Monitoring Microsoft Client Access Server

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The Client Access server role is required in every Exchange server 2007/2010 organization.

The Client Access server role supports the Microsoft Outlook Web Access and Microsoft Exchange ActiveSync client applications and the Post Office Protocol version 3 (POP3) and Internet Message Access Protocol version 4rev1 (IMAP4) protocols. The Client Access server role also supports services, such as the Autodiscover service and Web services.

The Client Access server role accepts connections to your Exchange 2007/2010 server from a variety of different clients. Software clients such as Microsoft Outlook Express and Eudora use POP3 or IMAP4 connections to communicate with the Exchange server. Hardware clients, such as mobile devices, use ActiveSync, POP3, or IMAP4 to communicate with the Exchange server.

Failure of any of these protocols or issues in network connection between the clients and the server can disrupt client-server communication and cause critical emails to go undelivered. In order to avoid such adversities, the operations of the Client Access server should be continuously monitored, and administrators proactively alerted to abnormalities. This is where eG Enterprise helps administrators.

Chapter 2: How to Monitor Microsoft Exchange 2007/2010 Servers with Client Access Server Role Using eG Enterprise

eG Enterprise adopts an agent-based approach to monitoring the Exchange 2007/2010 Client access server. The agent-based approach requires that you install and configure the eG agent on the Exchange 2007/2010 host (if one of the 'integrated' Exchange 2007 or Exchange 2010 models is being used) or on the host on which the server role to be monitored exists.

This internal agent, once started, periodically runs a wide variety of tests on the Exchange 2007/2010 server/server role to extract useful performance data. Some of these tests , namely – the Exchange Mailbox Status test, the Exchange Storage Group test, and the Exchange Queue Stats test – require **Exchange Administrator** privileges to execute. Therefore, prior to monitoring an Exchange 2007/2010 server/server role using eG Enterprise, make sure that you configure the eG agent to run with the privileges of an **Exchange Administrator**. Then, proceed to monitor the Microsoft Exchange Mailbox Server.

The broad steps for monitoring Microsoft Exchange Mailbox Server using eG Enterprise are as follows:

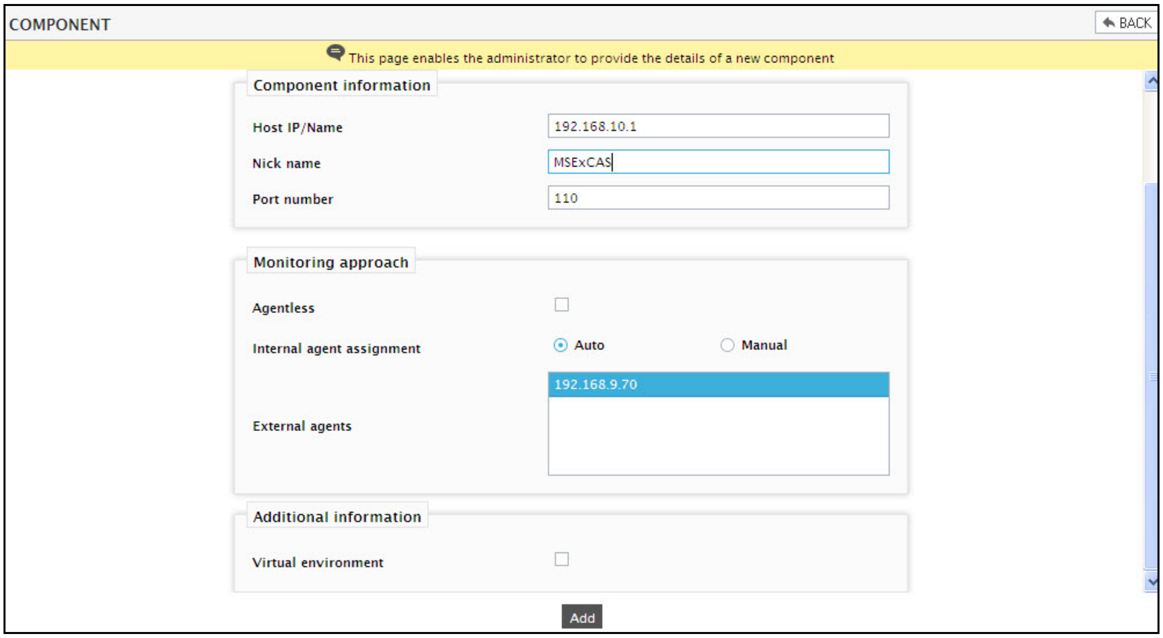
- Managing the Microsoft Exchange Client Access Server
- Configuring the tests

These steps have been discussed in this topic.

2.1 Managing the Microsoft Exchange Client Access Server

The eG Enterprise cannot automatically discover the Microsoft Exchange Client Access Server. This implies that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To manage a Exchange Client Access Server component, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENT** page that appears next, select *Microsoft Exchange Client Access Server* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.



This page enables the administrator to provide the details of a new component

Component information

Host IP/Name: 192.168.10.1

Nick name: MSExCAS

Port number: 110

Monitoring approach

Agentless □

Internal agent assignment ● Auto ○ Manual

External agents: 192.168.9.70

Additional information

Virtual environment □

Figure 2.1: Adding a Microsoft Exchange Client Access Server

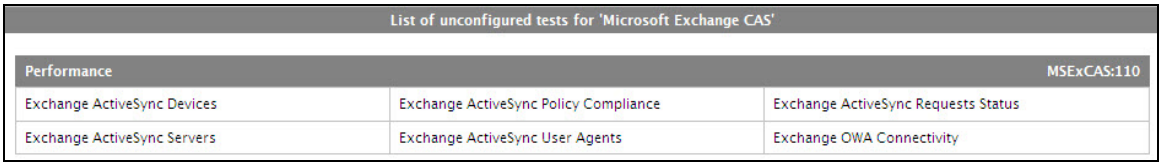
4. Specify the **Host IP** and the **Nick name** of the Exchange Client Access Server in Figure 2.1.

5. The **Port number** will be set as *110* by default. If the server is listening on a different port in your environment, then override this default setting.

6. Then, click the **Add** button to register the changes.

2.2 Configuring the tests

1. When you attempt to sign out of eG administrative interface, a list of unconfigured tests will appear as shown in Figure 2.2. This list reveals the unconfigured tests requiring manual configuration.



List of unconfigured tests for 'Microsoft Exchange CAS'

Performance		MSExCAS:110
Exchange ActiveSync Devices	Exchange ActiveSync Policy Compliance	Exchange ActiveSync Requests Status
Exchange ActiveSync Servers	Exchange ActiveSync User Agents	Exchange OWA Connectivity

Figure 2.2: List of unconfigured tests for the Microsoft Exchange Client Access Server

2. To configure the tests, click on the test names in the list of unconfigured tests. For the details on configuring the tests, refer to **Monitoring the Client Access Servers** chapter.

3. Once all the tests are configured, signout of the eG administrative interface.

Chapter 3: Monitoring the Client Access Servers

eG Enterprise prescribes a specialized Microsoft Exchange CAS model for monitoring Client Access servers.

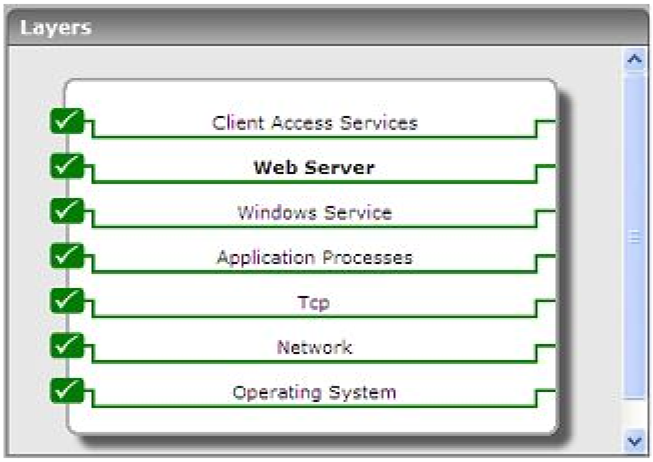


Figure 3.1: The layer model of the Client Access server

Each layer of Figure 3.1 reports critical performance metrics extracted from the Client access server, that enable administrators to answer the following questions easily and effectively.

- How efficient is the ActiveSync engine? Is it taking too long to process requests? How many requests to ActiveSync are still in queue?
- Were requests to the Availability service processed quickly?
- Were all connection requests to mailboxes serviced by the cache, or were any requests missed?
- What is the current session load on Outlook web access (OWA)?
- Does OWA respond swiftly to user requests?
- Does OWA take too long to complete search requests?
- Did any requests for web access fail?
- Is the Exchange web server responding promptly to requests?

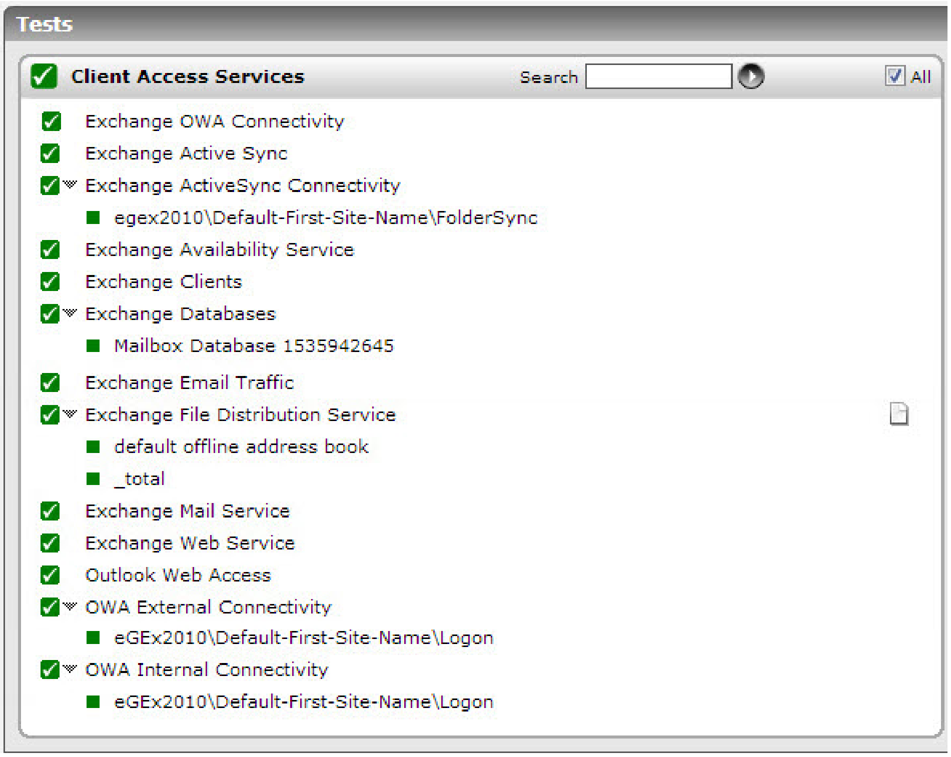
Since the bottom 6 layers of Figure 3.1 have already been discussed in the *Monitoring Unix and Windows Servers* document, the sections to come discuss the **Client Access Services** layer only.

3.1 The Client Access Services Layer

The tests mapped to this layer monitor the critical services offered by the Client Access server, which include:

- Exchange ActiveSync service
- Exchange Availability service
- Outlook Web Access service
- Exchange Web service

In addition, the layer monitors the availability of the Exchange 2007/2010 server to send and receive mails.



Tests

☑ Client Access Services   Search   ☑ All

- ☑ Exchange OWA Connectivity
- ☑ Exchange Active Sync
- ☑ Exchange ActiveSync Connectivity
  - 🟩 egex2010\Default-First-Site-Name\FolderSync
- ☑ Exchange Availability Service
- ☑ Exchange Clients
- ☑ Exchange Databases
  - 🟩 Mailbox Database 1535942645
- ☑ Exchange Email Traffic
- ☑ Exchange File Distribution Service
  - 🟩 default offline address book
  - 🟩 _total
- ☑ Exchange Mail Service
- ☑ Exchange Web Service
- ☑ Outlook Web Access
- ☑ OWA External Connectivity
  - 🟩 eGEx2010\Default-First-Site-Name\Logon
- ☑ OWA Internal Connectivity
  - 🟩 eGEx2010\Default-First-Site-Name\Logon

Figure 3.2: The tests associated with the Client Access Services layer

3.1.1 Exchange File Distribution Service Test

An Offline Address Book (OAB) is a container that stores a collection of Offline Address Lists. Typically, users download these address lists to obtain information about other users in their organization.

Exchange server 2007/2010 introduces a new mechanism for distributing Offline Address Books that does not involve Public Folders; it instead uses HTTP(S) and the Background Intelligent Transfer Service (BITS). This new web-based OAB distribution process depends on several components working together:

- **Exchange System Attendant Service** – this service runs on the mailbox server to create the OAB.
- **Exchange File Distribution Service** – this service runs on CAS (Client Access) servers and is responsible for obtaining the OAB content from the OABGen server.
- **OAB Virtual Directory** – This is an IIS virtual directory on a CAS server where the OAB is downloaded from.
- **Autodiscover** – Autodiscover runs on a CAS server and returns the correct OAB URL for a given client connection.

The OAB is typically generated on a mailbox server by the Exchange System Attendant Service. At configured intervals (default: every 8 hours), the Exchange Fle Distribution Service (FDS) on the CAS server polls the mailbox server for new OAB files. The first poll happens when the Exchange File Distribution Service starts; so, the exact time a server polls will be different on each CAS. If polling reveals new files, the Exchange Fle Distribution Service downloads the files from the mailbox server. The copied files are stored in a web distribution folder on the CAS server. The user then connects to the AutoDiscover service via Outlook to get the closest OAB distribution URL. Autodiscover returns the URL to the CAS server. Outlook then connects with BITS to the URL provided, and downloads the OAB.

From this, we can infer that the location of the CAS server, the quality of the network link between the CAS and the mailbox server, and the polling interval are key factors that influence the speed, frequency, and overall efficiency of the OAB download performed by the Exchange File Distribution Service. Carelessly made changes to the polling interval and issues with network connectivity can therefore significantly impact the OAB distribution process, thereby delaying users access to the latest information pertaining to other users.

Using the **Exchange File Distribution Service** test, you can periodically monitor the OAB downloads performed by the FDS service on the CAS server and promptly capture slowdowns (if any) in the downloading process and changes in polling interval (if any).

Target of the test : A server configured with the Client Access Server role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Client Access server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.
Port	The port number of the client access server. By default, this is 110.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Download task queued</td><td>Indicates whether any download tasks have been queued or not.</td><td></td><td>If one/more download tasks are in queue, this measure will report the value <i>Yes</i>. If no download tasks are in queue, then this measure will report the value <i>No</i>.
The numeric values that correspond to these measure values are as follows:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Yes</td><td>1</td></tr><tr><td>No</td><td>0</td></tr></table>
The value <i>Yes</i> for this measure could indicate that the CAS server is taking too much time to download the OAB files, thereby causing subsequent download tasks to be queued. The prolonged downloads could be due to a poor network link between the CAS server and the OAB Generation server. Slowdowns can also occur if a large number of OAB files are downloaded, or if the size of the OAB files is huge.
<b>Note:</b>
By default, this measure will report the <b>Measure Value</b>s in the table above to</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			indicate if any download task is pending. However, in the graph of this measure, the same will be represented using the numeric equivalents only.
Download task completed	Indicates the number of OAB downloads that have been completed since the last measurement period.	Number	Ideally, the value of this measure should be high. A very low value could indicate downloading bottlenecks that might require further investigation. Another reason for a change in the value of this measure is a change in the polling interval. While an increase in the polling frequency, can increase the value of this measure, a decrease in the polling frequency can cause a less number of download tasks to be completed and can hence, reduce the value of this measure. A reduction in the polling interval can cause critical updates to OAB files to be available to end users only after a long time.

3.1.2 Exchange Mail Service Test

This test monitors the availability and performance of a Microsoft Exchange 2007/2010 mail server from an external perspective. The test mimics a mail client activity by using the Exchange Web Service for sending and receiving mails.

Note:

For this test to execute smoothly, the external agent executing the test should be in the same domain as the Exchange 2007/2010 server.

Target of the test : A server configured with the Client Access Server role

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Client Access server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.
Port	The port number of the client access server. By default, this is 110.
From User Name	Provide the name of the **Exchange Administrator**, using whose credentials the eG agent executing this test is running. Alternatively, you can provide the email ID of the **Exchange Administrator** as well.
From User Password	Specify the password of the **Exchange Administrator**.
Confirm Password	Confirm the password by retyping it here.
Exchange Domain Name	Provide a valid domain in which the target server is running.

Web Service URL	To enable the test to connect to Exchange Web Services, you need to provide the **External Web Service URL** here. To know what URL to provide, run the following command from the Exchange server's powershell command prompt:
	`Get-WebServicesVirtualDirectory -server <servername> | select name, *url* | fl`
	For instance, if your Exchange server's name is **Exchange**, then your command will be:
	`Get-WebServicesVirtualDirectory -server Exchange | select name, *url* | fl`
	Upon successful execution of the command, a list of URLs will be displayed. Note down the URL displayed against the label **ExternalUrl** , and enter it against Web Service URL.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Send mail availability	Indicates the availability of the mail server for receiving the mails sent by the test.	Percent	A value of 0 indicates that the test was not successful in sending a mail. Possible reasons for this could include the mail server being down, the

Measurement	Description	Measurement Unit	Interpretation
			network connection to the server not being available, or the test configuration information being incorrect.
Sent messages	Indicates the number of messages sent to the mail server.	Number	A value of –1 indicates that the mail server may be down or the configuration information may be incorrect.
Avg time to send messages	Indicates time taken to send a mail to the mail server.	Secs	A high value of this measure could indicate high network traffic or that the mail server is busy.
Receive mail availability	Indicates the availability of the exchange server for sending mails to the mail client.	Percent	The value of 0 indicates that the test was not successful in receiving a mail message from the Exchange server. Possible reasons could be incorrect configuration information.
Received messages	Indicates the number of messages received by the mail client from the mail server.	Number	The value of 0 indicates that the test was not successful in receiving mail messages from the Exchange server. The possible reasons could be: • The sent messages could be in the message queue of the mail server but not routed to the mail box • Configuration information may be incorrect • Network failure • The mail service may not be running in the user account
Mail received time	Indicates the time taken by the mail client to receive a mail from the mail server.	Secs	A high value in this measure indicates that the mail server is busy or the network traffic is high.
Avg roundtrip time	The average of the round trip time (the time lapse	Mins	This is a key measure of quality of the mail service. An increase in roundtrip

Measurement	Description	Measurement Unit	Interpretation
	between transmission and reception of a message by the server) of all the messages received by the mail server during the last measurement period.		time may be indicative of a problem with the mail service. Possible reasons could include queuing failures, disk space being full, etc.
Max roundtrip time	The high water mark of the round trip time (the time lapse between transmission and reception of a message by the server) of all messages received by the mail server during the last measurement period.	Mins	If the value of the Received messages measure is 1, then the value of this measure will be the same as the *Avg roundtrip time* measure.

3.1.3 Exchange Active Sync Test

By default, when you install the Client Access server role on a computer that is running Microsoft Exchange server 2007/2010, you enable Microsoft Exchange ActiveSync. Exchange ActiveSync lets you synchronize a mobile device with your Exchange 2007/2010 mailbox.

Exchange ActiveSync is an Microsoft Exchange synchronization protocol (HTTP and XML) that is optimized to work together with high-latency and low-bandwidth networks. Exchange ActiveSync enables mobile device users to access their e-mail, calendar, contacts, and tasks and to continue to be able to access this information while they are working offline.

The performance of Microsoft Exchange ActiveSync is affected by many factors. These include the number of users who are synchronizing with Exchange ActiveSync, the types of mobile devices that are synchronizing with it, and how much data each user synchronizes between the Microsoft Exchange server and the mobile device. By using monitoring, you can understand the factors that affect the performance of Exchange ActiveSync.

This test measures the health of the ActiveSync engine.

Target of the test : A server configured with the Client Access Server role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Client Access server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.
Port	The port number of the client access server. By default, this is 110.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
ActiveSync request processing time	Indicates the average time elapsed waiting for a request to complete.	Secs	This measure includes Ping Request Time, which can increase the general response time. Adding ping counters helps clarify where performance is being impacted.
Ping commands pending on the server	Indicates the number of ping commands that are currently pending on the server.	Number	
Ping commands dropped	Indicates the number of Ping commands per second whose connection to the client was dropped before a response could be issued.	Dropped/sec	
ActiveSync requests to the server	Indicates the number of HTTP requests that are received from the client via ASP.NET per second.	Reqs/Sec	
ActiveSync requests queued for processing	Indicates the number of HTTP requests that are currently waiting to be assigned to a thread.	Number	A steady increase in this value over time is a cause for concern, as it is indicative of a processing bottleneck.
Sync commands processed	Indicates the number of sync commands that are	Number	

Measurement	Description	Measurement Unit	Interpretation
	currently processed by the server.		
Worker threads busy	Indicates the number of worker threads that are presently busy processing requests.	Number	
Worker threads idle	Indicates the number of worker threads that are currently idle.	Number	Ideally, this value should be low.

3.1.4 Exchange Availability Service Test

The Microsoft Exchange server 2007/2010 Availability service improves information workers' calendaring and meeting scheduling experience by providing secure, consistent, and up-to-date free and busy information to computers running Microsoft Office Outlook 2007. Outlook 2007 uses the Autodiscover service to obtain the URL of the Availability service. The Autodiscover service is similar to the Domain Name System (DNS) Web service for Exchange 2007/2010 Web services. Essentially, the Autodiscover service helps Outlook 2007 locate various Web services, such as the Unified Messaging (UM), Offline Address Book (OAB), and Availability services.

The following figure illustrates the process flow for the Availability service.

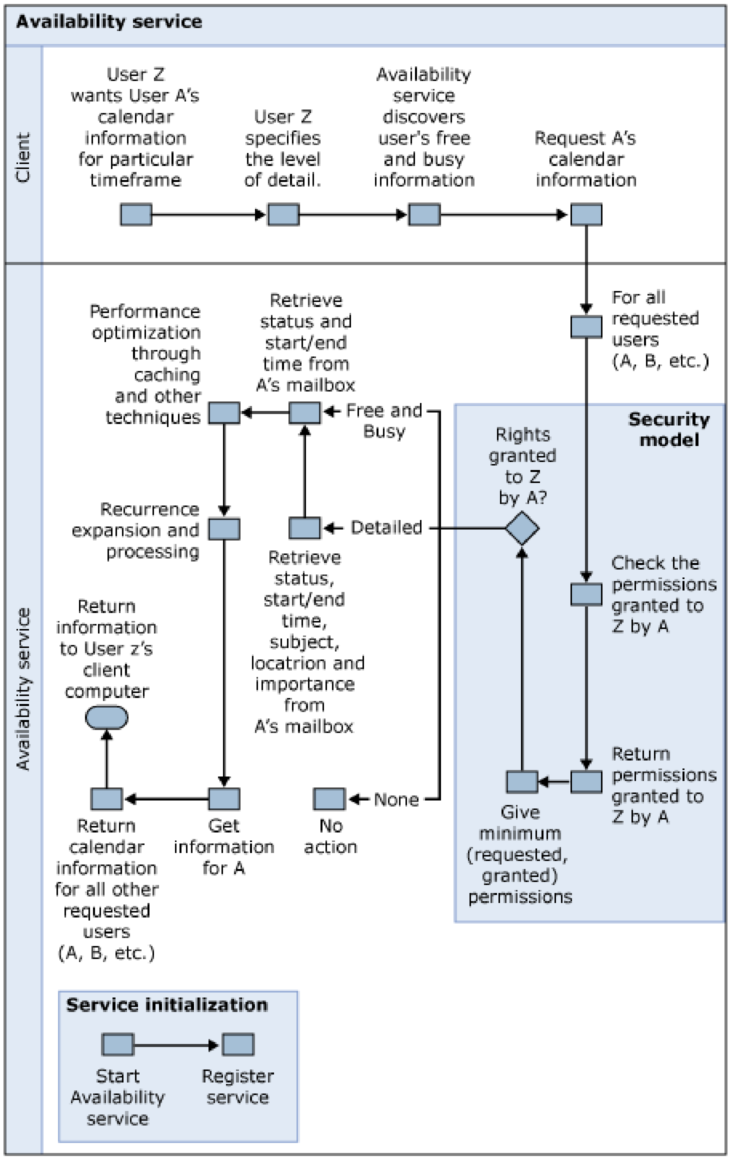

Availability service
Client
User Z wants User A's calendar information for particular timeframe
User Z specifies the level of detail.
Availability service discovers user's free and busy information
Request A's calendar information
Availability service
For all requested users (A, B, etc.)
Performance optimization through caching and other techniques
Retrieve status and start/end time from A's mailbox
Free and Busy
Security model
Rights granted to Z by A?
Recurrence expansion and processing
Detailed
Retrieve status, start/end time, subject, locatrion and importance from A's mailbox
Check the permissions granted to Z by A
Return information to User z's client computer
Return permissions granted to Z by A
None
Return calendar information for all other requested users (A, B, etc.)
Get information for A
No action
Give minimum (requested, granted) permissions
Service initialization
Start Availability service
Register service

Figure 3.3: The Availability Service

This test reports statistics indicating how healthy the Availability Service is.

Target of the test :A server configured with the Client Access Server role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Mailbox server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.
Port	The port number of the client access server. By default, this is 110.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Availability requests to the web service	Indicates the number of requests serviced per second.	Reqs/Sec	The request can be only for free busy or include suggestions. One request may contain multiple mailboxes. A very low request servicing rate could indicate a processing bottleneck.
Avg. mailboxes processed per request	Indicates the average number of mailboxes processed per request.	Mailboxes/Req	
Mailbox connection hits	Indicates the number of mailboxes opened per second without creating a new connection.	Hits/Sec	Ideally, this value should be high. A low cache hit rate could increase processing overheads.
Mailbox connection misses	Indicates the number of mailboxes opened per second, by creating a new connection, because there is no available connection in the cache.	Misses/Sec	Ideally, this measure should be low. A very high cache miss rate could indicate insufficient connections in the cache to service requests. You might want to consider resizing the cache.

3.1.5 Outlook Web Access Test

Outlook Web Access (OWA) is a HyperText Transfer Protocol (HTTP) virtual server that enables users to access their Microsoft Exchange inbox using a Web browser. In the event that users are unable to access their mailbox, you can use the metrics reported by this test to determine whether the problem in HTTP access is local to the client access server or not.

Target of the test : An Exchange 2007/2010 server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Client Access server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.
Port	The port number of the client access server. By default, this is 110.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Outlook web access sessions	Indicates the number of Outlook Web Access user sessions that are created per second.	Login/Sec	
Current unique web access users	Indicates the number of unique users currently logged on to Outlook Web Access.	Number	This value monitors the number of unique active user sessions, so that users are only removed from this count after they log off or their session times out.
Response time for web access - average	Indicates the average time in seconds that elapsed between the beginning and end of an OEH or ASPX request.	Secs	This is a good measure of the latency that a client is experiencing. Higher values may indicate high user load or higher than normal CPU time.
Search time during web access - average	Indicates the average time that elapsed while waiting for a search to complete.	Secs	Ideally, this value should be low at all times.
Request rate for web access	Indicates the number of requests handled by Outlook Web Access per second.	Reqs/Sec	
Failed requests for web access	Indicates the number of Outlook Web Access	Reqs/Sec	A zero value is typically desired. If the measure reports a non-zero value, the

Measurement	Description	Measurement Unit	Interpretation
	requests that failed, per second.		reason for the same should be investigated.
Store logon failures for web access	Indicates the percentage of Outlook Web Access user logons to Microsoft Exchange Mailbox servers that have failed currently.	Percent	Ideally, this value should be low.

3.1.6 Exchange Web Service Test

This test monitors requests from Exchange clients and reveals how quickly the Exchange 2007/2010 server responds to these requests.

Target of the test : An Exchange 2007/2010 server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Exchange 2007/2010 server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.
Port	The port number of the client access server. By default, this is 110.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Request rate to Exchange web server	Indicates the number of requests from clients that are processed each second.	Reqs/Sec	
Avg. response time for web service	Indicates the average time (in milliseconds) that has elapsed between the	Msecs	A high value for this measure is indicative of a slowdown in the responsiveness of the server.

Measurement	Description	Measurement Unit	Interpretation
	beginning and end of requests.		

3.1.7 Exchange RPC HTTP Test

This test assists you in assessing the load and issues with the RPC/HTTP Proxy component.

Target of the test : An Exchange 2007/2010 server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Exchange 2007/2010 server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.
Port	The port number of the client access server. By default, this is 110.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Current incoming RPCs	Indicates the number of front-end HTTP connections.	Number	This measure serves as a good indicator of the load imposed by the user.
Current unique users	Indicates the number of unique users currently connected to a back-end server via RPC/HTTP.	Number	This measure serves as a good indicator of level of user load.
RPC/HTTP requests	Indicates the rate of RPC/HTTP request send to the back-end server	Reqs/Sec	This measure indicates the current Outlook Anywhere load.
Failed backend connections	Indicates the rate at which the RPC proxy attempts	Conns/Sec	Ideally, this value should be 0.

Measurement	Description	Measurement Unit	Interpretation
	are occurring but fail to establish a connection to a back-end server.		

3.1.8 Exchange OWA Connectivity Test

This test verifies whether the Microsoft Office Outlook web app is running as expected. This test can be used to test Outlook Web App connectivity for all Microsoft Exchange Server 2010 virtual directories on a specified Client Access server for all mailboxes on servers running Exchange that are in the same Active Directory site.

This test is also used to test the connectivity for an individual Exchange Outlook Web App URL. To execute this test, you need to setup a test account in the exchange forest and you need to run the script which is available in the following location *\scripts\ new-TestCasConnectivityUser.ps1*.

Target of the test : An Exchange 2007/2010 server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Exchange 2007/2010 server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.
Port	The port number of the client access server. By default, this is 110.
XchgExtensionShellPath	The Exchange Management Shell is a command-line management interface, built on Windows PowerShell which enables you to administer every part of Microsoft Exchange. This test uses the Exchange management shell to run scripts and collect the desired performance metrics from the Exchange server. By default, the test auto-discovers the location of the Exchange management shell and thus, automatically loads the Exchange management shell snap-in (exshell.psc1) for script execution. This is why, the XchgExtensionShellPath is set to *none* by default.
Client Access Server	Specify the complete qualified hostname of the client access server in the Client Access Server text box.

Parameters	Description
Outlook Web App URL	Specify the website URL in the Outlook Web App URL. By Default, *none* will be provided.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Logon latency	Indicates the delay time in logging in to Outlook Web App.	Msecs	
OWA connectivity status	Indicates the status of the OWA connection.	MB	If the value of this measure reports to 100, it implies that the OWA connection is successfull, otherwise this measure reports to 0.

3.1.9 Exchange ActiveSync Connectivity Test

Exchange ActiveSync lets you synchronize a mobile device with your Exchange 2010 mailbox, so that you can check your emails from your mobile phone itself! Whenever a mobile phone user complaints that he/she is unable to check or is experiencing slowness when checking emails on his/her mobile phone, Exchange administrators need to quickly determine what is causing the non-sync – is it because ActiveSync is unable to synchronize with the user's mailbox? Or is it because ActiveSync is taking too long to perform the synchronization? At which stage of the synchronization did the failure/delay occur? This test helps answer all these questions. The test periodically checks ActiveSync connectivity at every stage (a.k.a scenario) of the synchronization – eg., the Logon stage, the FolderSync stage, the Options stage, etc. - reports issues and latencies (if any) in connectivity, and leads you to the exact stage at which the failure/slowdown occurred.

Target of the test : An Exchange 2010 server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each <ClientAccessServer>/<LocalSiteNameofClientAccessServer>/ <SynchronizationStage/Scenario tested>combination.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.
Port	The port number of the client access server. By default, this is 110.
XchgExtensionShellPath	The Exchange Management Shell is a command-line management interface, built on Windows PowerShell which enables you to administer every part of Microsoft Exchange. This test uses the Exchange management shell to run scripts and collect the desired performance metrics from the Exchange server. By default, the test auto-discovers the location of the Exchange management shell and thus, automatically loads the Exchange management shell snap-in (exshell.psc1) for script execution. This is why, the XchgExtensionShellPath is set to *none* by default.
Client Access Server	Specify the fully-qualified domain name of the Client Access server.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>ActiveSync connectivity status</td><td>Indicates whether the ActiveSync connectivity check was successful or not at this stage/scenario of the synchronization.</td><td></td><td>If the value of this measure is <i>Success</i>, it indicates that the ActiveSync connectivity check was successful at this stage. If the value of this measure is <i>Failure</i>, it indicates that mailbox synchronization using ActiveSync failed at this stage. The numeric values that correspond to these measure values are as follows:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Success</td><td>1</td></tr>
<tr><td>Failure</td><td>0</td></tr>
</table>
<b>Note:</b>
Typically, this measure reports the</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			Measure Values listed in the table above to indicate the ActiveSync connectivity status. However, in the graph of this measure, the Numeric values are used to represent the connectivity status.
ActiveSync latency	Indicates the time taken by ActiveSync to successfully complete this stage/scenario of the synchronization.	Secs	A low value is desired for this measure. A high value indicates that this stage/scenario of the synchronization is taking too long to complete. Compare the value of this measure across stages/scenarios to know where the maximum delay occurred. This will greatly aid troubleshooting.

3.1.10 OWA Internal Connectivity Test

Outlook Web App (OWA) is a browser-based email client accessible from the web. It allows you to check your email from computers that do not have an email client (such as Outlook 2010) installed. If an internal user (i.e., intranet user) complains that he/she is unable to check emails using OWA, you can run this test to figure out whether/not OWA is accessible, and if so, how long it takes to connect to OWA over the intranet. This test attempts to connect to the OWA URL from the intranet, and for every stage (a.k.a scenario) of the connection process, reports whether/not that stage completed successfully or not and the time taken for completion. This way, the test not only reports an OWA connectivity failure/slowdown, it also points you to the exact stage at which the failure/slowdown may have occurred. This brings connectivity issues in the internal network and their probable causes to light.

Target of the test : An Exchange 2010 server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each <ClientAccessServer>/<LocalSiteNameofClientAccessServer>/ <SynchronizationStage/Scenario tested>combination.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.
Port	The port number of the client access server. By default, this is 110.
XchgExtensionShellPath	The Exchange Management Shell is a command-line management interface, built on Windows PowerShell which enables you to administer every part of Microsoft Exchange. This test uses the Exchange management shell to run scripts and collect the desired performance metrics from the Exchange server. By default, the test auto-discovers the location of the Exchange management shell and thus, automatically loads the Exchange management shell snap-in (exshell.psc1) for script execution. This is why, the XchgExtensionShellPath is set to *none* by default.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
OWA internal connectivity status	Indicates whether the OWA connectivity check was successful or not at this stage/scenario of the connection.	Percent	The value 0 for this measure indicates that the connectivity check failed at this stage of the interaction. The value 100 on the other hand indicates that this stage of the interaction was cleared successfully. Use the detailed diagnosis of this

Measurement	Description	Measurement Unit	Interpretation
			measure to know the OWA URL that the test tried to connect to.
Logon internal latency	Indicates the time taken for the successful completion of this stage/scenario.	Secs	A low value is desired for this measure. A high value indicates a connection bottleneck. Compare the value of this measure across descriptors to isolate the exact stage/scenario that took the maximum time to complete, and investigate further to determine why.

3.1.11 OWA External Connectivity Test

Outlook Web App (OWA) is a browser-based email client accessible from the web. It allows you to check your email from computers that do not have an email client (such as Outlook 2010) installed. If an external user (i.e., internet user) complains that he/she is unable to check emails using OWA, you can run this test to figure out whether/not that OWA is accessible over the internet, and if so, how long that connection takes. This test attempts to connect to the OWA URL from the internet, and for every stage (a.k.a scenario) of the connection process, reports whether/not that stage completed successfully or not and the time taken for completion. This way, the test not only reports an OWA connectivity failure/slowdown, it also points you to the exact stage at which the failure/slowdown may have occurred. This brings connectivity issues in the internet and their probable causes to light.

Target of the test : An Exchange 2010 server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each <ClientAccessServer>/<LocalSiteNameofClientAccessServer>/ <SynchronizationStage/Scenario tested>combination.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.

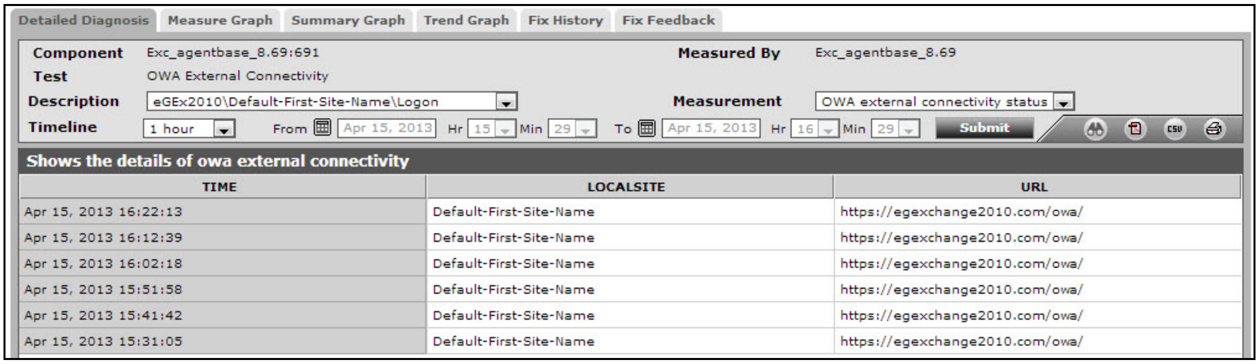
Parameters	Description
Port	The port number of the client access server. By default, this is 110.
XchgExtensionShellPath	The Exchange Management Shell is a command-line management interface, built on Windows PowerShell which enables you to administer every part of Microsoft Exchange. This test uses the Exchange management shell to run scripts and collect the desired performance metrics from the Exchange server. By default, the test auto-discovers the location of the Exchange management shell and thus, automatically loads the Exchange management shell snap-in (exshell.psc1) for script execution. This is why, the XchgExtensionShellPath is set to *none* by default.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
OWA external connectivity status	Indicates whether the OWA connectivity check was successful or not at this stage/scenario of the connection.	Percent	The value 0 for this measure indicates that the connectivity check failed at this stage of the interaction. The value 100 on the other hand indicates that this stage of the interaction was cleared successfully. Use the detailed diagnosis of this measure to know the OWA URL that the test tried to connect to.
Logon external latency	Indicates the time taken for the successful completion of this stage/scenario.	Secs	A low value is desired for this measure. A high value indicates a

Measurement	Description	Measurement Unit	Interpretation
			connection bottleneck. Compare the value of this measure across descriptors to isolate the exact stage/scenario that took the maximum time to complete, and investigate further to determine why.

Use the detailed diagnosis of the *OWA internal connectivity status* measure to know the OWA URL that the test tried to connect to. Sometimes, an incorrect URL may also report incorrect results. To avoid this, its best to check the URL of the OWA using the detailed diagnosis of the OWA internal connectivity status measure.



Component: Exc_agentbase_8.69:691
Test: OWA External Connectivity
Description: eGEx2010\Default-First-Site-Name\Logon
Measured By: Exc_agentbase_8.69
Measurement: OWA external connectivity status
Timeline: 1 hour From Apr 15, 2013 Hr 15 Min 29 To Apr 15, 2013 Hr 16 Min 29

Shows the details of owa external connectivity

TIME	LOCALSITE	URL
Apr 15, 2013 16:22:13	Default-First-Site-Name	https://egexchange2010.com/owa/
Apr 15, 2013 16:12:39	Default-First-Site-Name	https://egexchange2010.com/owa/
Apr 15, 2013 16:02:18	Default-First-Site-Name	https://egexchange2010.com/owa/
Apr 15, 2013 15:51:58	Default-First-Site-Name	https://egexchange2010.com/owa/
Apr 15, 2013 15:41:42	Default-First-Site-Name	https://egexchange2010.com/owa/
Apr 15, 2013 15:31:05	Default-First-Site-Name	https://egexchange2010.com/owa/

Figure 3.4: The detailed diagnosis of the OWA external connectivity status test

3.1.12 ActiveSync Device Status

Administrators must constantly track the devices connecting to ActiveSync, so that they can proactively identify devices that are unable to sync with user mailboxes, the users using these devices, and the probable reason for the non-sync, much before device users even notice that something is wrong! Likewise, administrators should also be able to zero-in on devices that are connected to ActiveSync, but have been inactive for long time periods, so that they can take efforts to clear out such devices en masse. To isolate such devices, administrators can use the **ActiveSync Device Status** test. This test reports the count of devices that are using ActiveSync without a glitch, those that are having problems using Activesync, and the stale (inactive) devices. Using the detailed diagnosis of this measure, the devices that are operating well, those that are not, and those that are stale can be clearly isolated.

Target of the test : A server configured with the Client Access Server role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Client access server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.
Port	The port number of the client access server. By default, this is 110.
XchgExtensionShellPath	The Exchange Management Shell is a command-line management interface, built on Windows PowerShell which enables you to administer every part of Microsoft Exchange. This test uses the Exchange management shell to run scripts and collect the desired performance metrics from the Exchange server. By default, the test auto-discovers the location of the Exchange management shell and thus, automatically loads the Exchange management shell snap-in (exshell.psc1) for script execution. This is why, the XchgExtensionShellPath is set to *none* by default.
Inactive Device Age in Days	Specify the minimum duration (in days) for which a device should not have synchronized with its mailbox for it to be counted as a stale/inactive device.
Show DD for OK Status Device	By default, this flag is set to **No**, indicating that detailed metrics will not be available by default for the **Device with OK status** measure reported by this test. To ensure that this test collects detailed metrics for this measure, set this flag to **Yes**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Device with OK status	Indicates the count of devices that are currently able to synchronize with their mailboxes via ActiveSync.	Number	Detailed diagnostics will be available for this measure only if the Show DD for OK Status device flag is set to '**Yes**'. If available, then, you can use the detailed diagnosis of this measure to know which devices are able to connect to ActiveSync and synchronize with their mailboxes, and which users are using these devices.
Device with not OK status	Indicates the number of devices that are currently unable to synchronize with their Exchange mailboxes via ActiveSync.	Number	Ideally, the value of this measure should be 0. A non-zero value for this measure implies that one/more devices are unable to synchronize with their Exchange mailboxes. To know these devices and their users, use the detailed diagnosis of this measure.
Stale devices	Indicates the current number of stale devices.	Number	Use the detailed diagnosis of this measure to know which devices are inactive, which users are using such devices, and how long these devices have remained inactive.

3.1.13 Exchange ActiveSync Servers Test

Where Exchange ActiveSync is used to synchronize mobile devices with Exchange server mailboxes, Exchange administrators may want to know which devices are connecting to the server at any given point in time, so that accesses by unauthorized devices can be instantly detected and blocked. Administrators may also want to track the usage of mailboxes by mobile devices over time and identify the most and the least effective users, so that access policies can be accordingly drawn. Moreover, when a device user complains of a slowdown when accessing his/her mailbox, administrators may want to take a look at the network traffic generated by every device that is connecting to the server at the time of the slowdown, so that devices that are choking the bandwidth and causing the slowness can be accurately isolated. The **Exchange ActiveSync Servers** test performs all these checks periodically and provides Exchange administrators with actionable information that will enable them to take well-informed

and intelligent performance/policy decisions.

This test auto-discovers the devices that are synchronizing with the Exchange 2010 mailboxes via ActiveSync, and for each device, reports the number of hits/accesses made by that device and the amount of data transmitted and received by that device. In the process, the test points administrators to the following:

- Devices that are currently connected to the Exchange server; unauthorized devices can thus be quickly captured;
- Devices that are accessing the Exchange server mailboxes frequently and those that seldom use the mailboxes; sizing and policy decisions can be taken based on this observation
- Devices that are consuming excessive bandwidth resources and could hence be contributing to the sluggish quality of the network;

Target of the test :A server configured with the Client Access Server role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each device or IP address that is currently accessing the mailboxes on the Exchange server.

Configurable parameters for the test

Parameters	**Description**
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.
Port	The port number of the client access server. By default, this is 110.
XchgExtensionShellPath	The Exchange Management Shell is a command-line management interface, built on Windows PowerShell v2, which enables you to administer every part of Microsoft Exchange Server 2007/2010. This test uses the Exchange management shell to run scripts and collect the desired performance metrics from the Exchange server. To enable the test to load the Exchange management shell snap-in (exshell.psc1) for script execution, you need to specify the full path to the Exchange management shell in the XchgExtensionShellPath text box. For instance, your specification can be, *c:\progra~1\micros~1\exchan~1\v14\bin\exshell.psc1*.

Parameters	Description
LogfileName	The Client Access Server is an IIS web server that hosts Exchange-related web pages. This is why, like any other IIS web server, the client access server creates a daily log of its activities – including Exchange ActiveSync-related activities - in the *C:\inetpub\logs\logfiles\W3SVC1\* directory by default. To report metrics on ActiveSync, this test parses the client access server's log file, reads the ActiveSync-related errors/warnings/general information messages that were recently logged (i.e., during the last 5 minutes) from the file, and writes them to a **ActiveSynchLog.log** file it creates in the <EG_AGENT_INSTALL_ DIR>\agent\logs directory. Then, the test reads the metrics of interest from this log file and reports them to the eG manager. To enable the test to do the above, you need to specify the exact path to the directory that contains the client access server's logs in the LogfileName text box.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total hits	Indicates the current number of hits/accesses to the Exchange mailbox server from this device.	Number	Comparing the value of this measure across devices will help you to identify the device that is constantly accessing the Exchange mailbox server and that which is not using the server as frequently. Based on these usage metrics, administrators can define access policies. Also, this measure serves as a good indicator of the level of device activity on the Exchange server; based on this knowledge, administrators can right-size their Exchange infrastructure – i.e., decide on how much CPU, memory, bandwidth, and disk resources the Exchange server has to be allocated so that it can handle the ActiveSync load.
Data sent	Indicates the amount of data this device is currently sending to the Exchange mail server.	KB	Compare the value of these measures across the devices to identify the device that is currently generating the maximum amount of network traffic

Measurement	Description	Measurement Unit	Interpretation
			when interacting with its mailbox on the Exchange server. In the event of a slowdown, this comparative analysis will point administrators to that device which is engaged in bandwidth-intensive conversations with the Exchange server, thus causing accesses to slow down. During normal operations on the other hand, administrators can analyze these measures over time to gauge the average network throughput of ActiveSync activities; this can help them decide whether/not more network resources need to be allocated to handle ActiveSync load efficiently.
Data received	Indicates the amount of data currently received by this device from the Exchange mail server.	KB	
Average unique devices	Indicates the number of unique devices currently accessing the ActiveSync server.		

3.1.14 Exchange ActiveSync Requests Status Test

When a mobile device attempts to synchronize with a mailbox on the Exchange server, the server returns an HTTP status code to the device indicating the status of the synchronization attempt. Some of the most critical HTTP status codes for ActiveSync and their interpretations are as follows:

HTTP status code	Description
HTTP_200	Indicates that the device successfully connected to the Exchange server and synchronized with the mailbox on the server.
HTTP_401	Indicates one or all of the following: • The credentials provided to access the server are incorrect; • The user is not enabled for synchronization

HTTP status code	Description
HTTP_404	Indicates that an issue exists with the user account
HTTP_404	Indicates that the file requested is not found on the server
HTTP_449	Indicates that the synchronization attempt should be retried
HTTP_500	Indicates one or all of the following: • The Internet Information Service is unavailable. • Windows Integrated Authentication is not enabled on the Exchange Server virtual directory of the server where the mailbox of the user resides. • Synchronization is tried when the mailbox is being moved.
HTTP_502	Indicates an error in the proxy server used to connect to the ActiveSync Server
HTTP_503	Indicates that the ActiveSync service is unavailable

Periodic review of these status codes and the synchronization attempts that resulted in these codes is imperative to understand how error-prone ActiveSync on the Exchange server is, identify the errors that occur frequently, investigate why these errors occur, and easily troubleshoot them. This is where the **Exchange ActiveSync Requests Status** test helps!

This test automatically discovers the HTTP status codes returned by the Exchange server for ActiveSync accesses. For each status code so discovered, the test reports the number and percentage of accesses that returned that status code. This way, the test points administrators to status codes that were returned most often, thus shedding light on ActiveSync errors that occurred frequently.

Target of the test :A server configured with the Client Access Server role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each status code returned by the ActiveSync server.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.
Port	The port number of the client access server. By default, this is 110.

Parameters	Description
XchgExtensionShellPath	The Exchange Management Shell is a command-line management interface, built on Windows PowerShell v2, which enables you to administer every part of Microsoft Exchange Server 2007/2010. This test uses the Exchange management shell to run scripts and collect the desired performance metrics from the Exchange server. To enable the test to load the Exchange management shell snap-in (exshell.psc1) for script execution, you need to specify the full path to the Exchange management shell in the XchgExtensionShellPath text box. For instance, your specification can be, *c:\progra~1\micros~1\exchan~1\v14\bin\exshell.psc1*.
LogfileName	The Client Access Server is an IIS web server that hosts Exchange-related web pages. This is why, like any other IIS web server, the client access server creates a daily log of its activities – including Exchange ActiveSync-related activities - in the *C:\inetpub\logs\logfiles\W3SVC1\* directory by default. To report metrics on ActiveSync, this test parses the client access server's log file, reads the ActiveSync-related errors/warnings/general information messages that were recently logged (i.e., during the last 5 minutes) from the file, and writes them to a **ActiveSynchLog.log** file it creates in the <EG_AGENT_INSTALL_ DIR>\agent\logs directory. Then, the test reads the metrics of interest from this log file and reports them to the eG manager. To enable the test to do the above, you need to specify the exact path to the directory that contains the client access server's logs in the LogfileName text box.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total hits	Indicates the current number of hits to the Exchange mailbox server that returned this status code.	Number	Compare the value of these measures across status codes to identify the status code that is returned frequently. High values for the 4xx or 5xx class of status codes is a cause for concern, as they indicate client and server errors respectively. If such status codes are returned often, administrators will have to look up the Microsoft documentation to understand what error condition each code represents and how to resolve it.
Hit ratio	Indicates the percentage of hits to the Exchange mailbox server that returned this status code.	Percent	

3.1.15 Exchange ActiveSync Devices Test

In environments where ActiveSync is enabled, it is normal for users wielding different types of devices to synchronize their mailbox with their device. In such environments, administrators should pay close attention to the device types that are connected to the Exchange server mailboxes at any given point in time, so that unsupported device types can be detected and the users using such types of devices identified and advised accordingly. It is also essential that administrators study how frequently each of these device types are accessing the Exchange server and monitor the level of activity generated by these device types on the server and on the network. If a device users complains of delays in accessing his/her mailbox, then this visibility will enable administrators to identify those device types to which the slowdown can be attributed. In addition, administrators will also need to know from time-to-time how much load ActiveSync imposes on the Exchange server and the network, across all device types! This aggregated measure will enable administrators to figure out whether/not the Exchange server is sized right to handle the load. To receive such in-depth insights into ActiveSync performance – both at the per-device type level and across all device types – administrators can use the **Exchange ActiveSync Devices** test.

This test auto-discovers the device types currently synchronizing with the Exchange server. For each device type, the test reports the number of ActiveSync accesses made by that device type and the number and size of items transmitted and received by that device type. This way, the test leads administrators to those device types that are utilizing the available network and server resources excessively, thus degrading the experience of some or all device users. Detailed metrics provided by the test also help administrators identify all the users who are using devices of a particular type and pinpoint the exact user who is engaged in a resource-intensive interaction with the Exchange server mailbox. Additionally, the test reports metrics across all device types, thus enabling administrators to measure the current load on the server and the network and assess the ability of the server to handle that load.

Target of the test : A server configured with the Client Access Server role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each device type that is accessing the Exchange server; an additional **All** descriptor is also supported, which reports a set of aggregated metrics across all device types.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.
Port	The port number of the client access server. By default, this is 110.
XchgExtensionShellPath	The Exchange Management Shell is a command-line management interface, built on Windows PowerShell v2, which enables you to administer every part of Microsoft Exchange Server 2007/2010. This test uses the Exchange management shell to run scripts and collect the desired performance metrics from the Exchange server. To enable the test to load the Exchange management shell snap-in (exshell.psc1) for script execution, you need to specify the full path to the Exchange management shell in the XchgExtensionShellPath text box. For instance, your specification can be, *c:\progra~1\micros~1\exchan~1\v14\bin\exshell.psc1*.
LogfileName	The Client Access Server is an IIS web server that hosts Exchange-related web pages. This is why, like any other IIS web server, the client access server creates a daily log of its activities – including Exchange ActiveSync-related activities - in the *C:\inetpub\logs\logfiles\W3SVC1\* directory by default. To report metrics on ActiveSync, this test parses the client access server's log file, reads the ActiveSync-related errors/warnings/general information messages that were recently logged (i.e., during the last 5 minutes) from the file, and writes them to a **ActiveSynchLog.log** file it creates in the <EG_AGENT_INSTALL_DIR>\agent\logs directory. Then, the test reads the metrics of interest from this log file and reports them to the eG manager. To enable the test to do the above, you need to specify the exact path to the directory that contains the client access server's logs in the LogfileName text box.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total hits	Indicates the number of hits/accesses made by this device type to the Exchange server mailbox.	Number	Comparing the value of this measure across device types will help administrators identify that device type which is very actively synchronizing with the Exchange mailbox. Using the detailed diagnosis of this

Measurement	Description	Measurement Unit	Interpretation
			measure, administrators can also identify the precise user who is making the maximum number of accesses, which device that user is using, and the details of that device. Based on this information, access policies can be defined. Also, by observing the variations in the value of this measure for the All descriptor, administrators can effectively gauge the typical level of activity on the Exchange server and figure out if the server is sized right to handle this load.
Total items sent	Indicates the number of items currently sent from this device type to the Exchange server.	Number	These measures indicate how much network traffic and I/O load is generated by each of the device types. By comparing the value of these measures across device types, administrators can easily and accurately identify that device type that is engaged in resource-intensive communication with the Exchange server. In the event of a slowdown, the results of this comparative analysis will lead administrators to that device type that could be contributing to the slowdown. Once the device type is identified, you can use the detailed diagnosis of the Total hits measure to know which user of that device type is actually choking the network/server and what device he/she is currently using.
Total items received	Indicates the number of items currently received by this device type from the Exchange server.	Number	
Data sent	Indicates the amount of data currently sent from this device type to the Exchange server.	KB	
Data received	Indicates the amount of data currently received by this device type from the Exchange server.	KB	

3.1.16 Exchange ActiveSync Policy Compliance Test

Exchange ActiveSync mailbox policies let you apply a common set of policy or security settings to a user or group of users. With the help of these policies, Exchange administrators can indicate what specific devices – thus users – connecting to ActiveSyc, can do.

EAS policies are applied to users; each user can have zero policies or one EAS policy at any given time. If you don't explicitly assign a policy to a user, the default policy is applied instead. During the initial sync of a new device (that is, one that has not been synchronized to the server before), the device and server exchange what EAS calls a policy key. Think of the policy key as a GUID or MAC address; it's a unique key that indicates one specific policy. If the device and server keys do not match, the device is required to request the most recent policy and then apply it. The process of applying a policy to the device is known as provisioning. On most devices, the user will see a dialog box indicating that the server is applying a policy and asking whether to accept it. If the user declines the policy, the server might or might not allow the device to continue to sync to it; the exact behavior depends on whether the default policy on the server allows non-provisioned devices.

Not every device that connects to ActiveSync will implement every setting defined in a policy; some devices may even lie about the policy settings that they implement. Hence, the onus of determining the number of devices that comply with the policy settings and to what extent is the compliance, lies with the administrator. To determine this, administrators can use the **Exchange ActiveSync Policy Compliance** test. This test reports the count and percentage of devices connecting to ActiveSync that are fully compliant, partially compliant, and completely non-compliant with their mailbox policies. This way, the test reveals the degree of compliance to configured policies.

Target of the test :A server configured with the Client Access Server role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each type of compliance – Compliant, Partially compliant, Not compliant, Unknown.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.
Port	The port number of the client access server. By default, this is 110.

Parameters	Description
XchgExtensionShellPath	The Exchange Management Shell is a command-line management interface, built on Windows PowerShell v2, which enables you to administer every part of Microsoft Exchange Server 2007/2010. This test uses the Exchange management shell to run scripts and collect the desired performance metrics from the Exchange server. To enable the test to load the Exchange management shell snap-in (exshell.psc1) for script execution, you need to specify the full path to the Exchange management shell in the XchgExtensionShellPath text box. For instance, your specification can be, *c:\progra~1\micros~1\exchan~1\v14\bin\exshell.psc1*.
LogfileName	The Client Access Server is an IIS web server that hosts Exchange-related web pages. This is why, like any other IIS web server, the client access server creates a daily log of its activities – including Exchange ActiveSync-related activities - in the *C:\inetpub\logs\logfiles\W3SVC1\* directory by default. To report metrics on ActiveSync, this test parses the client access server's log file, reads the ActiveSync-related errors/warnings/general information messages that were recently logged (i.e., during the last 5 minutes) from the file, and writes them to a **ActiveSynchLog.log** file it creates in the <EG_AGENT_INSTALL_ DIR>\agent\logs directory. Then, the test reads the metrics of interest from this log file and reports them to the eG manager. To enable the test to do the above, you need to specify the exact path to the directory that contains the client access server's logs in the LogfileName text box.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total hits	Indicates the number of devices currently accessing ActiveSync that are of this compliance type .	Number	Compare the value of this measure across compliance types to know how compliant the maximum number of devices are - fully compliant? partially compliant? non-compliant? or unknown? (i.e., the compliance level cannot be determined)
Hits ratio	Indicates the percentage of devices currently accessing ActiveSync that are of this compliance type.	Percent	Compare the value of this measure across compliance types to know the degree of compliance of devices accessing ActiveSync - fully compliant? partially compliant? or non-compliant? or unknown? (i.e., the

Measurement	Description	Measurement Unit	Interpretation
			compliance level cannot be determined)

3.1.17 Exchange ActiveSync User Agent Test

Devices communicating with Exchange via ActiveSync identify themselves to Exchange using a 'User Agent' string and a 'User Agent Type' string. For instance, an iPhone may identify itself to Exchange using the user agent string 'Apple-iPhone/xxx.xxx' and the user agent type 'iPhone'. While the user agent string is unique for every device, multiple devices can be of the same user agent type. By tracking the types of user agents that are accessing Exchange via ActiveSync, administrators can determine which type of devices are attempting to synchronize with the Exchange mailboxes. In times of an overload, this information may point administrators to the exact type of devices that could be contributing to the heavy load. To obtain this useful information, administrators can use the **Exchange ActiveSync User Agent** test. For every user agent type, this test reports the total number of user agents of that type that are accessing ActiveSync at any given point in time. In addition, it also reports the number of unique devices of each type synchronizing with Exchange. This not only indicates the current synchronization load on Exchange, but also helps identify the user agent types (i.e., device types) that could be contributing to the workload.

Target of the test :A server configured with the Client Access Server role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each user agent type.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Client Access server.
Port	The port number of the client access server. By default, this is 110.
XchgExtensionShellPath	The Exchange Management Shell is a command-line management interface, built on Windows PowerShell v2, which enables you to administer every part of Microsoft Exchange Server 2007/2010. This test uses the Exchange management shell to run scripts and collect the desired performance metrics from the Exchange

Parameters	Description
	server. To enable the test to load the Exchange management shell snap-in (exshell.psc1) for script execution, you need to specify the full path to the Exchange management shell in the XchgExtensionShellPath text box. For instance, your specification can be, *c:\progra~1\micros~1\exchan~1\v14\bin\exshell.psc1*.
LogfileName	The Client Access Server is an IIS web server that hosts Exchange-related web pages. This is why, like any other IIS web server, the client access server creates a daily log of its activities – including Exchange ActiveSync-related activities - in the *C:\inetpub\logs\logfiles\W3SVC1\* directory by default. To report metrics on ActiveSync, this test parses the client access server's log file, reads the ActiveSync-related errors/warnings/general information messages that were recently logged (i.e., during the last 5 minutes) from the file, and writes them to a **ActiveSynchLog.log** file it creates in the <EG_AGENT_INSTALL_ DIR>\agent\logs directory. Then, the test reads the metrics of interest from this log file and reports them to the eG manager. To enable the test to do the above, you need to specify the exact path to the directory that contains the client access server's logs in the LogfileName text box.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total hits	Indicates the current number of synchronization requests from user agents of this type.	Number	This is a good indicator of the current synchronization load on the Exchange server. You can compare the value of this measure across user agents to know which type of user agents are actually overloading the server.
Unique devices	Indicates the number of unique devices of this user agent type that are currently accessing ActiveSync.	Number	Compare the value of this measure across user agent types to identify the device type that is significantly impacting the server workload.

3.1.18 Exchange ActiveSync Device Errors Test

In order to enable administrators to quickly troubleshoot current issues with ActiveSync, the eG Exchange Monitor intelligently reads ActiveSync-related errors/warnings/general information or status messages related to ActiveSync commands captured recently (i.e., in the last 5 minutes) from the client access server's log file and writes them to the *ActiveSynchLog.log* file it creates in the <EG_AGENT_INSTALL_DIR>\agent\logs directory. At specified intervals, this test scans the *ActiveSynchLog.log* file for configured patterns of errors and reports the number and nature of such errors (if found).

Note:

At least one of the following tests should be running and reporting metrics for this test to work:

- Exchange ActiveSync Servers Test
- Exchange ActiveSync Status Test
- Exchange ActiveSync Users Test
- Exchange ActiveSync Policy Compliance Test
- Exchange ActiveSync User Agents Test

Target of the test : An Exchange Client Access Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every SearchPattern configured.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port at which the server listens.
AlertFile	By default, the full path to the **ActiveSynchLog.log** file is set here.
SearchPattern	Enter the specific patterns of alerts to be monitored. The pattern should be in the following format: *<PatternName>:<Pattern>*, where *<PatternName>* is the pattern name that will be displayed in the monitor interface and *<Pattern>* is an expression of the form - *expr* or expr or *expr or expr*, etc. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. For example, say you specify *ItemNotFound:Item** in the SearchPattern text box. This indicates that "ItemNotFound" is the pattern name to be displayed in the monitor interface. "Item*" indicates that the test will monitor only those lines in the alert log which start with the term "Item". Similarly, if your pattern specification reads:

Parameters	Description
	*UserDisabledForSync:*Sync*, then it means that the pattern name is UserDisabledForSync and that the test will monitor those lines in the alert log which end with the term Sync. A single pattern may also be of the form e1+e2, where + signifies an OR condition. That is, the <PatternName> is matched if either e1 is true or e2 is true. Multiple search patterns can be specified as a comma-separated list. For example: *ItemNotFound:Item*, UserDisabledForSync:*Sync* If you want all the messages in a log file to be monitored, then your specification would be: *<PatternName>:**.
Lines	Specify two numbers in the format *x:y*. This means that when a line in the alert file matches a particular pattern, then x lines before the matched line and y lines after the matched line will be reported in the detail diagnosis output (in addition to the matched line). The default value here is 0:0. Multiple entries can be provided as a comma-separated list. If you give 1:1 as the value for LINES, then this value will be applied to all the patterns specified in the SearchPattern field. If you give 0:0,1:1 as the value for Lines and if the corresponding value in the SearchPattern filed is like *ItemNotFound:Item*, UserDisabledForSync:*Sync*, then: 0:0 will be applied to *ItemNotFound* pattern 1:1 will be applied to *UserDisabledForSync* pattern
ExcludePattern	Provide a comma-separated list of patterns to be excluded from monitoring in the ExcludePattern text box. For example **critical*, *exception**. By default, this parameter is set to '*none*'.
UniqueMatch	By default, the UniqueMatch parameter is set to **False,** indicating that, by default, the test checks every line in the log file for the existence of each of the configured SearchPatterns. By setting this parameter to **True**, you can instruct the test to ignore a line and move to the next as soon as a match for one of the configured patterns is found in that line. For example, assume that *Pattern1:*fatal*,Pattern2:*error** is the Searchpattern that has been configured. If UniqueMatch is set to **False**, then the test will read every line in the log file completely to check for the existence of messages embedding the strings 'fatal' and 'error'. If both the patterns are detected in the same line, then the number of matches will be incremented by 2. On the other hand, if UniqueMatch is set to **True**, then the test will read a line only until a match for one of the configured patterns is found and not both. This means that even if the strings 'fatal' and 'error' follow one another in the same line, the test will consider only the first match and not the next. The match count in this case will therefore be incremented by only 1.

Parameters	Description
RotatingFile	This flag governs the display of descriptors for this test in the eG monitoring console. If this flag is set to **True** and the AlertFile text box contains the full path to a specific (log/text) file, then, the descriptors of this test will be displayed in the following format: *Directory_containing_monitored_file:<SearchPattern>*. For instance, if the AlertFile parameter is set to *c:\eGurkha\logs\syslog.txt*, and RotatingFile is set to **True**, then, your descriptor will be of the following format: *c:\eGurkha\logs:<SearchPattern>*. On the other hand, if the rotatingfile flag had been set to false, then the descriptors will be of the following format: *<FileName>:<SearchPattern>* - i.e., *syslog.txt:<SearchPattern>* in the case of the example above. If this flag is set to **True** and the AlertFile parameter is set to the directory containing log files, then, the descriptors of this test will be displayed in the format: *Configured_directory_path:<SearchPattern>*. For instance, if the AlertFile parameter is set to *c:\eGurkha\logs*, and rotatingfile is set to **True**, then, your descriptor will be: *c:\eGurkha\logs:<SearchPattern>*. On the other hand, if the RotatingFile parameter had been set to **False**, then the descriptors will be of the following format: *Configured_directory:<SearchPattern>* - i.e., *logs:<SearchPattern>* in the case of the example above. If this flag is set to **True** and the AlertFile parameter is set to a specific file pattern, then, the descriptors of this test will be of the following format: *<FilePattern>:<SearchPattern>*. For instance, if the alertfile parameter is set to *c:\eGurkha\logs\*sys**, and RotatingFile is set to **True**, then, your descriptor will be: **sys*:<SearchPattern>*. In this case, the descriptor format will not change even if the RotatingFile flag status is changed .
CaseSensitive	This flag is set to **No** by default. This indicates that the test functions in a 'case-insensitive' manner by default. This implies that, by default, the test ignores the case of your AlertFile and SearchPattern specifications. If this flag is set to **Yes** on the other hand, then the test will function in a 'case-sensitive' manner. In this case therefore, for the test to work, even the case of your AlertFile and SearchPattern specifications should match with the actuals.
RolloverFile	By default, this flag is set to **False**. Set this flag to **True** if you want the test to support the 'roll over' capability of the specified AlertFile. A roll over typically occurs when the timestamp of a file changes or when the log file size crosses a pre-determined threshold. When a log file rolls over, the errors/warnings that pre-exist in that file will be automatically copied to a new file, and all errors/warnings that are captured subsequently will be logged in the original/old file. For instance, say, errors and warnings were originally logged to a file named *error_log*. When a roll over occurs, the

Parameters	Description
	content of the file *error_log* will be copied to a file named *error_log.1*, and all new errors/warnings will be logged in *error_log*. In such a scenario, since the RolloverFile flag is set to **False** by default, the test by default scans only *error_log.1* for new log entries and ignores *error_log*. On the other hand, if the flag is set to **True**, then the test will scan both *error_log* and *error_log.1* for new entries. If you want this test to support the 'roll over' capability described above, the following conditions need to be fulfilled: • The AlertFile parameter has to be configured only with the name and/or path of one/more alert files. File patterns or directory specifications should not be specified in the AlertFile text box. • The roll over file name should be of the format: "<alertfile>.1", and this file must be in the same directory as the alertfile.
OverwrittenFile	By default, this flag is set to **False**. Set this flag to **True** if log files do not 'roll over' in your environment, but get overwritten instead. In such environments typically, new error/warning messages that are captured will be written into the log file that pre-exists and will replace the original contents of that log file; unlike when 'roll over' is enabled, no new log files are created for new entries in this case. If the OverwrittenFile flag is set to **True**, then the test will scan the new entries in the log file for matching patterns. However, if the flag is set to **False**, then the test will ignore the new entries.
UseUTF8	Set this flag to **Yes**, if the test needs to use the UTF-8 encoding format for reading from the specified alert file.
UseUTF16	Set this flag to **Yes**, if the test needs to use the UTF-16 encoding format for reading from the specified alert file.
EncodeFormat	By default, this is set to *none*, indicating that no encoding format applies by default. However, if the test has to use a specific encoding format for reading from the specified AlertFile , then you will have to provide a valid encoding format here - eg., UTF-8, UTF-16, etc. Where multiple log files are being monitored, you will have to provide a comma-separated list of encoding formats – one each for every log file monitored. Make sure that your encoding format specification follows the same sequence as your AlertFile specification. In other words, the first encoding format should apply to the first alert file, and so on. For instance, say that your AlertFile specification is as follows:*D:\logs\report.log,E:\logs\error.log, C:\logs\warn_log*. Assume that while **UTF-8** needs to be used for reading from *report.log* , **UTF-16** is to be used for reading from *warn_log* . No encoding format need be applied to *error.log*. In this case, your EncodeFormat specification will be: UTF-8,none,UTF-16.

Parameters	Description
	Note: If your AlertFile specification consists of file patterns that include wildcard characters (eg.,*/tmp/db/*dblogs*,/tmp/app/*applogs**), then such configurations will only be supported in the ANSI format, and not the UTF format.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Recent errors	Indicates the number of errors that were added to the **ActiveSynchLog.log** file when the test was last executed.	Number	The value of this measure is a clear indicator of the number of “new” errors detected in ActiveSync. The detailed diagnosis of this measure, if enabled, provides the detailed descriptions of the errors of the configured patterns.

3.1.19 Exchange ActiveSync Device Commands Test

In order to enable administrators to quickly troubleshoot current issues with ActiveSync, the eG Exchange Monitor intelligently reads ActiveSync-related errors/warnings/general information or status messages related to ActiveSync commands captured recently (i.e., in the last 5 minutes) from the client access server's log file and writes them to the **ActiveSynchLog.log** file it creates in the <EG_AGENT_INSTALL_DIR>\agent\logs directory. At specified intervals, this test scans the **ActiveSynchLog.log** file for configured patterns of command-related messages and reports the number and nature of messages (if found) matching the configured patterns.

Note:

At least one of the following tests should be running and reporting metrics for this test to work:

- Exchange ActiveSync Servers Test
- Exchange ActiveSync Status Test
- Exchange ActiveSync Users Test
- Exchange ActiveSync Policy Compliance Test
- Exchange ActiveSync User Agents Test

Target of the test : An Exchange Client Access Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every SearchPattern configured.

Configurable parameters for the test

Parameters	**Description**
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port at which the server listens.
AlertFile	By default, the full path to the **ActiveSynchLog.log** file is set here.
SearchPattern	Enter the specific patterns of alerts to be monitored. The pattern should be in the following format: *<PatternName>:<Pattern>*, where *<PatternName>* is the pattern name that will be displayed in the monitor interface and *<Pattern>* is an expression of the form - *expr* or expr or *expr or expr*, etc. A leading '*' signifies any number of

Parameters	Description
	leading characters, while a trailing '*' signifies any number of trailing characters. For example, say you specify *Sync:Sync** in the SearchPattern text box. This indicates that "Sync" is the pattern name to be displayed in the monitor interface. "Sync*" indicates that the test will monitor only those lines in the alert log which start with the term "ORA-". Similarly, if your pattern specification reads: *SendMail:*SendMail*, then it means that the pattern name is *SendMail* and that the test will monitor those lines in the alert log which end with the term *SendMail*. A single pattern may also be of the form e1+e2, where + signifies an OR condition. That is, the <*PatternName*> is matched if either e1 is true or e2 is true. Multiple search patterns can be specified as a comma-separated list. For example: *Sync:Sync*, SendMail:*SendMail* If you want all the messages in a log file to be monitored, then your specification would be: <*PatternName*>*:**.
Lines	Specify two numbers in the format *x:y*. This means that when a line in the alert file matches a particular pattern, then x lines before the matched line and y lines after the matched line will be reported in the detail diagnosis output (in addition to the matched line). The default value here is 0:0. Multiple entries can be provided as a comma-separated list. If you give 1:1 as the value for Lines, then this value will be applied to all the patterns specified in the SearchPattern field. If you give 0:0,1:1 as the value for Lines and if the corresponding value in the SearchPattern filed is like *Sync:Sync**, *SendMail:*SendMail*, then: 0:0 will be applied to *Sync* pattern 1:1 will be applied to *SendMail* pattern
ExcludePattern	Provide a comma-separated list of patterns to be excluded from monitoring in the ExcludePattern text box. For example **critical*, *exception**. By default, this parameter is set to '*none*'.
UniqueMatch	By default, the UniqueMatch parameter is set to **False,** indicating that, by default, the test checks every line in the log file for the existence of each of the configured SearchPatterns. By setting this parameter to **True**, you can instruct the test to ignore a line and move to the next as soon as a match for one of the configured patterns is found in that line. For example, assume that *Pattern1:*fatal*,Pattern2:*error** is the Searchpattern that has been configured. If UniqueMatch is set to **False**, then the test will read every line in the log file completely to check for the existence of messages

Parameters	Description
	embedding the strings 'fatal' and 'error'. If both the patterns are detected in the same line, then the number of matches will be incremented by 2. On the other hand, if UniqueMatch is set to **True**, then the test will read a line only until a match for one of the configured patterns is found and not both. This means that even if the strings 'fatal' and 'error' follow one another in the same line, the test will consider only the first match and not the next. The match count in this case will therefore be incremented by only 1.
RotatingFile	This flag governs the display of descriptors for this test in the eG monitoring console. If this flag is set to **True** and the AlertFile text box contains the full path to a specific (log/text) file, then, the descriptors of this test will be displayed in the following format: *Directory_containing_monitored_file:<SearchPattern>*. For instance, if the AlertFile parameter is set to *c:\eGurkha\logs\syslog.txt*, and RotatingFile is set to **True**, then, your descriptor will be of the following format: *c:\eGurkha\logs:<SearchPattern>*. On the other hand, if the rotatingfile flag had been set to false, then the descriptors will be of the following format: *<FileName>:<SearchPattern>* - i.e., *syslog.txt:<SearchPattern>* in the case of the example above. If this flag is set to **True** and the AlertFile parameter is set to the directory containing log files, then, the descriptors of this test will be displayed in the format: *Configured_ directory_path:<SearchPattern>*. For instance, if the AlertFile parameter is set to *c:\eGurkha\logs*, and rotatingfile is set to **True**, then, your descriptor will be: *c:\eGurkha\logs:<SearchPattern>*. On the other hand, if the RotatingFile parameter had been set to **False**, then the descriptors will be of the following format: *Configured_directory:<SearchPattern>* - i.e., *logs:<SearchPattern>* in the case of the example above. If this flag is set to **True** and the AlertFile parameter is set to a specific file pattern, then, the descriptors of this test will be of the following format: *<FilePattern>:<SearchPattern>*. For instance, if the alertfile parameter is set to *c:\eGurkha\logs\*sys**, and RotatingFile is set to **True**, then, your descriptor will be: **sys*:<SearchPattern>*. In this case, the descriptor format will not change even if the RotatingFile flag status is changed .
CaseSensitive	This flag is set to **No** by default. This indicates that the test functions in a 'case-insensitive' manner by default. This implies that, by default, the test ignores the case of your AlertFile and SearchPattern specifications. If this flag is set to **Yes** on the other hand, then the test will function in a 'case-sensitive' manner. In this case therefore, for the test to work, even the case of your AlertFile and SearchPattern specifications should match with the actuals.

Parameters	Description
RolloverFile	By default, this flag is set to **False**. Set this flag to **True** if you want the test to support the 'roll over' capability of the specified AlertFile. A roll over typically occurs when the timestamp of a file changes or when the log file size crosses a pre-determined threshold. When a log file rolls over, the errors/warnings that pre-exist in that file will be automatically copied to a new file, and all errors/warnings that are captured subsequently will be logged in the original/old file. For instance, say, errors and warnings were originally logged to a file named *error_log*. When a roll over occurs, the content of the file *error_log* will be copied to a file named *error_log.1*, and all new errors/warnings will be logged in *error_log*. In such a scenario, since the RolloverFile flag is set to **False** by default, the test by default scans only *error_log.1* for new log entries and ignores *error_log*. On the other hand, if the flag is set to **True**, then the test will scan both *error_log* and *error_log.1* for new entries. If you want this test to support the 'roll over' capability described above, the following conditions need to be fulfilled: • The AlertFile parameter has to be configured only with the name and/or path of one/more alert files. File patterns or directory specifications should not be specified in the AlertFile text box. • The roll over file name should be of the format: “<alertfile>.1”, and this file must be in the same directory as the alertfile.
OverwrittenFile	By default, this flag is set to **False**. Set this flag to **True** if log files do not 'roll over' in your environment, but get overwritten instead. In such environments typically, new error/warning messages that are captured will be written into the log file that pre-exists and will replace the original contents of that log file; unlike when 'roll over' is enabled, no new log files are created for new entries in this case. If the OverwrittenFile flag is set to **True**, then the test will scan the new entries in the log file for matching patterns. However, if the flag is set to **False**, then the test will ignore the new entries.
UseUTF8	Set this flag to **Yes**, if the test needs to use the UTF-8 encoding format for reading from the specified alert file.
UseUTF16	Set this flag to **Yes**, if the test needs to use the UTF-16 encoding format for reading from the specified alert file.
EncodeFormat	By default, this is set to *none*, indicating that no encoding format applies by default. However, if the test has to use a specific encoding format for reading from the specified AlertFile , then you will have to provide a valid encoding format here - eg., UTF-8, UTF-16, etc. Where multiple log files are being monitored, you will have to provide a comma-separated list of encoding formats – one each for every log file monitored.

Parameters	Description
	Make sure that your encoding format specification follows the same sequence as your AlertFile specification. In other words, the first encoding format should apply to the first alert file, and so on. For instance, say that your AlertFile specification is as follows:*D:\logs\report.log,E:\logs\error.log, C:\logs\warn_log*. Assume that while **UTF-8** needs to be used for reading from *report.log* , **UTF-16** is to be used for reading from *warn_log* . No encoding format need be applied to *error.log*. In this case, your EncodeFormat specification will be: UTF-8,none,UTF-16. **Note:** If your AlertFile specification consists of file patterns that include wildcard characters (eg.,*/tmp/db/*dblogs*,/tmp/app/*applogs**), then such configurations will only be supported in the ANSI format, and not the UTF format.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
New messages	Indicates the number of messages that were added to the ActiveSynchLog.log file when the test was last executed.	Number	The detailed diagnosis of this measure, if enabled, provides the detailed descriptions of the messages of the configured patterns.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of eG Innovations. eG Innovations makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information contained in this document is subject to change without notice.

All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of eG Innovations. All trademarks, marked and not marked, are the property of their respective owners. Specifications subject to change without notice.