information that UC Diagnostics has collected about the performance of a system, such as perfmon counters. The information may be a numeric value (a number or percentage), a string of text, or some other piece of data.

Each time the UC Diagnostics window is refreshed, UC Diagnostics retrieves the latest value of the metric, which can be displayed in a drilldown or on the home page.

The Metric editor allows you to view and edit the properties of UC Diagnostics metrics, including their thresholds and severities. You can open the Metric editor for a component or a drilldown by right-clicking on the component and choosing Metrics from the invoked shortcut menu.

When you open the Metric editor, the General tab is open by default. Several metrics contain data source descriptions for the metric. The data source descriptions use the following list of functions.

Table 12. Lync/Skype metrics.

Function	Description
max(x)	the maximum of a set of values in list x
max(x,y)	the maximum of x and y
min(x)	the minimum of a set of values in list x

Table 12. Lync/Skype metrics.

Function	Description
count(x)	the number of values in list x
sum(x)	the sum of a set of values in list x
if(x,y,z)	if x is true, then return y, otherwise, return z
snull(x)	if x could not be collected, then return true
avg(x)	the average of values in list x

To view the perfmon counters

- Right-click a component and select **Metrics**.

The perfmon counter is visible in the Metric help section in the General tab.

Reporting Using Web Reports

- Understanding Web Reports
- Types of Reports

Understanding Web Reports

Web reports are a collection of web-based reports that are accessible from the following URL:
http://<servername>/UCDiagnostics.

The reports provide a tool to report on the usage of the messaging environment. These reports help you make informed decisions about the various methods of collaboration taking place in the environment.

You can perform the following tasks using Web reports:

- Use subscriptions to generate specific reports on a regular schedule. You can set up email notifications that either link to the reports or include attachments that contain actual report data.

- Create custom reports using the Web Report Wizard. You can build your own reports based on existing data sources. You can select fields, filters, format, grouping, and sorting options. Custom reports can be edited, depending on your security permissions within the Web reports, and saved for future use.

- Browse reports using the Reports Console, Toolbar Buttons, File Menu Commands, Treeview, Listview, Report Parts, Report Information, and Report and Quick Filters.

Other tasks you can perform include:

- Group, insert, append, remove, and sort fields on reports. Quick Filters allow you to change relevant report parameters quickly and easily to better focus your report.

- Display report data in bar graphs, line graphs, and pie charts.

- Export reports in Microsoft Excel, text (as comma-separated values or tab-separated values), XML, Word file, HTML, or MHTML

Web Reports Technical Information

UC Diagnostics has a separate web-based reporting component called UC Diagnostics Reports.

UC Diagnostics Reports provides a collection of reports called Preconfigured Reports. Preconfigured Reports allow report consumers to view data across multiple subsections of your organization. You can change relevant report parameters immediately using Quick Filters. UC Diagnostics Reports also provides a Web Report Wizard, which allows you to create customized reports based on any data available in your Web Reports database.

Security Recommendations

UC Diagnostics Diagnostic Pack for Exchange Web Reports supports both Windows Authentication and SQL Server Authentication. When you select SQL Server Authentication, the installer creates a Universal Data Link (UDL) file to store your SQL credentials. If you would like to protect your credentials to your UC Diagnostics database, you can do the following depending if you have installed Web Reports on the same computer as SQL database, or if you have Web Reports installed on a separate computer.

Table 1. Options for authentication.

If	Then
Web Reports (IIS web site) are installed on the same machine as your SQL database	Change your authentication from SQL Server Authentication to Windows Authentication.
Web Reports (IIS web site) are installed on a separate computer than your SQL database	Protect the UDL file by using New Technologies File System (NTFS) file permissions to guard against connection information being exposed or modified. Then, restrict the SQL account to have read-only rights to your database.

Types of Reports

To get data for a Web Report, you must first create a test. The test you run depends on the Web Report you want generated. For example, if you want to generate the CPU Utilization report or the BlackBerry Any Counter report, you must first run the BlackBerry Server Health Test.

The Web Reports hosts two types of reports: Custom Reports and Preconfigured Reports.

Custom Reports

You can create custom reports using the Web Report Wizard. The Web Report Wizard allows you to build your own reports based on existing data sources. You can select fields, filters, format, grouping, and sorting options. Custom reports can be edited, depending on your security clearance within Web Reports. You cannot create a chart from a custom report. You can create a chart from the Any Counter report.

Preconfigured Reports

Preconfigured Reports are specific to the application and are delivered with the product.

UC Diagnostics contains the following Web Reports.

Table 2. BlackBerry reports.

Web Report	Description
BlackBerry Any Counter	Allows you to report on any numeric counter available for the selected server. This report can be generated from data from the BlackBerry Server Health Test only.
BlackBerry CPU Utilization	Displays the BlackBerry servers in your Exchange organization and their respective CPU utilization.
BlackBerry Message Delivery	Displays message delivery information between Exchange and BlackBerry devices.
BlackBerry Physical Memory Utilization	Displays the BlackBerry servers in your Exchange organization and their respective physical memory utilization.
BlackBerry SRP Status	Displays connection status information between BlackBerry servers and SRP servers.
BlackBerry System Disk Utilization	Displays the BlackBerry servers in your BlackBerry organization and their respective system disk utilization.

Table 3. Exchange reports.

WEb Report	Description
Exchange Any Counter	Allows you to report on any numeric counter available for the selected server.
	This report can be generated from data from the Exchange Server Health test only.
Exchange Available Physical Memory	Displays the servers in your Exchange organization and their respective available physical memory. This report allows you to examine the performance of Exchange servers, identify bottlenecks, and upgrade servers when required.
Exchange CPU Utilization	Displays the servers in your Exchange organization and their respective CPU utilization.
Exchange External Message Delivery	Displays message delivery information between Exchange and external email addresses.
Exchange Internal Message Delivery	Displays information about message delivery between internal mailboxes within your Exchange organizations.
Exchange Internal Server Delivery	Displays message delivery information between Exchange servers.
Exchange Queues	Displays the servers in your Exchange organization and their respective queues.
Exchange Storage Group Disk Utilization	Displays the storage groups in your Exchange organization and their respective disk utilization.
Exchange System Disk Utilization	Displays the servers in your Exchange organization and their respective system disk utilization.

Table 4. Exchange Online reports

Web Report	Description
Internal Message Delivery	Displays information about message delivery between Exchange on-premise mailboxes and Exchange Online mailboxes or between mailboxes within Exchange Online.
External Message Delivery	Displays message delivery information between Exchange Online and external email addresses.

Table 5. Generic reports

Web Report	Description
Any Counter	Allows you to report on any numeric counter available for the selected server.

Table 6. Lync/Skype for Business reports.

Web Report	Description
Lync/Skype Any Counter	Allows you to report on any numeric counter available for the selected server.
Lync/Skype Available Physical Memory	Displays the servers in your Lync or Skype for Business environment and their respective available memory.
Lync/Skype CPU Utilization	Displays the servers in your Lync or Skype for Business organization and their respective CPU utilization.
Lync/Skype System Disk Utilization	Displays the servers in your or Skype for Business environment and their respective system disk utilization.

Table 6. Lync/Skype for Business reports.

Web Report	Description
Lync/Skype Address Book Service Health	Displays the pools in your Lync or Skype for Business environment and their respective transaction latency, the time taken to verify connection to the Address Book Download web service.
Lync/Skype Audio/Video Conferencing Health	Displays the pools in your Lync or Skype for Business environment and their respective transaction latency, the time taken to verify an occurrence of an audio/video conference.
Lync/Skype Instant Messaging Conference Health	Displays the pools in your Lync or Skype for Business environment and their respective transaction latency, the time taken to verify if two users can sign on to Lync pool and Exchange messaging.
Lync/Skype Instant Messaging Health	Displays the pools in your Lync or Skype for Business environment and their respective transaction latency, the time taken to verify instant messaging and Exchange messaging sessions.
Lync/Skype Logon Registration Health	Displays the pools in your Lync or Skype for Business environment and their respective transaction latency, the time taken to verify if users can sign on to a Lync pool.
Lync/Skype Peer To Peer Audio Video Call Health	Displays the pools in your Lync or Skype for Business environment and their respective transaction latency, the time taken to verify the occurrence of a peer-to-peer audio/video conversation.
Lync/Skype Presence Status Health	Displays the pools in your Lync or Skype for Business environment and their respective transaction latency, the time taken to verify Exchange presence information and user log on to a Lync pool.
Lync/Skype Persistent Chat Message Health	Displays the pools in your Lync or Skype for Business environment and their respective transaction latency, the time taken to verify if two users can exchange messages using the Persistent Chat service.

Table 7. OCS reports.

WEb Report	Description
OCS Server at a Glance	Provides a summary of the specified Office Communications Server configuration and the activity occurring on that server.
OCS CPU Utilization	Displays the servers in your OCS organization and their respective CPU utilization.
OCS Critical Process Time	Displays the servers in your OCS environment and their respective critical process times.
OCS Available Physical Memory	Displays the servers in your OCS organization and their respective available physical memory.
OCS Critical Process Working Set	Displays the servers in your OCS environment and their critical process working sets.
OCS System Disk Utilization	Displays the servers in your OCS environment and their respective system disk utilization.
OCS Active Connections	Displays the servers in your OCS environment and their respective Active Connections.
OCS TLS Active Connections	Displays the servers in your OCS environment and their respective TLS Active Connections.
OCS Database Latency	Displays the amount of time a request, such as a stored procedure, spends in the database queue before it is executed.
OCS Database Physical Disk Usage	Displays the servers in your OCS organization and their physical disk utilization.
OCS IM Conferencing Load	Shows how many IM conferences are running on the servers, and how many users are connected to those conferences.

Table 7. OCS reports.

WEb Report	Description
OCS Telephony Conferencing Load	Shows how many Telephony conferences are running on the servers, and how many users are connected to those conferences.
OCS Audio/Video Conferencing Load	Shows how many Audio Video conferences are running on the servers, and how many users are connected to those conferences.
OCS Web Conferencing Load	Shows how many Web conferences are running on the servers, and how many users are connected to those conferences.
OCS Any Counter	Allows you to report on any numeric counter available for the selected server.

You can specify counter names available in the server on which you want to report.

To report on a specific counter

1   Select **File | New Custom Report,** and click **Next**.

2   Select **OCS Any Counter Daily** or **OCS Any Counter Hourly**, and click **Next**.

3   Move **Counter Value** and/or **Counter Name** to Selected Fields, and click **Next**.

4   As filter criteria, select **Counter Name** and/or **Counter Value**, then select a parameter, then select a counter name or value. Click **Next**.

5   If necessary, click **Add New Filters** to define additional filters. When done, click **Next**.

6   Select how you would like to group the new reports, and click **Next**.

7   Select how you would like to sort the report, and click **Next**.

8   Configure how you would like to format your report, and click **Next**.

9   Add a description if desired, and click **Next**.

10 Click **Finish**.

Counters with Non-Zero Alarm Values

Some of the monitored counters are subject to spikes, short bursts that exceed a threshold but quickly return to normal levels. To avoid raising unnecessary alerts, each counter has a parameter that is displayed as Alarms To Skip. An alert is raised only if a count exceeds its threshold for a number of consecutive monitoring intervals that exceeds the value of this parameter.

For example, if the Alarms To Skip parameter has a value of 2, then 3 consecutive measurements above the threshold are required to raise an alert.

This appendix provides the recommended values for the Alarms To Skip parameter. Counters that do not appear in this appendix have a recommended value of zero.

If you have created the Server Health tests in a previous release, your parameter values do not change during upgrade. However, the recommended value for a counter may have changed since your previous release. Review the tables that follow.

Table 1. Preconfigured values for Exchange 2007 client access server (CAS) counters.

Counter	Preconfigured Value
MSExchangeOWA\Average Response Time	3

Table 2. Preconfigured values for Exchange 2007 edge transport server counters.

Counter	Preconfigured Value
MSExchangeTransportQueues\Active Mailbox Delivery Queue Length	1
MSExchangeTransportQueues\Active Non-SMTP Delivery Queue Length	1
MSExchangeTransportQueues\Aggregate Delivery Queue Length (All Queues)	1
MSExchangeTransportQueues\Largest Delivery Queue Length	1
MSExchangeTransportQueues\Submission Queue Length	1

Table 3. Preconfigured values for Exchange 2007 hub server counters.

Counter	Preconfigured Value
MSExchangeTransportQueues\Active Mailbox Delivery Queue Length	1
MSExchangeTransportQueues\Active Non-SMTP Delivery Queue Length	1
MSExchangeTransportQueues\Aggregate Delivery Queue Length (All Queues)	1
MSExchangeTransportQueues\Largest Delivery Queue Length	1
MSExchangeTransportQueues\Submission Queue Length	1

Table 4. Preconfigured values for Exchange 2007 server counters.

Counter	Preconfigured Value
PhysicalDisk\Avg. Disc sec/Read	1
PhysicalDisk\Avg. Disc sec/Write	1
PhysicalDisk\Current Disk Queue Length (<All instances except _Total>)	1
Memory\Available MBytes	1
Network Interface\Bytes Total/sec	1

Table 5. Preconfigured values for Exchange 2007 mailbox server counters.

Counter	Preconfigured Value
MSExchangeISClient\RPC Average Latency (<All instances>)	1
MSExchangeISMailbox\Messages Queued for Submission (_Total)	1
MSExchangeISMailbox\Receive Queue Size (_Total)	1
MSExchangeISPublic\Messages Queued for Submission (_Total)	1
MSExchangeISPublic\Receive Queue Size (_Total)	1
MSExchangeIS\RPC Average Latency	1

Table 6. Preconfigured values for Exchange 2010 client access server (CAS) counters.

Counter	Preconfigured Value
MSExchangeOWA\Average Response Time	3

Table 7. Preconfigured values for Exchange 2010 edge transport server counters.

Counter	Preconfigured Value
MSExchangeTransportQueues\Active Mailbox Delivery Queue Length (<All instances>)	1
MSExchangeTransportQueues\Active Non-SMTP Delivery Queue Length (<All instances>)	1
MSExchangeTransportQueues\Aggregate Delivery Queue Length (All Queues) (<All instances>)	1
MSExchangeTransportQueues\Largest Delivery Queue Length (<All instances>)	1
MSExchangeTransportQueues\Submission Queue Length (<All instances>)	1

Table 8. Preconfigured values for Exchange 2010 hub server counters.

Counter	Preconfigured Value
MSExchangeTransportQueues\Active Mailbox Delivery Queue Length (<All instances>)	1
MSExchangeTransportQueues\Active Non-SMTP Delivery Queue Length (<All instances>)	1
MSExchangeTransportQueues\Aggregate Delivery Queue Length (All Queues) (<All instances>)	1
MSExchangeTransportQueues\Largest Delivery Queue Length (<All instances>)	1
MSExchangeTransportQueues\Submission Queue Length (<All instances>)	1

Table 9. Preconfigured values for Exchange 2010 server counters.

Counter	Preconfigured Value
PhysicalDisk\Avg. Disc sec/Read (<All instances except _Total>)	1
PhysicalDisk\Avg. Disc sec/Write (<All instances except _Total>)	1
PhysicalDisk\Current Disk Queue Length (<All instances except _Total>)	1
Memory\Available MBytes	1
Network Interface\Bytes Total/sec (<All instances except _Total>)	1

Table 10. Preconfigured values for Exchange 2010 mailbox server counters.

Counter	Preconfigured Value
MSExchangeISClient\RPC Average Latency (<All instances>)	1
MSExchangeISMailbox\Messages Queued for Submission (_Total)	1
MSExchangeISMailbox\Receive Queue Size (_Total)	1
MSExchangeISPublic\Messages Queued for Submission (_Total)	1
MSExchangeISPublic\Receive Queue Size (_Total)	1
MSExchangeIS\RPC Averaged Latency	1

Table 11. Preconfigured values for Exchange 2013/2016 server counters.

Counter	Preconfigured Value
Memory\Available MBytes	2
Memory\% Committed Bytes in Use	2
MSExchangeADAccess Domain Controllers\LDAP Searches Timed out per Minute (<All instances>)	2
Network Interface\Bytes Total/sec (<All instances except _Total>)	1
PhysicalDisk\Avg.Disk Sec/Read (<All instances except _Total>)	1
PhysicalDisk\Current Disk Queue Length (<All instances except _Total>)	1

Table 12. Preconfigured values for Exchange 2013 mailbox server counters.

Counter	Preconfigured Value
MSExchangeISClient\RPC Average Latency (<All instances>)	1
MSExchange Assistants - Per Assistant\Average Event Processing Time in Seconds (microsoft exchange mailbox tranport submission - total)	3
MSExchange Assistants - Per Assistant\Percentage of Failed Events Dispatchers (calendarassistant)	2
MSExchange Assistants - Per Assistant\Average Event Processing Time in Seconds (sexchangemailboxassistants)	2
MSExchange Assistants - Per Assistant\Average Event Processing Time in Seconds (esourcebookingassistant)	2
MSExchange Availability Service\Average Time to Process a Free Busy Request	2
MSExchange Database ==> Instances\I/O Database Reads (Recovery) Average Latency (_Total)	3

Table 12. Preconfigured values for Exchange 2013 mailbox server counters.

Counter	Preconfigured Value
MSExchange Database ==> Instances\I/O Log Writes Average Latency (_Total)	3
MSExchange Database ==> Instances\Log Bytes Write/sec (_Total)	3
MSExchange Database ==> Instances\Log Generation Checkpoint Depth (_Total)	3
MSExchange OWA\Average Response Time	6
MSExchange Replication\Failed (<All instances except _Total>)	1
MSExchange Replication\FailedSuspended (<All instances except _Total>)	1
MSExchange Replication\Suspended (<All instances except _Total>)	1
MSExchange RpcClientAccess Per Server\RPC Active Backend Connections (% of Limit) (<All instances>)	5
MSExchange RpcClientAccess Per Server\RPC Average Latency (Backend) (<All instances>)	5
MSExchange RpcClientAccess Per Server\RPC Average Latency (End To End) (<All instances>)	5
MSExchange RpcClientAccess Per Server\RPC Failed Backend Connections (<All instances>)	5
MSExchange RpcClientAccess\RPC Averaged Latency	1
MSExchange Throttling Service Client\Percentage of Bypassed Submission Requests. (<All instances>)	5
MSExchange Throttling Service Client\Percentage of Denied Submission Request. (<All instances>)	5
MSExchangeAB\NSPI RPC Requests Average Latency	5
MSExchangeIS Client Type\RPC Average Latency (_Total)	1
MSExchangeIS Store\Messages Delivered/sec (_Total)	1
MSExchangeIS Store\Messages Submitted/sec (_Total)	1
MSExchangeTransport Delivery Failures\Delivery Agent: Total Delivery Failures	1
MSExchangeTransport Delivery Failures\Foreign Connector: Total Delivery Failures	1
MSExchangeTransport Delivery Failures\Resolver: Percentage of 5.1.4 Failures	1
MSExchangeTransport Delivery Failures\Resolver: Percentage of 5.2.0 Failures	1
MSExchangeTransport Delivery Failures\Resolver: Percentage of 5.2.4 Failures	1
MSExchangeTransport Delivery Failures\Resolver: Percentage of 5.4.6 Failures	1
MSExchangeTransport Delivery Failures\Routing: Percentage of 5.4.4 Failures	1
MSExchangeTransport Delivery Failures\SMTP: Percentage of 5.6.0 Failures	1
MSExchangeTransport Delivery Failures\Store Driver: Percentage of 5.2.0 Failures	1
MSExchangeTransport Delivery Failures\Store Driver: Percentage of 5.6.0 Failures	1
MSExchangeTransport DSN\Delay DSNs (internal)	12
MSExchangeTransport Queues\Active Mailbox Delivery Queue Length (_Total)	1
MSExchangeTransport Queues\Active Non-Smtp Delivery Queue Length (_Total)	1
MSExchangeTransport Queues\Categorizer Job Availability (_total)	1
MSExchangeTransport Queues\External Active Remote Delivery Queue Length (_Total)	1
MSExchangeTransport Queues\External Aggregate Delivery Queue Length (All External Queues) (_Total)	2
MSExchangeTransport Queues\External Largest Delivery Queue Length (_Total)	2
MSExchangeTransport Queues\Internal Active Remote Delivery Queue Length (_Total)	1

Table 12. Preconfigured values for Exchange 2013 mailbox server counters.

Counter	Preconfigured Value
MSExchangeTransport Queues\Internal Aggregate Delivery Queue Length (All Internal Queues) (_Total)	2
MSExchangeTransport Queues\Internal Largest Delivery Queue Length (_Total)	2
MSExchangeTransport Queues\Messages Completing Categorization (_total)	1
MSExchangeTransport Queues\Poison Queue Length (_Total)	2
MSExchangeTransport Queues\Retry Mailbox Delivery Queue Length (_Total)	1
MSExchangeTransport Queues\Retry Mailbox Delivery Queue Length (_Total)	3
MSExchangeTransport Queues\Submission Queue Length (_Total)	1
MSExchangeTransport Queues\Unreachable Queue Length (_Total)	1
MSExchangeTransport ServerAlive\Server Alive (_total*)	1
MSExchangeTransport SMTPAvailability\% Activity (client proxy)	1
MSExchangeTransport SMTPAvailability\% Activity (default)	1
MSExchangeUMAvailability\Total Queued Messages	1

Table 13. Preconfigured values for Exchange 2016 mailbox server counters.

Counter	Preconfigured Value
MSExchangeISClient\RPC Average Latency (<All instances>)	1
MSExchange Assistants - Per Assistant\Average Event Processing Time in Seconds (msexchangesubmission-total)	3
MSExchange Assistants - Per Assistant\Percentage of Failed Events Dispatchers (calendarassistant)	2
MSExchange Assistants - Per Assistant\Average Event Processing Time in Seconds (sexchangemailboxassistants)	2
MSExchange Assistants - Per Assistant\Average Event Processing Time in Seconds (esourcebookingassistant)	2
MSExchange Availability Service\Average Time to Process a Free Busy Request	2
MSExchange Database ==> Instances\I/O Database Reads (Recovery) Average Latency (_Total)	3
MSExchange Database ==> Instances\I/O Log Writes Average Latency (_Total)	3
MSExchange Database ==> Instances\Log Bytes Write/sec (_Total)	3
MSExchange Database ==> Instances\Log Generation Checkpoint Depth (_Total)	3
MSExchange OWA\Average Response Time	6
MSExchange Replication\Failed (<All instances except _Total>)	1
MSExchange Replication\FailedSuspended (<All instances except _Total>)	1
MSExchange Replication\Suspended (<All instances except _Total>)	1
MSExchange RpcClientAccess\RPC Averaged Latency	1
MSExchange Throttling Service Client\Percentage of Bypassed Submission Requests. (<All instances>)	5
MSExchange Throttling Service Client\Percentage of Denied Submission Request. (<All instances>)	5
MSExchangeAB\NSPI RPC Requests Average Latency	5
MSExchangeIS Client Type\RPC Average Latency (_Total)	1
MSExchangeIS Store\Messages Delivered/sec (_Total)	1
MSExchangeIS Store\Messages Submitted/sec (_Total)	1

Table 13. Preconfigured values for Exchange 2016 mailbox server counters.

Counter	Preconfigured Value
MSExchangeTransport Delivery Failures\Delivery Agent: Total Delivery Failures	1
MSExchangeTransport Delivery Failures\Foreign Connector: Total Delivery Failures	1
MSExchangeTransport Delivery Failures\Resolver: Percentage of 5.1.4 Failures	1
MSExchangeTransport Delivery Failures\Resolver: Percentage of 5.2.0 Failures	1
MSExchangeTransport Delivery Failures\Resolver: Percentage of 5.2.4 Failures	1
MSExchangeTransport Delivery Failures\Resolver: Percentage of 5.4.6 Failures	1
MSExchangeTransport Delivery Failures\Routing: Percentage of 5.4.4 Failures	1
MSExchangeTransport Delivery Failures\SMTP: Percentage of 5.6.0 Failures	1
MSExchangeTransport Delivery Failures\Store Driver: Percentage of 5.2.0 Failures	1
MSExchangeTransport Delivery Failures\Store Driver: Percentage of 5.6.0 Failures	1
MSExchangeTransport DSN\Delay DSNs (internal)	12
MSExchangeTransport Queues\Active Mailbox Delivery Queue Length (_Total)	1
MSExchangeTransport Queues\Active Non-Smtp Delivery Queue Length (_Total)	1
MSExchangeTransport Queues\Categorizer Job Availability (_total)	1
MSExchangeTransport Queues\External Active Remote Delivery Queue Length (_Total)	1
MSExchangeTransport Queues\External Aggregate Delivery Queue Length (All External Queues) (_Total)	2
MSExchangeTransport Queues\External Largest Delivery Queue Length (_Total)	2
MSExchangeTransport Queues\Internal Active Remote Delivery Queue Length (_Total)	1
MSExchangeTransport Queues\Internal Aggregate Delivery Queue Length (All Internal Queues) (_Total)	2
MSExchangeTransport Queues\Internal Largest Delivery Queue Length (_Total)	2
MSExchangeTransport Queues\Messages Completing Categorization (_total)	1
MSExchangeTransport Queues\Poison Queue Length (_Total)	2
MSExchangeTransport Queues\Retry Mailbox Delivery Queue Length (_Total)	1
MSExchangeTransport Queues\Retry Mailbox Delivery Queue Length (_Total)	3
MSExchangeTransport Queues\Submission Queue Length (_Total)	1
MSExchangeTransport Queues\Unreachable Queue Length (_Total)	1
MSExchangeTransport ServerAlive\Server Alive (_total*)	1
MSExchangeTransport SMTPAvailability\% Activity (client proxy)	1
MSExchangeTransport SMTPAvailability\% Activity (default)	1
MSExchangeUMAvailability\Total Queued Messages	1

Table 14. Preconfigured values for BlackBerry configuration server counters.

Counter	Preconfigured Value
Physical Disk\Current Disk Queue Length	1
Processor\Processor Time	1

Table 15. Preconfigured values for BlackBerry enterprise server counters.

Counter	Preconfigured Value
Physical Disk\Current Disk Queue Length	1
Memory\Available MBytes	1
Network Interface\Output Queue Length	1
Network Interface\Bytes Total	1

Table 16. Preconfigured values for OCS 2007 R2 server counters.

Counter	Preconfigured Value
Process\% Processor Time	1
Memory\Available MBytes	1
Memory\Pages/sec	1
Network Interface\Bytes Total/sec	1
PhysicalDisk\% Idle Time	1
PhysicalDisk\Av.g Disk Read Queue Length	1
PhysicalDisk\Avg.Disk sec/Read	1
PhysicalDisk\Avg. Disk sec/Transfer	1
PhysicalDisk\Avg. Disk sec/Write	1
PhysicalDisk\Avg. Disk Write Queue Length	1
PhysicalDisk\Current Disk Queue Length (_Total)	1
PhysicalDisk\Current Disk Queue Length	1
System\Processor Queue Length	1

Table 17. Preconfigured values for OCS Archiving server counters.

Counter	Preconfigured Value
Process\% Processory Time (RTCARCH)	1
LC:Arch Service - 00 - DBArch\Arch Service - 002 - Queue Latency (msec)	1
LC:Arch Service - 00 - DBArch\Arch Service - 000 - Queue Depth	1
LC:Arch Service - 00 - DBArch\Arch Service - 004 - Sproc Latency (msec)	1

Table 18. Preconfigured values for OCS 2007 R2 archiving server counters.

Counter	Preconfigured Value
Process\% Processory Time (RTCARCH)	1
LC:Arch Service - 00 - DBArch\Arch Service - 002 - Queue Latency (msec)	1
LC:Arch Service - 00 - DBArch\Arch Service - 000 - Queue Depth	1
LC:Arch Service - 00 - DBArch\Arch Service - 004 - Sproc Latency (msec)	1

Table 19. Preconfigured values for OCS conferencing web server counters.

Counter	Preconfigured Value
Process\% Processory Time (DATAMCUSVC)	1
LC:DATAMCU - 01 - CCCP Processing\DATAMCU - 0259 - Average processing time of incoming CCCP messages	3

Table 20. Preconfigured values for OCS 2007 R2 conferencing web server counters.

Counter	Preconfigured Value
Process\% Processory Time (DATAMCUSVC)	1
AVMCU - 03 - CCCP Processing\AVMCU - 029 - Average Processing time of incoming CCCP messages	3

Table 21. Preconfigured values for OCS 2007 R2 conferencing application sharing server counters.

Counter	Preconfigured Value
AVMCU - 03 - CCCP Processing\AVMCU - 029 - Average processing time of incoming CCCP messages	3

Table 22. Preconfigured values for OCS 2007 R2 conferencing AV server counters.

Counter	Preconfigured Value
Process\% Processory Time (AVMCUSVC)	1
AVMCU - 03 - CCCP Processing\AVMCU - 029 - Average processing time of incoming CCCP messages	3

Table 23. Preconfigured values for OCS 2007 R2 conferencing IM server counters.

Counter	Preconfigured Value
Process\% Processory Time (IMMCUSVC)	1
LC:ImMcu - 01 - CCCP Processing\IMMCU - 029 - Average processing time of incoming CCCP messages	3

Table 24. Preconfigured values for OCS CWA server counters.

Counter	Preconfigured Value
CWA - 01 - Authentication Module\CWA - 016 - Average latency for successful authorization (_Total)	1

Table 25. Preconfigured values for OCS database server counters.

Counter	Preconfigured Value
Process\Page Faults/sec(SQLSERVER*)	1
Process\% Processor Time (SQLSERVER*)	1
Memory\Pages/sec	1

Table 26. Preconfigured values for OCS 2007 R2 database server counters.

Counter	Preconfigured Value
Process\Page Faults/sec(SQLSERVER*)	1
Process\% Processor Time (SQLSERVER*)	1
Memory\Pages/sec	1

Table 27. Preconfigured values for OCS director server counters.

Counter	Preconfigured Value
PhysicalDisk\Avg. Disk sec/Read	1
PhysicalDisk\Avg. Disk sec/Write	1
PhysicalDisk\Current Disk Queue Length	1
Memory\Available MBytes	1
Memory\Pages/sec	1
Memory\Pool Paged Bytes	1
Memory\Pool Non-Pages Bytes	1
Network Interface\Bytes Total/sec	1

Table 28. Preconfigured values for OCS edge access server counters.

Counter	Preconfigured Value
Process\% Processor Time(RTCSRV)	1
LC:SIP - 01 - Peers\SIP - 019 - Sends Timed-Out/sec(_Total)	1
LC:SIP - 01 - Peers\SIP - 020 - Average Outgoing Queue Delay(_Total)	1
LC:SIP - 02 - Protocol\SIP - 005 - Incoming Requests Dropped/sec:	1
LC:SIP - 02 - Protocol\SIP - 009 - Incoming Responses Dropped/sec	1
LC:SIP - 02 - Protocol\SIP - 021 - Average Incoming Message Processing Time	1
LC:SIP - 09 - Access Edge Server Messages\SIP - 003 - External Messages/sec Received With Allowed Partner Server Domain	1
LC:SIP - 09 - Access Edge Server Messages\SIP - 005 - External Messages/sec Received With IM Service Provider Domain	1
LC:SIP - 09 - Access Edge Server Messages\SIP - 007 - External Messages/sec Received With a Configured Allowed Domain	1
LC:SIP - 09 - Access Edge Server Messages\SIP - 009 - External Messages/sec Received With a Discovered Domain	1
LC:SIP - 09 - Access Edge Server Messages\SIP - 021 - Messages/sec Dropped Due To Unknown Domain	1
LC:SIP - 09 - Access Edge Server Messages\SIP - 027 - External Messages/sec Dropped Due To Blocked Domain	1
LC:SIP - 09 - Access Edge Server Messages\SIP - 029 - Remote User Client Messages/sec Dropped Due To Unsupported Internal Domain	1
LC:SIP - 09 - Access Edge Server Messages\SIP - 049 - Messages/sec From Users Not Enabled For Federation	1
LC:SIP - 09 - Access Edge Server Messages\SIP - 051 - Messages/sec From Users Not Enabled For Public IM Providers	1

Table 28. Preconfigured values for OCS edge access server counters.

Counter	Preconfigured Value
LC:SIP - 09 - Access Edge Server Messages\SIP - 053 - External Messages/sec Dropped Due To Unresolved Domain	1
LC:SIP - 09 - Access Edge Server Messages\SIP - 055 - External Messages/sec Dropped Due To Blocked IM Service Provider Domain	1
LC:SIP - 09 - Access Edge Server Messages\SIP - 057 - External Messages/sec Dropped Due To Unauthorized IM Service Provider Domain	1
LC:SIP - 09 - Access Edge Server Messages\SIP - 059 - External Messages/sec Dropped Due To Unauthorized Allowed or Discovered Domain	1
LC:SIP - 09 - Access Edge Server Messages\SIP - 061 - External Messages/sec Dropped Due To Incompatible Message Domain	1
LC:SIP - 09 - Access Edge Server Messages\SIP - 063 - Messages/sec Dropped Due To Incompatible Asserted Identity	1

Table 29. Preconfigured values for OCS 2007 R2 edge access counters.

Counter	Preconfigured Value
Process\% Processor Time(RTCSRV)	1
LC:SIP - 02 - Protocol\SIP - 005 - Incoming Requests Dropped/sec:	1
LC:SIP - 02 - Protocol\SIP - 009 - Incoming Responses Dropped/sec	1

Table 30. Preconfigured values for OCS edge AV server counters.

Counter	Preconfigured Value
Process\% Processor Time (MRASSVC)	1
Process\% Processor Time (MEDIARELAYSVC)	1
A/V Edge - 02 - Total Counters\-023 - Packets Dropped/sec (_Total)	1

Table 31. Preconfigured values for Lync 2010, Lync 2013, and Skype for Business 2015 server counters.

Counter	Preconfigured Value
Ping Time in milliseconds	2
Memory\% Committed Bytes in Use	2
Memory\Available MBytes	2
Network Interface\Bytes Total/sec (<All instances except _Total>)	1
PhysicalDisk\Avg.Disk sec/Read (<All instances except _Total>)	1
PhysicalDisk\Current Disk Queue Length (<All instances except _Total>)	1

Glossary

This glossary includes definitions taken from Microsoft publications.

C

Custom Group

An arbitrary group of servers created to simplify test management.

D

Database Availability Group (DAG)

A clustering functionality for Exchange 2010 and later servers that ensures fast recovery from a network, server, or database failure.

Diagnostic Console

A console that allows you to monitor and troubleshoot one server at a time.

Domain

A logical collection of resources consisting of computers, printers, and computer and user accounts. A domain also has a system of logon authentication of computer and user accounts.

Domain Controller (DC)

A server that authenticates domain logon passwords. It maintains security policy and the security accounts master database for a domain.

F

Federation

Allows users to provide presence information with external clients.

Forest

A collection of domains and domain trees.

G

Global Filter

Allows you to hide any servers in which you are not interested. It hides the servers from both the treeview and topology view.

H

Health Test

Detects problems by collecting and analyzing data or simulating user interaction with the server at regular intervals

M

Maintenance Mode

Allows you to mark servers as offline so that you can perform maintenance on those servers

Management Console

A console that unifies and simplifies day-to-day system management tasks. It hosts tools and displays them as consoles. These tools, consisting of one or more applications, are built with modules called snap-ins.

W

Web Reports

A tool that provides administrators with a tool to report on usage and trends.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.

Index