The eG Enterprise Logon Simulator for Microsoft Exchange

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Slow logons have been the most common complaint in Exchange infrastructures. For an Exchange user, slow logons can lead to frustration, lower productivity and efficiency. For an enterprise that uses Exchange for its business correspondence, slow logons and frustrated users can increase support costs and can result in significant revenue loss.

A typical user logon in an Exchange infrastructure begins with the user attempting to access his/her mailbox via one of the following interfaces:

- Outlook Web Access (OWA) interface
- Office 365 portal

Once the user connects to the preferred interface (OWA or Office 365), he/she provides his/her login credentials at the login prompt. As soon as the credentials are validated, he/she will be allowed access to their mailbox.

Many factors impact a user's logon experience. Slowness/failure of the web interface, authentication failures/delays, and network latencies can contribute to a sub-par logon experience. Because the failure points are one too many, proactive detection of a failed/slow logon and precise isolation of its root-cause is often a challenge for administrators. Another bottleneck to effective troubleshooting is the fact that logon issues do not come to light until a user actually logs in.

Collecting logon metrics of real user activity is challenging. Metrics have to collected from the different tiers involved - the web interface, the network, and the Exchange server. Furthermore, there will be times when no one is logging into the Exchange server, and at those times, it is important to know if Exchange logon is working or not.

The eG Enterprise Logon Simulator for Exchange, a part of the eG Enterprise suite, is a purpose-built solution for delivering proactive visibility into the logon performance in Exchange infrastructures. Using an agentless approach, the eG Enterprise Logon Simulator for Exchange simulates a user logging into an OWA interface or Office 365 portal through a browser and accessing his/her mailbox. By emulating the exact same process that users go through when they logon to Exchange, the eG Enterprise Logon Simulator for Exchange provides a realistic measure of the user experience during Exchange logon. Since every simulation tests the entire Exchange infrastructure, the results represent the cumulative health of all of the tiers supporting Exchange logons.

Unlike traditional simulation tools that require recording of a script that captures the typical steps a user performs, the eG Enterprise Logon Simulator for Exchange requires no recording and hence, is simple to implement. Installed on any , the simulator targets the configured logon URL and mailbox

at pre-configured intervals and tests the Exchange logon availability and performance. When a problem is detected, the offending step is clearly highlighted, so administrators can start working on a resolution immediately.

The simulation can be configured to run from different remote locations to understand the logon performance from each location. By testing the simulated session from different locations and at different times, administrators can diagnose and resolve logon issues before users experience them and call up the helpdesk. Licensing is based on number of simulation locations, not on the number of logons simulated.

1.1 How does the eG Enterprise Logon Simulator for Exchange Work?

A light-weight eG Logon Simulator Agent drives the logon simulation. You only have toinstall this agent on any Windows host in your environment and configure it to simulate accesses to a mailbox on an Exchange 2013/2016 server or on Office 365. The agent then periodically emulates the entire process of a user logging into an Exchange server via a web interface and accessing his/her mailbox. To perform this simulation, the Logon Simulator Agent has to be configured with the following:

- The URL of the Outlook Web Access (OWA) interface or Office 365 portal that it needs to hit
- The email ID and valid login credentials of the mailbox on the Exchange server that it needs to access;

Once the Logon Simulator Agent is configured, it runs at a pre-configured frequency. Every time it runs, it simulates the logon process, as detailed below:

1. The Logon Simulator Agent first opens the Chrome browser and connects to the configured URL.
2. It then logs in through the web interface (which can be an OWA interface or an Office 365 portal) and captures the time taken to login. The success/failure of the login is also determined.
3. The agent next opens the configured mailbox and records the duration of the access. In the process, it figures out whether/not the mailbox was accessed successfully.
4. Finally, the agent closes the mailbox and logs out of the Exchange server. The log out duration is also captured.
5. Steps 1 to 4 are then repeated for every mailbox (i.e., email ID) that has been configured for monitoring.

1.2 Pre-requisites for Using the eG Enterprise Logon Simulator for Exchange

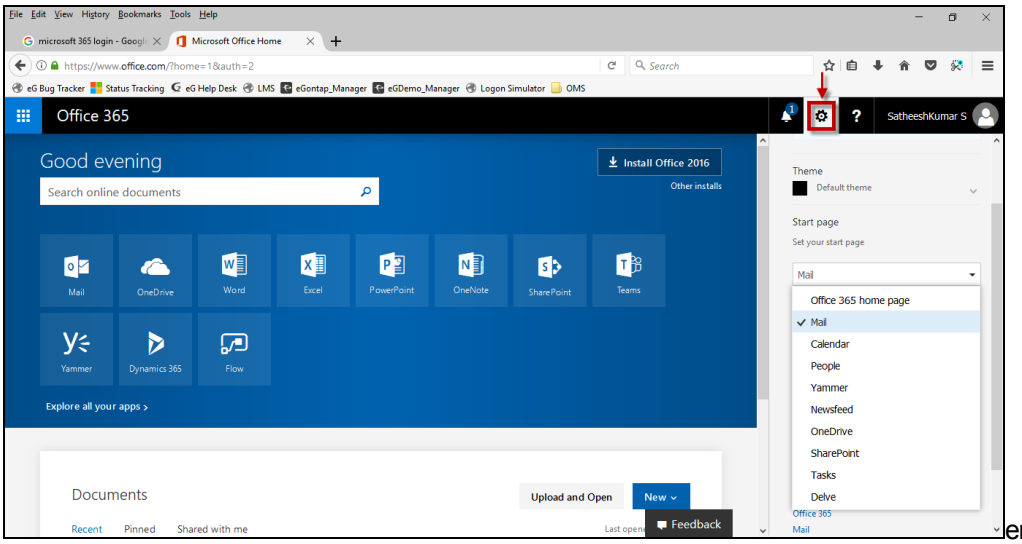
Category	Pre-requisites
Logon Simulator Agent / Simulation Endpoint	• The Logon Simulator Agent should be installed on a dedicated endpoint. **The dedicated endpoint should only run an English version of Windows operating system.** • No other eG agent should exist on the same host on which the Logon Simulator Agent has been installed. • .Net 3.5 (or above) should pre- exist on the system hosting the Logon Simulator Agent. • The simulator requires a user account with local administrator rights on the simulation endpoint - i.e., on the system hosting the Logon Simulator Agent. This user should be logged in at all times for the simulator to run continuously.
Environment	• The simulator will only work with Exchange 2013 / Exchange 2016 / Office 365 environments. • One/more valid and dedicated email IDs on the Exchange server is required for the purpose of the simulation. • The simulation can use either Outlook Web Access (OWA) interface or the Office 365 portal to access the configured mailbox. If Office 365 is used, then make sure that the default start page of the Office 365 portal is set to *Mail* for every email ID that has been configured for the purpose of the simulation. To know how to achieve this, refer to Section **1.2.1**. Once this is done, make sure you clear the browser history. • If a firewall separates the simulation endpoint from the web interface, then make sure you configure the firewall to allow two- way communication between the endpoint and the web interface.
Browser	The eG Logon Simulator for Exchange mandates the presence of the Chrome browser v81 (and above). No other browser supports this simulation. **Note:**

	Chrome is capable of automatically applying updates and upgrading itself to higher versions. Sometimes, when Chrome auto-upgrades, some drivers that the eG Logon Simulator Agent uses may suddenly be rendered incompatible with Chrome. This can cause problems in simulation. To avoid this, the eG Enterprise Logon Simulator for Exchange, by default, prevents Chrome upgrades/updates (both automatic and manual) from being applied at the simulation endpoint. However, whenever a new version of the eG agent with updated drivers is released, you will have to manually upgrade Chrome to ensure continued compatibility. In this case therefore, you will have to make sure that the simulation endpoint allows Chrome upgrades. To achieve this, before manually upgrading Chrome, follow the steps below: • Login to the eG agent host. • Open the Windows command prompt as Administrator. • Switch to the <EG_AGENT_INSTALL_DIR>\lib directory, and issue the following command: **ChromeUpgradeHandler.exe enable**

1.2.1 Configuring the Default Start Page for Office 365

If the simulation uses the Office 365 portal to login to the Exchange server, then before beginning the simulation, you need to make sure that the default start page of the Office 365 portal is set to *Mail*. To achieve this, follow the steps below:

1. Open your Chrome browser and connect to the Office 365 portal.
2. Login to the portal using an email ID and corresponding access credentials (see Figure 1.1) that you have configured for the purpose of the simulation. In other words, use any of the **EMAIL IDs** that you have configured for the **Exchange Logon Simulator** test.
3. Once you login successfully, go to the Office 365 Settings page by clicking on the  icon (indicated by Figure 1.1).



email

Figure 1.1: Clicking on the Settings icon in the Office 365 portal

4. In the Settings page that appears next (see Figure 1.2), select *Mail* from the **Start page** drop-down and click the **Save** button to save the changes.

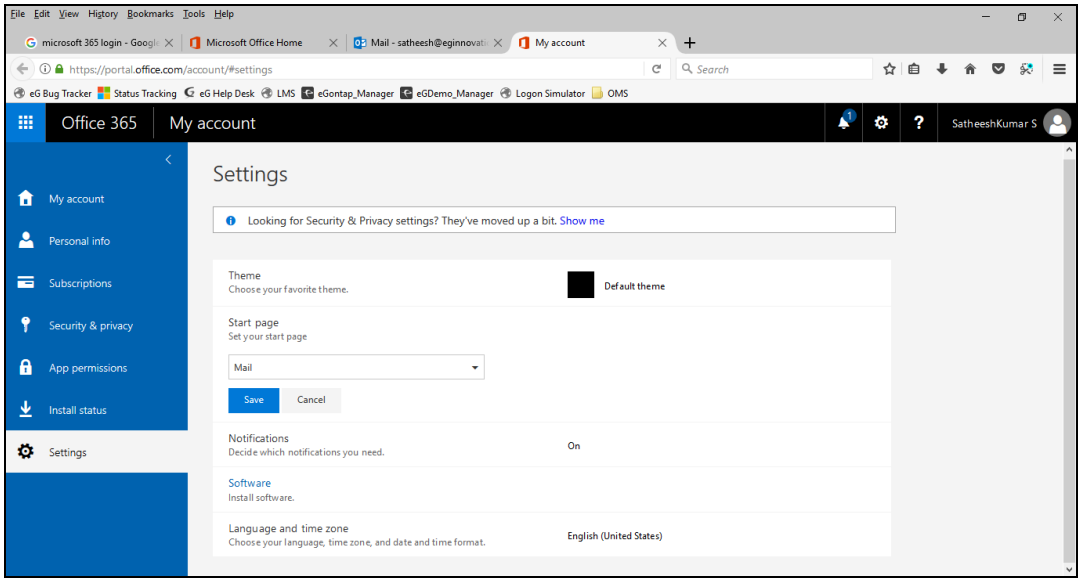


Figure 1.2: Setting Mail as the Start page

5. Repeat steps 2 to 4 for each email ID that has been configured for the **Exchange Logon Simulator** test.

Chapter 2: Configuring the eG Enterprise Logon Simulator for Exchange to Perform the Simulation

Once the pre-requisites listed in Section **1.2** are fulfilled, follow the steps detailed below to get the simulator up and running.

1. Log into the eG administrative interface.
2. Add a dedicated external agent for the purpose of the simulation. For that, follow the Agents -> External Agents menu sequence and click on the **Add New Agent** button. Then, specify the IP address/host name of the system that is hosting the dedicated external agent, and also provide a **Nick name** for the agent (see Figure 2.1).

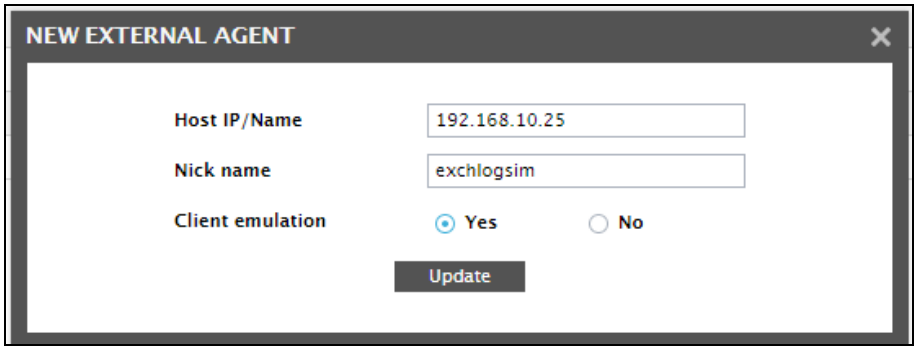


Figure 2.1: Adding a dedicated external agent for the simulation

3. Also, make sure that the **Client emulation** flag is set to **Yes** for the agent.
4. Finally, click the **Update** button in Figure 2.1 to save the changes.
5. Once this external agent is started, it simulates the entire logon process by periodically running an **Exchange Logon Simulator** test. Since this test is mapped to an Exchange Logon Simulator component, you now need to manage a component of that type. For this, follow the Infrastructure -> Components -> Add/Modify menu sequence, and then pick **Exchange Logon Simulator** from the list of **Component types**. Then, click **Add New Component**. When Figure 2.2 appears, add an Exchange Logon Simulator using any IP address and nick name you want.

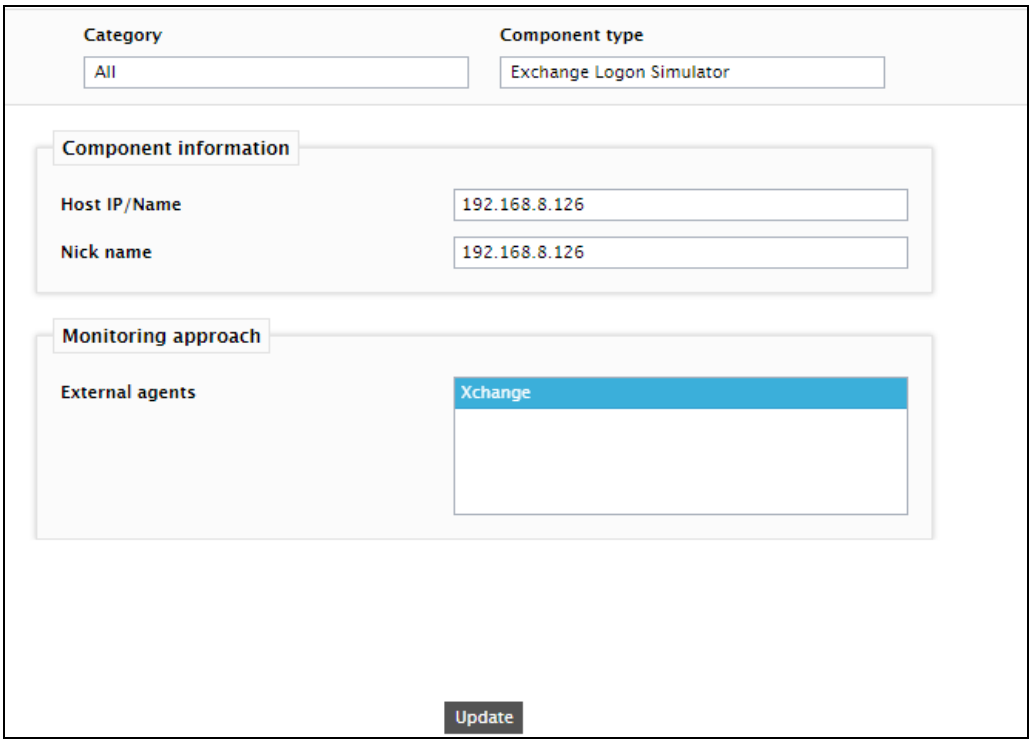
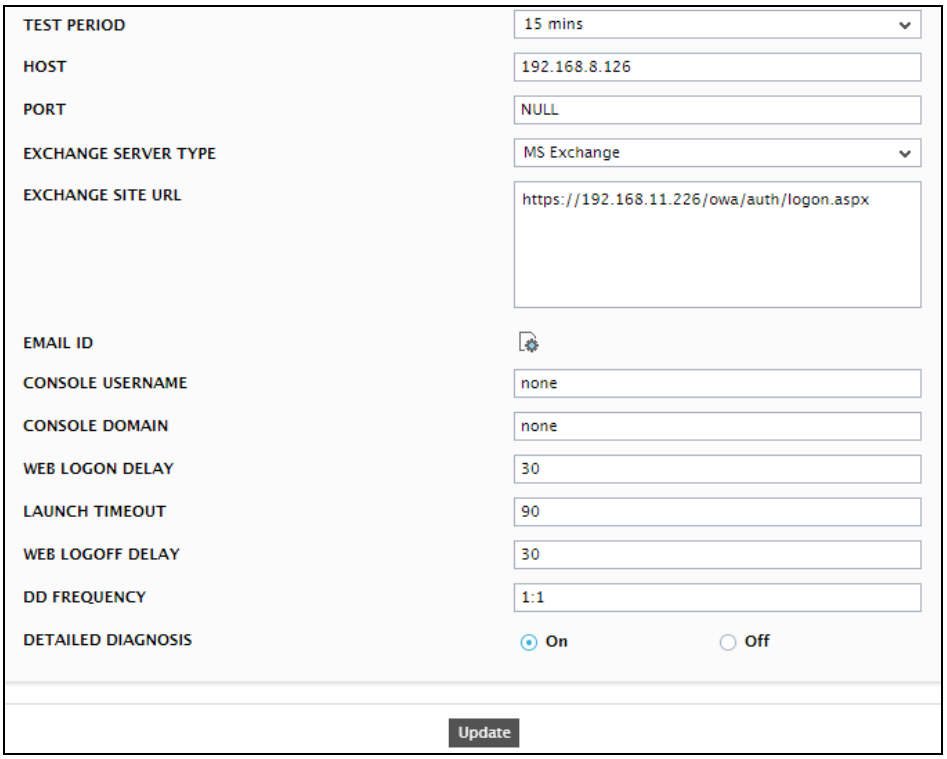


Figure 2.2: Adding an Exchange Logon Simulator

6. When adding, make sure you assign the dedicated external agent, which you had previously installed and configured for the sole purpose of this simulation, to the simulator component.
7. After clicking **Update** in Figure 2.2, proceed to sign out of the eG administrative interface. You will then be prompted to configure the **Exchange Logon Simulator** test for this component. Click on the test to configure it.
8. Chapter 2 will then appear.



9. To know how to configure the test, refer to the Section **Chapter 3** topic.
10. Once all parameters are configured, click the **Update** button to save the configuration.

Chapter 3: Analyzing the Simulation Results

Once the simulation ends, the Logon Simulator Agent sends the availability and duration measures it collects to the eG manager. Using a specialized **Exchange Logon Simulator** monitoring model, the eG manager captures these metrics and publishes them in the eG monitoring console for analysis.

Figure 3.1: The layer model of an Exchange Logon Simulator component

As can be inferred from Figure 3.1, this monitoring model consists of a single **Exchange User Experience** layer, to which the **Exchange Logon Simulator** test is mapped. The Exchange Logon Simulator Test section describes how this test works and the measures it reports.

3.1 The Exchange Logon Simulator Test

This test emulates a user logging into an Exchange server and accessing a mailbox. In the process, the test reports the total duration of the simulation, time taken for the login, and the time taken for accessing the mailbox. Additionally, the test also captures failures (if any) at each step of the simulation. Using the real-time and detailed insights provided by this test, Exchange administrators can proactively detect logon slowness/failures and precisely pinpoint when the slowness/failure occurred - is it when accessing the web interface? during login authentication? or during mailbox access? This way, Exchange administrators are enabled to isolate the probable pain-points of the Exchange infrastructure, even before users complain.

Target of the test : Exchange 2013/2016 server

Agent deploying the test : An external agent

Outputs of the test : One set of results for every email ID configured for monitoring

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed. The default is 15 minutes.

   Note:

   Some parameter changes can sometimes impact the simulation duration. Most often, this can

happen in the following situations:

- If multiple mailboxes are configured for monitoring against **EMAIL ID**: In this case, the test will repeat the entire sequence of steps for every configured email ID - i.e., after a mailbox is accessed, the test will logoff and then log in again to attempt opening another mailbox. This can increase the duration of the simulation.
- If the value of the **LAUNCH TIMEOUT**, **WEB LOGON DELAY**, and/or the **WEB LOGOFF DELAY** parameters of the test is significantly increased: If this is done, then the test will wait that much longer for the mailbox access or logoff to happen, thereby increasing simulation duration.

Sometimes, these changes can cause the simulation to take more time than the configured **TEST PERIOD**.

If this happens, the test will fail after logging an error to that effect in the <EG_AGENT_INSTALL_DIR>\agent\error_log file. To avoid this, it would be good practice to relook at the **TEST PERIOD** configuration every time one of the parameters mentioned above is modified, and increase it if required.

2. **HOST** - The host for which the test is to be configured
3. **PORT** - Refers to the port used by the Exchange server
4. **EXCHANGE SERVER TYPE** - Indicate how the test should access the Exchange server. If the test should access Exchange via the Outlook Web Access (OWA) interface, then select the **MS Exchange** option from this drop-down. If the test should access Exchange via the Office 365 portal, then pick the **Office365** option from this drop-down. If the *Office365* option is chosen, then make sure that the default start page of the Office 365 portal is set to *Mail* for every **EMAIL ID** that you configure for this test. The steps for achieving this are detailed in Section **1.2.1**. Once this is done, make sure you clear the browser history.
5. **EXCHANGE SITE URL** - Specify the URL for connecting to Exchange server. You can provide an HTTP or an HTTPS URL here.
6. **EMAIL ID -** To know how to configure the email IDs for the simulation, refer to Section **3.1.1**.
7. **CONSOLE USERNAME** - The Logon Simulator Agent needs to run in the account of a user who has local administrator rights on the simulation end point - i.e., the system on which the agent has been installed. Specify the name of this user here. This user should also be logged in at all times for the simulator to run continuously.
8. **CONSOLE DOMAIN** - Specify the domain to which the user configured against **CONSOLE USERNAME** belongs.
9. **LAUNCH TIMEOUT** - By default, this parameter is set to 90 seconds. This implies that the

simulator will wait for a maximum of 90 seconds (by default) for a configured mailbox to open. If the mailbox cannot be opened even after the 90 seconds have elapsed, then the simulation will be automatically terminated, and the simulator will report that the mailbox is unavailable. Accordingly, the *Inbox availability* measure for that email ID will report the value 0, and no *Inbox folder access duration* will be reported for the same.

In some environments, it may be normal for some mailboxes to take longer than the rest to open. In such environments, you can instruct the simulator to wait longer for each mailbox to open, by increasing the **LAUNCH TIMEOUT**. The high time out setting for mailbox access ensures that the simulator captures and reports only genuine failures, and does not treat an access delay as a failure.

10. **WEB LOGON DELAY** - By default, this parameter is set to 30 seconds. This implies that the test will wait for a maximum of 30 seconds (by default) to login to the Exchange server. If the login does not happen even after the 30 seconds have elapsed, then the simulation will be automatically terminated, and the simulator will mark the login attempt as 'failed'. A login duration will hence not be computed or reported in this case.

    In some environments, even during normal operation, login may take longer. In such environments, you can instruct the simulator to wait longer for the login to occur, by increasing the **WEB LOGON DELAY**. The high time out setting for login ensures that the simulator waits for the login to complete and captures and reports the accurate login duration.

11. **WEB LOGOFF DELAY** - By default, this parameter is set to 30 seconds. This implies that the test will wait for a maximum of 30 seconds (by default) after each mailbox access, for the logoff to occur. If the logoff does not happen even after 30 seconds, then the simulation will be automatically terminated, and the simulator will mark the logoff attempt as 'failed'. A logoff duration will hence not be computed or reported in this case.

    In some environments, even during normal operation, logoff may take longer. In such environments, you can instruct the simulator to wait longer for the logoff to occur, by increasing the **WEB LOGOFF DELAY**. The high time out setting for logoff ensures that the simulator waits for the log off to complete and captures and reports the accurate logoff duration.

12. **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.

13. **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

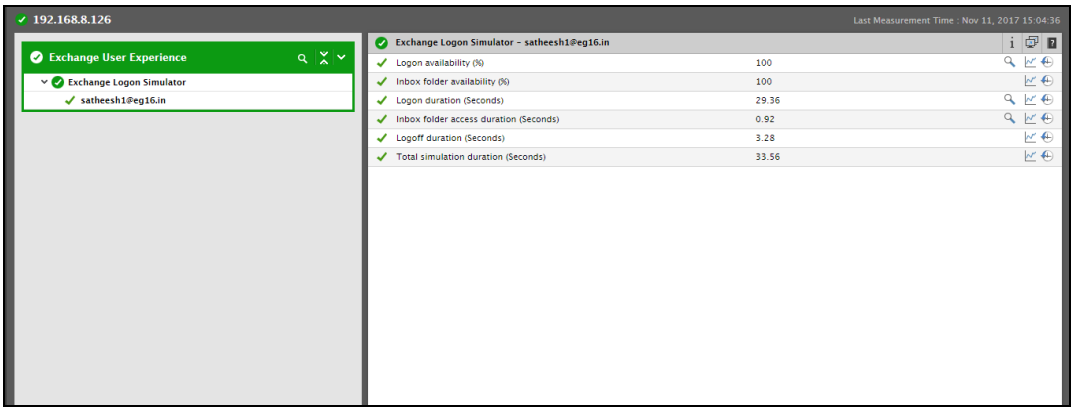


Figure 3.2: The measures reported by the Exchange Logon Simulator test

Measurement	Description	Measurement Unit	Interpretation
Logon availability:	Indicates whether/not the simulator logged into the Exchange server successfully, when attempting to access this mailbox.	Percent	The value 100 for this measure indicates that logon was successful, and the value 0 indicates that logon failed. If this measure reports the value 0, then no other measures will be reported for that mailbox. You can also use the detailed diagnosis of this measure to view the output of the simulation script,

Measurement	Description	Measurement Unit	Interpretation
			scrutinize it, and isolate the failure and problem points of the Exchange infrastructure at first glance.
Logon duration:	Indicates the time taken by the simulator to login to the Exchange server (via the OWA interface or Office365 portal), when attempting to access this mailbox.	Secs	If the *Total simulation duration* for a mailbox exceeds its threshold, compare the value of this measure with that of the other duration values reported by the test to know where the bottleneck lies - in login? or mailbox access? or log out? If the comparison reveals a bottleneck at login, then use the detailed diagnosis of this measure to view the output of the simulation script. This will point you to the exact login step where the delay/failure occurred - was it when launching the chrome browser? was it because the login form took too long to open? or was it due to a delay in authentication?
Inbox folder availability:	Indicates whether/not this mailbox was successfully opened.	Percent	The value 100 for this measure indicates that the mailbox was successfully opened, and the value 0 indicates that access failed.
Inbox folder access duration:	Indicates the time taken for this mailbox to open.	Secs	If the *Total simulation duration* for a mailbox exceeds its threshold, compare the value of this measure with that of the other duration values reported by the test to know where the bottleneck lies - in login? or mailbox access? or log out? If the comparison reveals a bottleneck at login, then use the detailed diagnosis of this measure to view the output of the simulation script. This will point you to the exact login step where the delay/failure occurred - was

Measurement	Description	Measurement Unit	Interpretation
			it when launching the chrome browser? was it because the login form took too long to open? or was it due to a delay in authentication?
Logoff duration:	Indicates the time taken by the simulator to log out of the OWA interface or Office 365 portal, while simulating a user access to this mailbox.	Secs	If the *Total simulation duration* for a mailbox exceeds its threshold, compare the value of this measure with that of the other duration values reported by the test to know where the bottleneck lies - in login? or mailbox access? or log out?
Total simulation duration:	Indicates the total time taken by the simulator to simulate a user access to this mailbox.	Secs	An abnormally high value for this measure could indicate a logon slowness. In such a case, compare the value of all the duration values reported by the test to know where the bottleneck lies - in login authentication? application enumera in login? or mailbox access? or log out? If the comparison reveals a bottleneck at login, then use the detailed diagnosis of this measure to view the output of the simulation script. This will point you to the exact login step where the delay/failure occurred - was it when launching the chrome browser? was it because the login form took too long to open? or was it due to a delay in authentication?

Use the detailed diagnosis of the Logon availability measure to view the output of the simulation script, scrutinize it, and isolate the failure and problem points of the Exchange infrastructure in a single glance. A summary of the simulation is also provided as part of the detailed diagnostics. This includes the Site URL configured for monitoring, the email ID configured for the simulation, and the exact time at which the simulated user logged into the site.

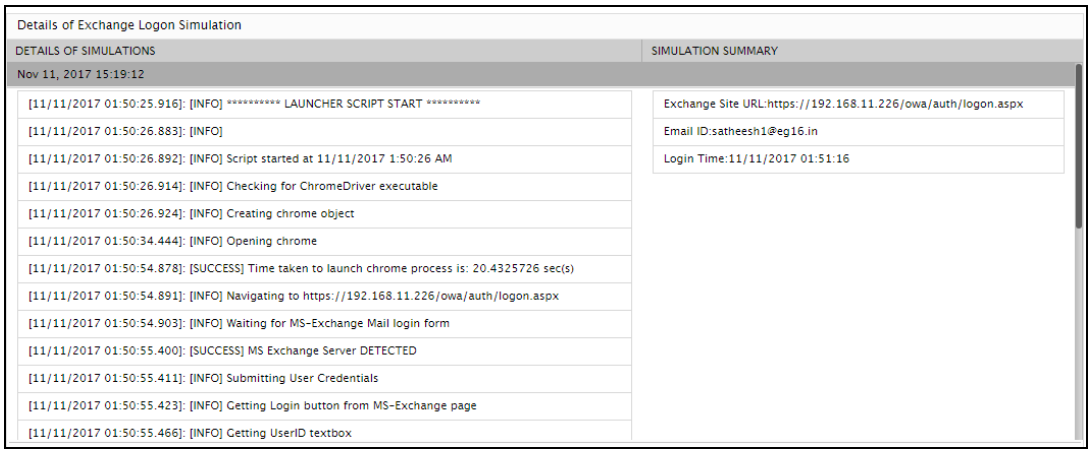


Figure 3.3: The detailed diagnosis of the Logon availability measure

3.1.1 How to Configure Email IDs for Monitoring?

eG Enterprise provides a special page using which you can configure multiple email IDs and their access credentials for monitoring. To access this page, click the button against the **EMAIL ID** parameter in the Exchange Logon Simulator test configuration page. This will invoke Figure 3.4.

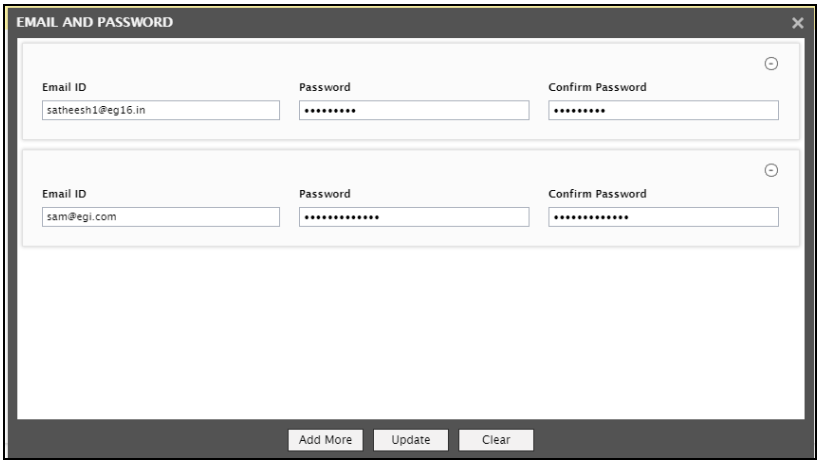


Figure 3.4: Configuring email IDs for monitoring

To configure email IDs using Figure 3.4, follow the steps below:

1. In the **Email ID** text box, configure a valid email ID that the simulation should use.
2. Specify the **Password** for accessing the mailbox mapped to the configured **Email ID**.
3. Confirm the **Password** by retyping it in the **Confirm Password** text box.

4. To configure one more email ID, click the **Add More** button in Figure 3.4. A blank record will pop up, using which you can configure one more email ID and its password.
5. To remove an email ID, click the ⊖ button corresponding to that record.
6. To save the changes, click the **Update** button.
7. To cancel all changes, click the **Clear** button.

Chapter 4: Fine-tuning the Simulation

One of the key pre-requisites for the simulation is a user account with local administrator rights on the simulation endpoint. This user should also be logged in at all times for the simulator to run continuously. Sometimes however, this user session may get disconnected. For instance, if the simulation endpoint is rebooted due to automatic updates, scheduled reboots, power failure etc., the user session on the simulation endpoint may get disconnected.

Every time a session disconnect occurs owing to reasons cited above, the administrator will have to login to the endpoint by manually providing the user credentials at the login prompt, while the system boots. If this is not done, then the user session will not get up and running; consequently, the simulation will not occur.

To save the time and effort involved in manually typing the login credentials everytime the endpoint reboots, and to make sure that a user is always logged into the endpoint (even when it reboots) for the purpose of the simulation, you can automate a user login at the time of a reboot. To achieve this, you can either run *Autologon.exe* or manually *edit the windows registry*.

4.1 Fine-tuning the simulation using Autologon.exe

If you wish to automate the user logon by executing Autologon.exe, follow the steps below:

1. Download the **Autologon.zip** file from the **Download Autologon** link from the following location:

   https://docs.microsoft.com/en-us/sysinternals/downloads/autologon

2. Extract the contents of the **Autologon.zip** file.
3. Once extracted, run the **Autologon.exe** file.

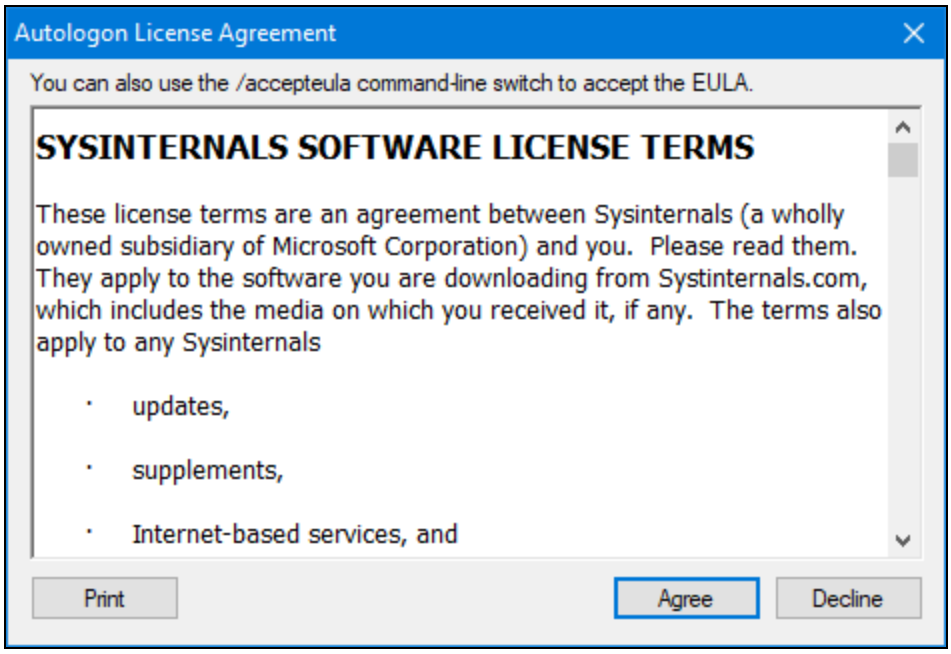


Figure 4.1: Agreeing to the Software License Terms

4. Figure 4.1 then appears. Click **Agree** to accept the Sysinternals Software License Terms.

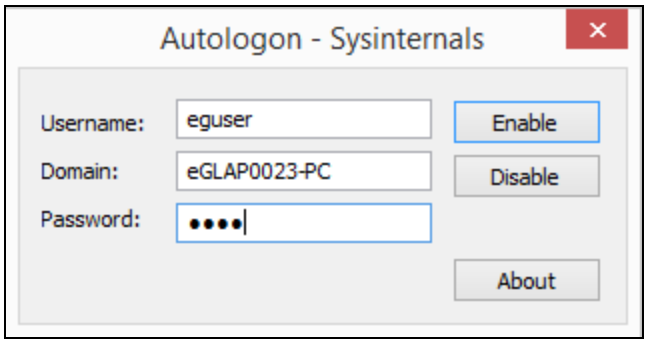


Figure 4.2: Provide the password in this form

5. In Figure 4.2 that appears next, the name of the user and the domain to which the user belongs will be automatically populated against the **Username** and **Domain** fields. Specify the password that should be used for automatic user logon against the **Password** text box.
6. Click the **Enable** button.
7. Ensure that the **eGurkhaAgentServices** are delayed for a period of 5 minutes (using Automatic (Delayed Start) Service properties) before restarting the simulation endpoint.
8. Finally, restart the simulation endpoint.

4.2 Fine-tuning the simulation by editing the windows registry

If you wish to automate the user login by editing the windows registry, follow the steps below:

1. Open the Windows Registry Editor.
2. Locate the following registry entry:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
3. In this registry entry, add the following REG_SZ string values:
   - **AutoAdminLogon:** To enable automatic user logon on the simulation endpoint, set this string value to 1.
   - **DefaultUserName:** Specify the name of the user who is authorized to login into the simulation endpoint.
   - **DefaultPassword:** Specify the password for the user mentioned in the DefaultUserName. **Note that the password should be entered in plain text.**
   - **DefaultDomainName:** Specify the domain to which the user belongs to.
4. Ensure that the **eGurkhaAgentServices** are delayed for a period of 5 minutes (using Automatic (Delayed Start) Service properties) before restarting the simulation endpoint.
5. Finally, restart the simulation endpoint.

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.