The eG Enterprise Logon Simulator for VMware Horizon

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

For years, slow logons have been the most common complaint in VMware Horizon infrastructures. For a VMware Horizon user, slow logons can lead to frustration, lower productivity and efficiency. For a VMware administrator, logon slowness is a complex problem that takes a long time to resolve. There are dozens of steps involved in the logon process and they involve multiple components – VMware Horizon Client, VMware Horizon Connection Server, Active Directory, VMware vCenter, VMware vSphere ESX/VDI, VMware Horizon Composer and so on. Identifying exactly what is causing the slowdown is often time consuming and laborious.

To ensure great VMware Horizon user experience, administrators need to monitor their infrastructure proactively and be alerted to issues in advance, before users notice and complain. In order to do so, administrators need a consistent measure of VMware Horizon logon performance – one that is available 24x7, even when there are no users accessing the farm. Collecting logon metrics of real user activity is challenging. Metrics have to collected from the different tiers involved. Even then, it is difficult to get a consistent assessment of VMware Horizon logon performance because different users have different profiles and policies associated with them. Furthermore, there will be times when no one is logging in to the VMware Horizon farm, and at those times, it is important to know if VMware Horizon logon is working and whether users can launch their applications and desktops successfully.

The eG Logon Simulator, a part of the eG Enterprise suite, is a purpose-built solution for delivering proactive visibility into the logon performance in VMware Horizon infrastructures. Using an agentless approach, the eG VMware Horizon Logon Simulator simulates a user logging in to a VMware Unified Access Gateway or Access Point through a browser, reviewing the list of applications/desktops accessible, clicking on a selected application or desktop, launching it VMware Horizon Connection Server by initiating a session and then logging off. By emulating the exact same process that users go through when they logon to to VMware Horizon Connection server, the eG VMware Horizon Logon Simulator provides a realistic measure of the user experience during logon. Since every simulation tests the entire VMware infrastructure (VMware Horizon Client, VMware Horizon Connection Server, Active Directory, VMware vCenter, VMware vSphere ESX/VDI, VMware Horizon Composer, etc.), the results represent the cumulative health of all of the tiers supporting logons.

Unlike traditional simulation tools that require recording of a script that captures the typical steps a user performs, the eG VMware Horizon Logon Simulator requires no recording and hence, is simple to implement. Installed on any desktop that has the Chrome browser configured, the simulator targets the configured VMware Horizon logon URL and application/desktop 24x7 at pre-configured intervals and tests the VMware horizon 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 Pre-requisites for Using the VMware Horizon Logon Simulator

Before attempting to use the simulator, make sure that the following pre-requisites are fulfilled:

Category	Pre-requisites
Logon Simulator Agent / Simulation Endpoint	• Client Emulation capability should be enabled on the eG license. • The logon simulator agent / external agent should be installed on a dedicated virtual machine or a physical server running Windows 2008/2012/2016/2019 or Windows 7/8/10 operating system. • The logon simulator agent / external agent should only run an English version of Windows operating system. **Note:** If Multilingual User Interface pack is applied on the Windows operating system, then, ensure that the English language is chosen as the System locale. • The logon simulator agent / external agent should not be used to monitor any other component in the target environment. • Microsoft .Net 3.5 (or above) should pre-exist on the system hosting the logon simulator agent/external agent. • The simulator requires a dedicated VMware Horizon user account with rights to launch applications/desktops. • The simulator also 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.

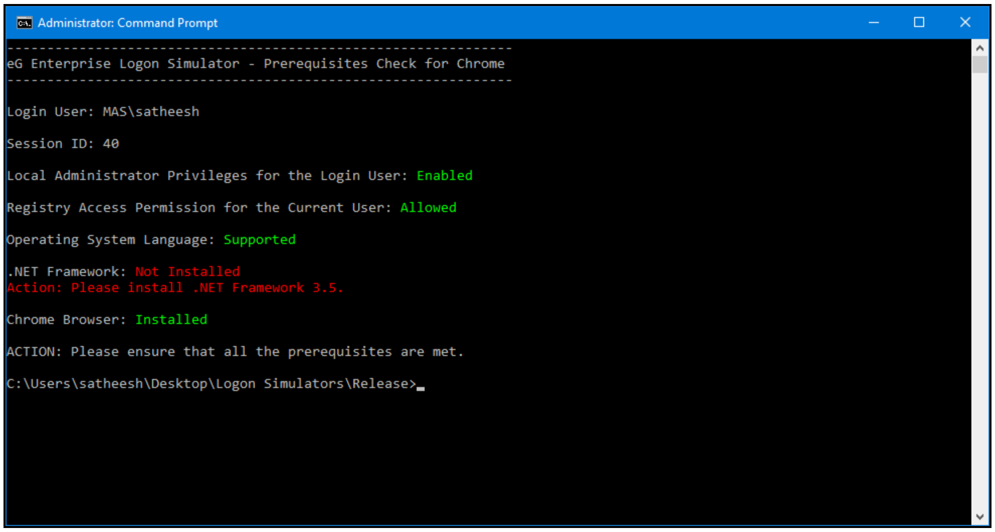
	Note: - The logon simulation will not work if the session is closed.
Environment	- The simulator will only work with VMware Horizon Connection Server 7.x environments. - The simulator will work only when VMware Horizon HTML Access is installed on the VMware Horizon Connection Server. Ensure that the *'Enabled'* check box against the **Allow HTML Access to Desktops and Applications on this farm** field of each desktop/application within a VMware Horizon farm is checked. Similarly, ensure that the *'Enabled'* check box against the **HTML Access** field in the **Desktop Pool settings** pop up window of each application /desktop within a desktop pool is checked. - The VMware Horizon Workspace cannot be used for the simulation. - Single Sign-On i.e., True SSO feature should be enabled on the VMware Horizon Connection Server. - The eG Enterprise Express Logon Simulator for VMware Horizon can be used to simulate logons to the on-premise VMware installations. Typically, the simulator simulates a user logging into an Access Point (VMware Unified Access Gateway) or VMware Horizon Connection Server through a browser, reviewing the list of applications/desktops accessible, clicking on a selected application or desktop, launching it by initiating a session, and then logging off. Sometimes, the simulator may not be able to cleanly logoff the application/desktop sessions it created. Such sessions may continue to linger on the server in a disconnected state. In simulations that are performed on-premise, where you have control over the target VMware infrastructure, you can avoid such disconnected sessions and ensure clean application/desktop logoffs by deploying the light-weight **eG Logoff Helper** software. Install the helper software on the VMware Horizon Connection Server. - The allocated desktop that is to be launched by simulation should be powered on and also should be a dedicated desktop. - If a firewall separates the simulation endpoint from the Access Point (VMware Unified Access Gateway) / VMware Horizon Connection Server, then make sure you configure the firewall to allow two-way

	communication between the endpoint and Access Point (VMware Unified Access Gateway) / VMware Horizon Connection Server. - By default, the **Hide domain list in client user interface** global setting of the VMware Horizon Connection server is enabled implying that the users logging into the VMware Horizon Connection through the Horizon client can provide the domain credentials along with the user credentials in the **User Name** text box in the format: **domain\username or username@domain** . If two- factor authentication is also enabled on the VMware Horizon Connection Server, then, administrators should not enforce Windows user name matching. Enforcing Windows user name matching will prevent users from being able to enter domain information in the **User Name** text box resulting in login failures.
Browser	Chrome browser v81 (and above) should be available on the dedicated endpoint. **Note:** In some environments where browsers are automatically updated to their latest versions, incompatibility is cited between the browser version and the Chrome drivers. This may sometimes lead to the nonstart of simulation. Therefore, ensure that the Chrome drivers are also updated whenever the browser is updated to the latest version. 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, eG Enterprise Logon Simulator for VMware, 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**

Note:

To ensure that all the pre-requisites of the VMware Horizon Logon Simulator is fulfilled, you can execute the **LogonSimulatorChecks.exe** which is available in the **<eG_INSTALL_DIR>\lib** folder. This executable should be executed by a user with administrator privileges from the command prompt of the target agent host. If any pre-requisite has not been fulfilled, failure will be highlighted in Red (as shown by Figure 1.1).

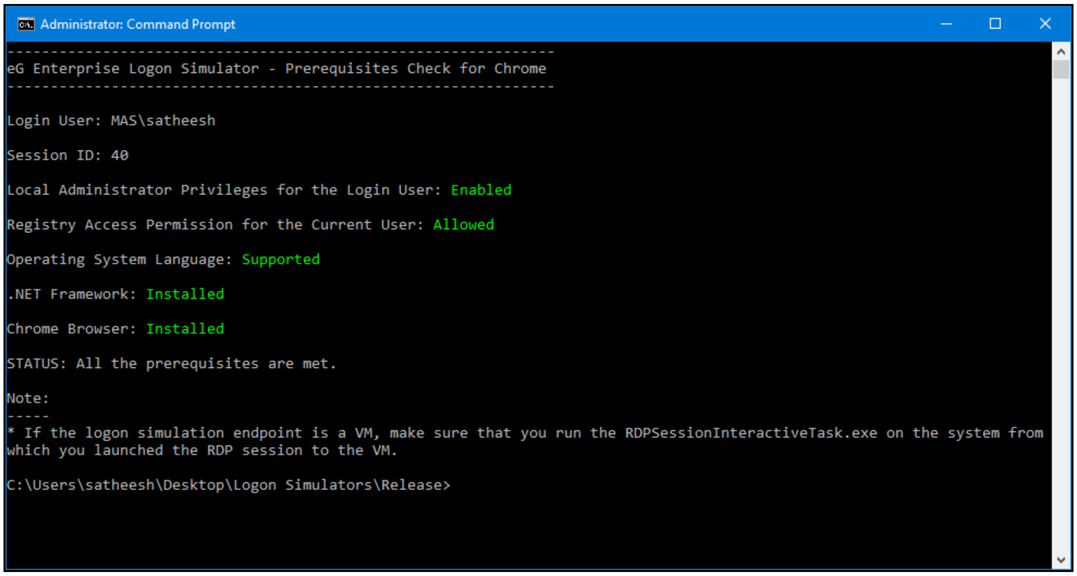


```
---------------------------------------------------------------
eG Enterprise Logon Simulator - Prerequisites Check for Chrome
---------------------------------------------------------------

Login User: MAS\satheesh

Session ID: 40

Local Administrator Privileges for the Login User: Enabled

Registry Access Permission for the Current User: Allowed

Operating System Language: Supported

.NET Framework: Not Installed
Action: Please install .NET Framework 3.5.

Chrome Browser: Installed

ACTION: Please ensure that all the prerequisites are met.

C:\Users\satheesh\Desktop\Logon Simulators\Release>
```

Figure 1.1: Setup script where a pre-requisite has failed

Use the pointers provided in Figure 1.1, just below the failed pre-requisite, to know how to fulfill that requirement. Then, rerun the **LogonSimulatorChecks.exe** to make sure that all pre-requisites are fulfilled, and then proceed.

If all pre-requisites are fulfilled, then Figure 1.2 will appear.



```
---------------------------------------------------------------
eG Enterprise Logon Simulator - Prerequisites Check for Chrome
---------------------------------------------------------------

Login User: MAS\satheesh

Session ID: 40

Local Administrator Privileges for the Login User: Enabled

Registry Access Permission for the Current User: Allowed

Operating System Language: Supported

.NET Framework: Installed

Chrome Browser: Installed

STATUS: All the prerequisites are met.

Note:
-----
* If the logon simulation endpoint is a VM, make sure that you run the RDPSessionInteractiveTask.exe on the system from
which you launched the RDP session to the VM.

C:\Users\satheesh\Desktop\Logon Simulators\Release>
```

Figure 1.2: All pre-requisites are fulfilled

1.1.1 The eG Logoff Helper

The eG Enterprise Express Logon Simulator for VMware Horizon can be used to simulate logons to on-premise VMware Horizon installations. Typically, the simulator simulates a user logging into a VMware Horizon Connection Server or VMware Unified Access Gateway through a browser, reviewing the list of applications/desktops accessible, clicking on a selected application or desktop, launching it through the VMware Horizon Client by initiating a session, and then logging off. Sometimes, the simulator may not be able to cleanly logoff the application/desktop sessions it created. Such sessions may continue to linger on the server in a disconnected state. In simulations that are performed on- premise, where you have control over the target VMware Horizon infrastructure, you can avoid such disconnected sessions and ensure clean application/desktop logoffs by deploying the light-weight **eG Logoff Helper** software. Install the helper software on the VMware Horizon Connection Server.

To install the eG Logoff Helper, follow the steps below:

1. Run the **eGLogoffHelper.exe** as an *Administrator* (see Figure 1.3).

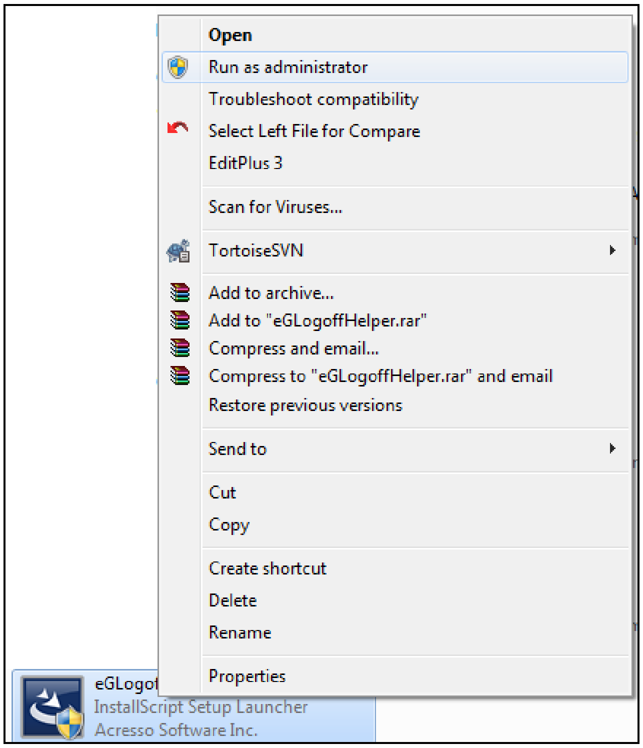
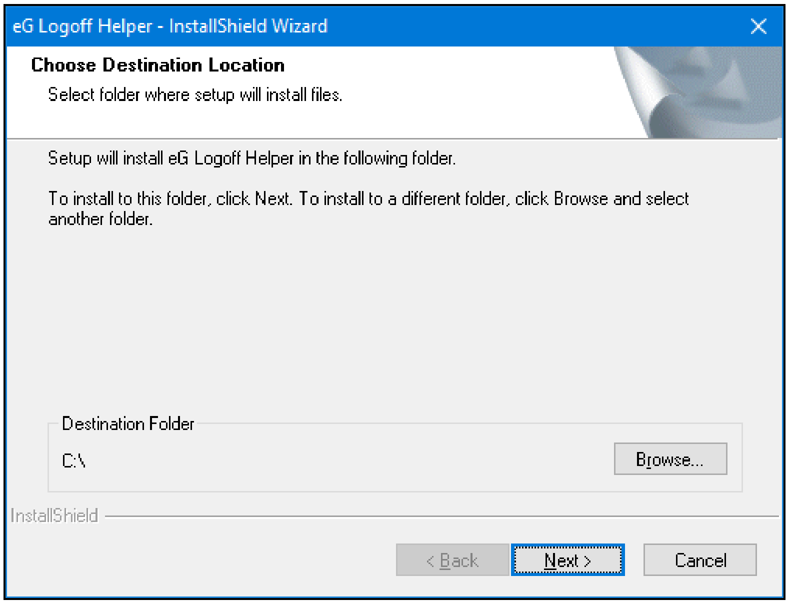


Figure 1.3: Running the eGLogoffHelper.exe as an Administrator

2. Figure 1.4 will then appear. By default, the logoff helper will be installed in the C drive. You can change the location of the helper by specifying a different install location. For making this change, use the **Browse** button in Figure 1.4. Then, click the **Next** button in Figure 1.4 to proceed.



eG Logoff Helper - InstallShield Wizard

Choose Destination Location

Select folder where setup will install files.

Setup will install eG Logoff Helper in the following folder.

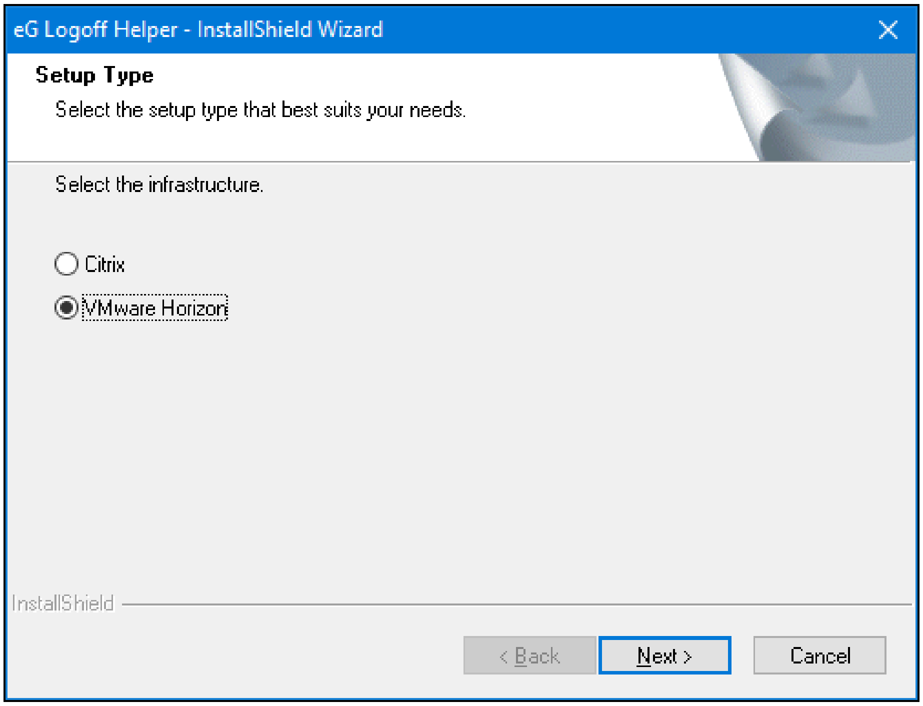
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\

Figure 1.4: Specifying where the logoff helper is to be installed

3. When Figure 1.5 appears, select **VMware Horizon** as the infrastructure and click **Next** to move on.



eG Logoff Helper - InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

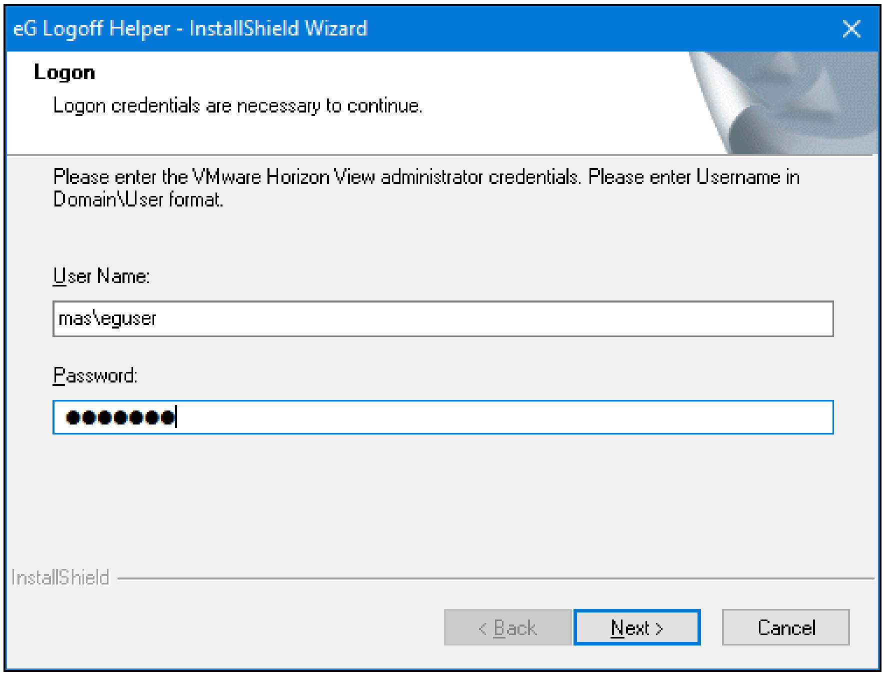
Select the infrastructure.

○ Citrix

● VMware Horizon

Figure 1.5: Selecting VMware Horizon as the infrastructure

4. In Figure 1.6 that appears next, provide the VMware Horizon farm administrator's credentials. This is essential for creating and running the eG Logoff Helper Windows service on the VMware Horizon Connection Server. **Note that the User Name of the VMware Horizon farm administrator should be provided in the format, <DomainName>\<UserName>**.


eG Logoff Helper - InstallShield Wizard
Logon
Logon credentials are necessary to continue.
InstallShield
< Back
Next >
Cancel

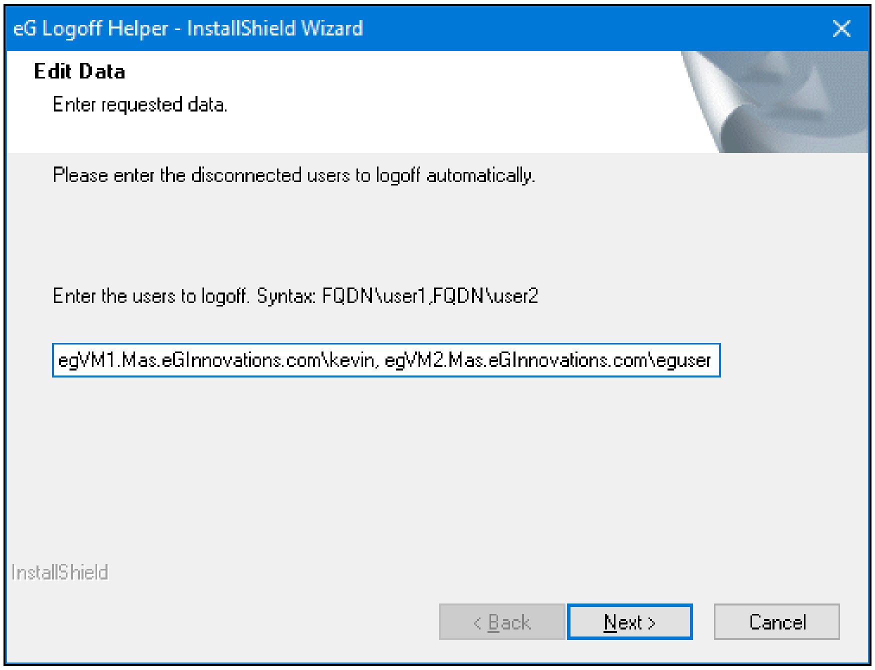
Please enter the VMware Horizon View administrator credentials. Please enter Username in Domain\User format.

User Name:
mas\eguser

Password:
●●●●●●●

Figure 1.6: Providing the credentials of a VMware Horizon administrator

5. Next, provide a comma-separated list of application/desktop users to be logged off. This user list should be the whole or a part of the list of users who you have configured for your simulation. Each user name in this comma-separated list should be specified in the format, *<DomainName>\<UserName>*. Then, click the **Next** button.



Edit Data

Enter requested data.

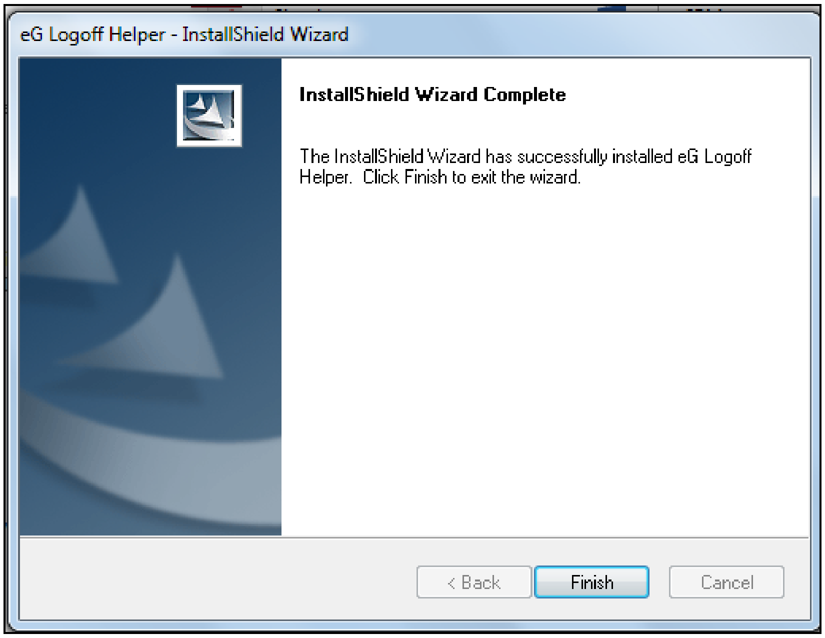
Please enter the disconnected users to logoff automatically.

Enter the users to logoff. Syntax: FQDN\user1,FQDN\user2

egVM1.Mas.eGInnovations.com\kevin, egVM2.Mas.eGInnovations.com\eguser

Figure 1.7: Providing a comma-separated list of application/desktop users to logoff

6. Upon successful installation of the helper, a message depicted by Figure 1.8 will appear.



InstallShield Wizard Complete

The InstallShield Wizard has successfully installed eG Logoff Helper. Click Finish to exit the wizard.

Figure 1.8: Successful installation of the logoff helper

7. Click the **Finish** button in Figure 1.8 to exit the installation wizard.

You can confirm the successful installation of the eG Logoff Helper by verifying the following:

- A folder named **eGLogoffHelper** will be created in the install location specified at step 2 above.
- You will find a new Windows service named **eG Logoff Helper** running with VMware Horizon Connection Server administrator privileges.

1.1.2 Configuring Logging for the eG Logoff Helper

The operations of the eG Logoff Helper are tracked and their status logged in the **eGLogoffHelperLog.txt** file that is automatically created in the <EG_LOGOFF_HELPER_ INSTALL_DIR>\bin directory. By default, only 'information' messages are logged in this log file. From such messages, you can infer when the helper service sent a logoff request for a particular user session, and whether that user session logged off successfully or not. If you want more diagnostic messages to be logged in the log file so that troubleshooting becomes easy, you can enable the logging of DEBUG messages. For this, follow the steps below:

1. Edit the **eGLogoffHelper.exe.config** file in the <EG_LOGOFF_HELPER_INSTALL_ DIR>\bin directory.
2. Search for the parameter, **priority value**, in the file. By default, this will be set to *INFO*. To enable debug message logging, set this parameter to *DEBUG*.
3. Then, save the file.
4. Finally, restart the **eGLogoffHelper** Windows service, so that the changes to the file take effect.

1.2 How does the VMware Horizon Logon Simulator Work?

As stated earlier, a dedicated eG external agent drives the logon simulation. This agent periodically runs a **VMware Horizon Logon Simulator** test that emulates the entire process of a user logging into a VMware Horizon farm and launching an application / desktop. Since the test is what performs the simulation, let's call it the **simulator**. To perform this simulation, the simulator has to be configured with the following:

- The URL of the Access Point (VMware Unified Access Gateway)/VMware Horizon Connection Server that it needs to access
- The credentials using which it needs to log into the VMware Horizon Connection Server;
- The applications and/or desktops that it needs to launch
- The two-factor authentication code, if VMware Horizon Connection Server is enabled with two-factor authentication

To know how to configure the simulator with the details listed above, refer to the Section **Chapter 2** topic.

Once the simulator is configured, it runs at the configured frequency. Every time it runs, it simulates the logon process as depicted by Figure 1.9 below.

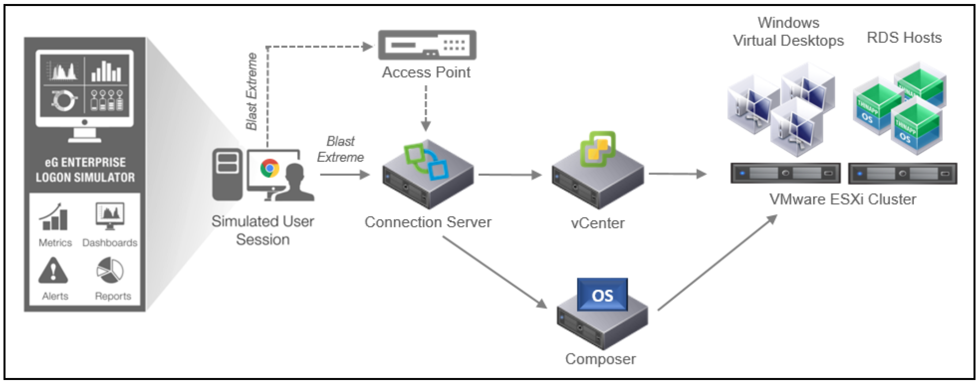


Figure 1.9: How the VMware Horizon Logon Simulator Works

The process depicted by Figure 1.9 is described below:

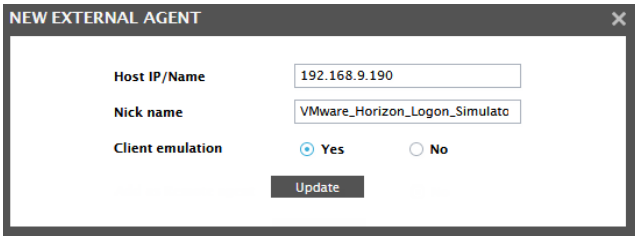
1. The simulator first opens the Chrome and connects to the configured Access Point (VMware Unified Access Gateway)/VMware horizon Connection Server URL
2. It then logs in through the web browser and captures the time taken to login. The success/failure of the login is also determined.
3. The simulator next waits for the applications/desktops to be enumerated and records the time it took for the enumeration to complete. The success/failure of this step is also ascertained.
4. The configured application/desktop is then launched and the duration of the launch is recorded. In the process, the simulator also figures out whether/not the launch was successful.
5. Finally, the simulator closes the application and logs out of the VMware Horizon session. The log out status and duration is also captured.
6. Steps 1 to 5 are then repeated for every application/desktop that has been configured for launching.

The simulator then reports the metrics so collected to the eG manager. The manager captures these metrics into a **VMware Horizon Logon Simulator** component and presents them in the eG monitoring console for analysis. Refer to the Section **Chapter 3** topic for a detailed discussion on the **VMware Horizon Logon Simulator** model.

Chapter 2: Configuring the VMware Horizon Logon Simulator to Perform the Simulation

Once the Section **1.1** 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).



NEW EXTERNAL AGENT

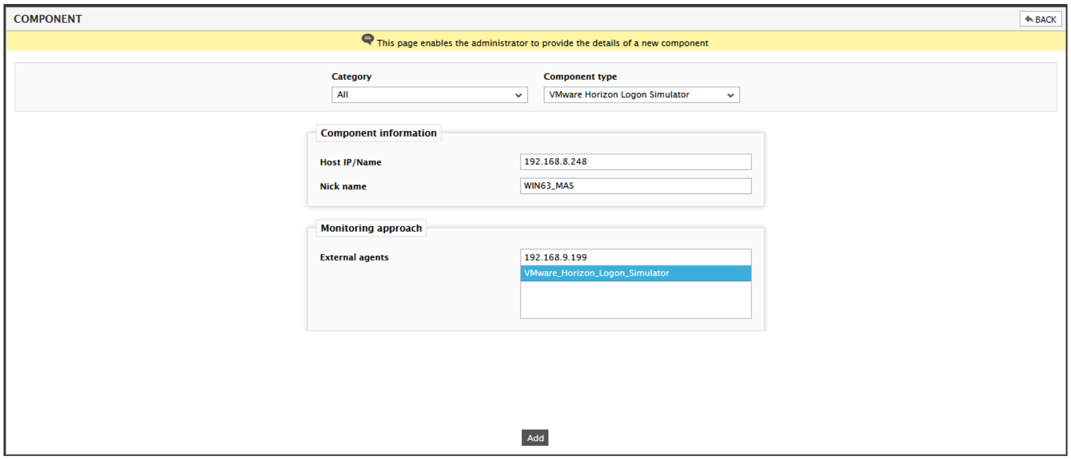
Host IP/Name: 192.168.9.190

Nick name: VMware_Horizon_Logon_Simulato

Client emulation: ● Yes ○ No

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 a **VMware Horizon Logon Simulator** test. It is this test that serves as the **eG VMware Horizon Logon Simulator**. Since this test is mapped to a VMware Horizon 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 **VMware Horizon Logon Simulator** from the list of **Component types**. Then, click **Add New Component**. When Figure 2.2 appears, add a VMware Horizon Logon Simulator using any IP address and nick name you want.



COMPONENT

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

Category: All

Component type: VMware Horizon Logon Simulator

Component information

Host IP/Name: 192.168.8.248

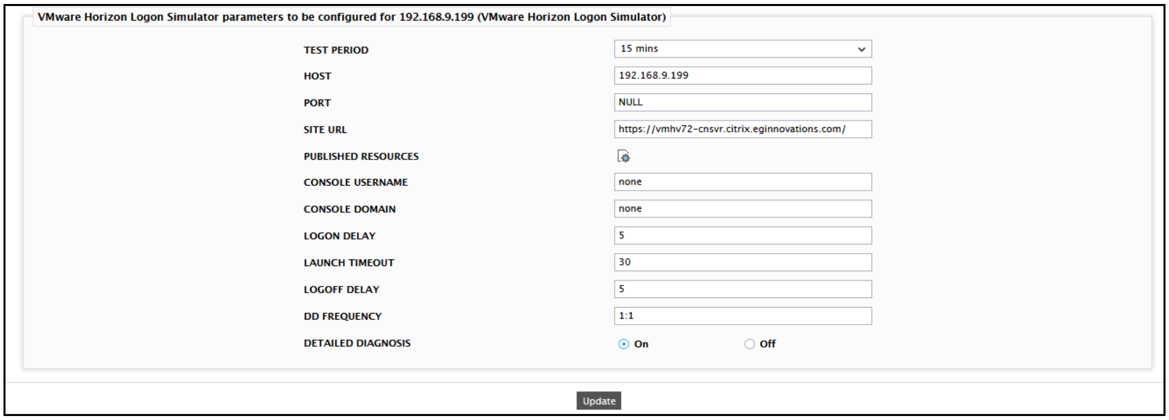
Nick name: WIN63_MAS

Monitoring approach

External agents: 192.168.9.199, VMware_Horizon_Logon_Simulator

Figure 2.2: Adding a VMware Horizon 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 **VMware Horizon Logon Simulator** test for this component. Click on the test to configure it.
8. Figure 2.3 will then appear.



VMware Horizon Logon Simulator parameters to be configured for 192.168.9.199 (VMware Horizon Logon Simulator)

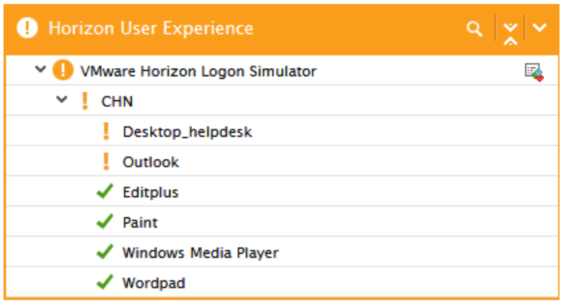
TEST PERIOD	15 mins
HOST	192.168.9.199
PORT	NULL
SITE URL	https://vmhv72-cnsvr.citrix.eginnovations.com/
PUBLISHED RESOURCES	
CONSOLE USERNAME	none
CONSOLE DOMAIN	none
LOGON DELAY	5
LAUNCH TIMEOUT	30
LOGOFF DELAY	5
DD FREQUENCY	1:1
DETAILED DIAGNOSIS	● On ○ Off

Figure 2.3: Configuring the VMware Horizon Logon Simulator test

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 simulator - i.e., the VMware Horizon Logon Simulator test - sends the availability and duration measures it collects to the eG manager. Using a specialized **VMware Horizon Logon Simulator** monitoring model, the eG manager captures these metrics and publishes them in the eG monitoring console for analysis.



Horizon User Experience

- VMware Horizon Logon Simulator
  - CHN
    - Desktop_helpdesk
    - Outlook
    - Editplus
    - Paint
    - Windows Media Player
    - Wordpad

Figure 3.1: The layer model of a VMware Horizon Logon Simulator component

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

3.1 The VMware Horizon Logon Simulator Test

This test emulates a user logging into a VMware Horizon farm and launching an application/desktop. In the process, the test reports the total duration of the simulation, time taken for the login to be authenticated, the time taken for application/desktop ennumeration, duration of application/desktop launch, and log out duration. Additionally, the test also captures failures (if any) at each step of the simulation. Using the insights provided by this test, VMware Horizon administrators can proactively detect logon slowness/failures and precisely pinpoint the root-cause of the anomaly - is it login authentication? enumeration? application/desktop launch? or logout? This way, administrators are enabled to isolate the probable pain-points of their VMware Horizon infrastructure, even before users begin to actively use applications/desktops.

Target of the test : VMware Horizon Connection Server 7.x

Agent deploying the test : An external agent

Outputs of the test : One set of results for every published application and/or virtual desktop that the simulator is configured to launch

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 applications/desktops are configured for launching against **PUBLISHED RESOURCES**: In this case, the test will repeat the entire sequence of steps for every configured application/desktop - i.e., after an application is launched, the test will logoff and then log in again to attempt the launch of the next application. This can increase the duration of the simulation.
   - If the value of the **LAUNCH TIMEOUT** and/or the **LOGOFF DELAY** parameters of the test is significantly increased: If this is done, then the simulator will wait that much longer for the application launch 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 VMware Horizon Connection Server
4. **SITE URL** - Specify the URL for connecting to the Access Point (VMware Unified Access Gateway) / VMware Horizon Connection Server. You can provide an HTTP or an HTTPS URL here. Before specifying the URL, ensure the following:

   - Only VMware Horizon Connection Server 7.x (or above) is supported.

5. **PUBLISHED RESOURCES -** To know how to configure the resources to be monitored, refer to the How to Configure Published Resources for Monitoring? topic.
6. **CONSOLE USERNAME** - The simulator 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 external agent and the VMware Horizon Connection Server have 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.

7. **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 an application/desktop to launch. If the application/desktop does not launch even after the 90 seconds have elapsed, then the simulation will be automatically terminated, and the simulator will mark that application/desktop launch as 'failed'. Accordingly, the *Application launch availability* measure for that published resource (i.e., application/desktop) will report the value 0, and no launch duration will be reported for the same.

   In some environments, one/more published applications may take a little longer to launch than the rest. In such environments, you can instruct the simulator to wait longer for launching each of the configured published resources, by increasing the **LAUNCH TIMEOUT**. The high time out setting for resource launch ensures that the simulator captures and reports only genuine launch failures, and does not treat a launch delay as a failure.

8. **LOGON DELAY** - By default, this parameter is set to 5 seconds. This implies that the simulator will wait for a maximum of 5 seconds (by default) during each resource launch, for the logon to actually occur. If the logon does not happen even after the lapse of 5 seconds, then the simulation will be automatically terminated, and the simulator will mark the logon attempt as 'failed'. A logon duration will hence not be computed or reported in this case.

9. **LOGOFF DELAY** - By default, this parameter is set to 5 seconds. This implies that the simulator will wait for a maximum of 5 seconds (by default) after each resource launch, for the logoff to occur. If the logoff does not happen even after the lapse of 5 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.

10. **2FA CODE** - Two-factor authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are. If the Access Point (VMware Unified Access Gateway) / VMware Horizon Connection Server is enabled with two-factor authentication, then to authenticate the specified **User** login, Access Point (VMware Unified Access Gateway) / VMware Horizon Connection Server will require an additional layer of security other than the **Password** you have provided. This can be any piece of information that only the **Use**r knows or has immediately in hand - such as a verification code that the Access Point (VMware Unified Access Gateway) / VMware Horizon Connection Server provides. In this case therefore,

specify this verification code against **2FA code**, so that the configured **User** login is validated and the simulation proceeds without a glitch. On the other hand, if Access Point (VMware Unified Access Gateway) / VMware Horizon Connection Server is not enabled with two-factor authentication, specify *none* here.

11. **DISCLAIMER** - Set this flag to *Yes*, if you want the simulator to automatically accept the disclaimers that typically appear when opening a session on a desktop. If you set *No* here, then the simulation will terminate as soon as a disclaimer appears.

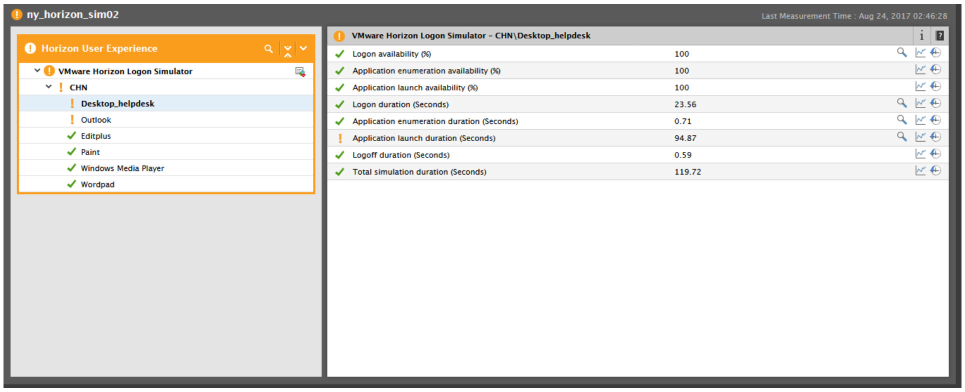
12. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify 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



ny_horizon_sim02

Last Measurement Time : Aug 24, 2017 02:46:28

Horizon User Experience

- VMware Horizon Logon Simulator
  - CHN
    - Desktop_helpdesk
    - Outlook
    - ✓ Editplus
    - ✓ Paint
    - ✓ Windows Media Player
    - ✓ Wordpad

VMware Horizon Logon Simulator - CHN\Desktop_helpdesk

✓	Logon availability (%)	100
✓	Application enumeration availability (%)	100
✓	Application launch availability (%)	100
✓	Logon duration (Seconds)	23.56
✓	Application enumeration duration (Seconds)	0.71
!	Application launch duration (Seconds)	94.87
✓	Logoff duration (Seconds)	0.59
✓	Total simulation duration (Seconds)	119.72

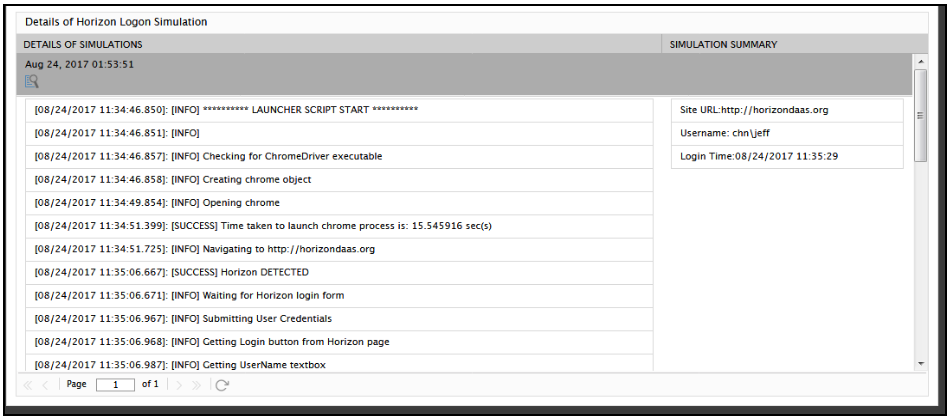
Figure 3.2: The measures reported by the VMware Horizon Logon Simulator test

Measurement	Description	Measurement Unit	Interpretation
Logon availability	Indicates whether/not the simulator logged into the web store successfully, when attempting to launch this application/desktop.	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 application/desktop. You can also use the detailed diagnosis of this measure to view the output of the simulation script, scrutinize it, and isolate the failure and problem points of the VMware Horizon infrastructure at first glance.
Logon duration	Indicates the time taken by the simulator to login to Access Point (VMware Unified Access Gateway) / VMware Horizon Connection Server, when attempting to launch this application/desktop.	Secs	If the *Total simulation duration* for an application/desktop 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 authentication? application enumeration? application launch? or log out?
Application enumeration availability	Indicates whether/not applications/desktops were successfully enumerated on the Access Point (VMware Unified Access Gateway) / VMware Horizon Connection Server console,	Percent	The value 100 for this measure indicates that application/desktop enumeration was successful, and the value 0 indicates that enumeration failed.

Measurement	Description	Measurement Unit	Interpretation
	when the simulator attempted to launch this application/desktop.		
Application enumeration duration	Indicates the time taken for application/desktop enumeration to complete, when the simulator attempted to launch this application/desktop.	Secs	If the *Total simulation duration* for an application/desktop 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 authentication? application enumeration? application launch? or log out?
Application launch availability	Indicates whether/not the simulator launched this application/desktop successfully.	Percent	The value 100 for this measure indicates that application/desktop launch was successful, and the value 0 indicates that the launchn failed. By comparing the value of this measure across applications/desktops, you can quickly identify which application/desktop could not be launched.
Application launch duration	Indicates the time taken by the simulator to launch this application/desktop.	Secs	If the *Total simulation duration* for an application/desktop 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

Measurement	Description	Measurement Unit	Interpretation
			authentication? application enumeration? application launch? or log out?
Logoff duration	Indicates the time taken by the simulator to log out of Access Point (VMware Unified Access Gateway) / VMware Horizon Connection Server.	Secs	If the *Total simulation duration* for an application/desktop 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 authentication? application enumeration? application launch? or log out?
Total simulation duration	Indicates the total time taken by the simulator to simulate the launch of this application / desktop.	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 enumeration? application launch? or log out?

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 VMware Horizon infrastructure at first look. A summary of the simulation is also provided as part of the detailed diagnostics. This includes the Site URL configured for monitoring, the user name used for the simulation, the exact time at which the simulated user logged into the site, and the published resource that was accessed as part of the simulation.



Details of Horizon Logon Simulation

DETAILS OF SIMULATIONS

Aug 24, 2017 01:53:51

```
[08/24/2017 11:34:46.850]: [INFO] ********** LAUNCHER SCRIPT START **********
[08/24/2017 11:34:46.851]: [INFO]
[08/24/2017 11:34:46.857]: [INFO] Checking for ChromeDriver executable
[08/24/2017 11:34:46.858]: [INFO] Creating chrome object
[08/24/2017 11:34:49.854]: [INFO] Opening chrome
[08/24/2017 11:34:51.399]: [SUCCESS] Time taken to launch chrome process is: 15.545916 sec(s)
[08/24/2017 11:34:51.725]: [INFO] Navigating to http://horizondaas.org
[08/24/2017 11:35:06.667]: [SUCCESS] Horizon DETECTED
[08/24/2017 11:35:06.671]: [INFO] Waiting for Horizon login form
[08/24/2017 11:35:06.967]: [INFO] Submitting User Credentials
[08/24/2017 11:35:06.968]: [INFO] Getting Login button from Horizon page
[08/24/2017 11:35:06.987]: [INFO] Getting UserName textbox
```

SIMULATION SUMMARY

Site URL:http://horizondaas.org

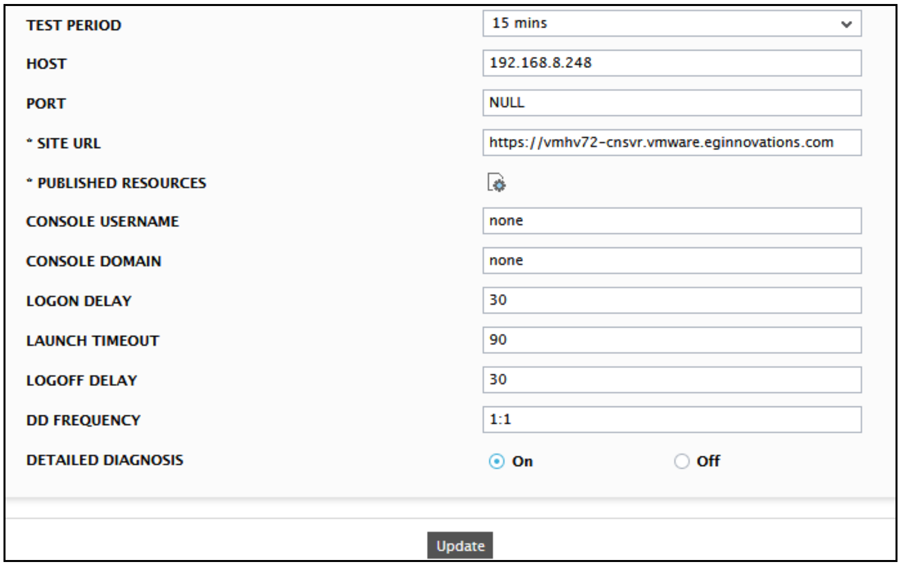
Username: chn\jeff

Login Time:08/24/2017 11:35:29

Figure 3.3: The detailed diagnosis of the Logon availability measure

3.1.1 How to Configure Published Resources for Monitoring?

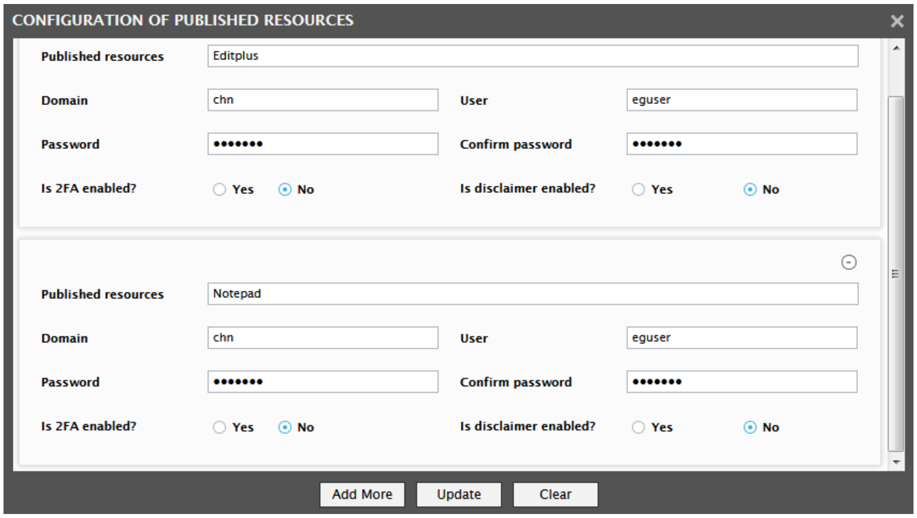
To configure the applications / desktops that the simulator has to launch, click on the icon against **Published Resources** in 3.1.1.



TEST PERIOD	15 mins
HOST	192.168.8.248
PORT	NULL
* SITE URL	https://vmhv72-cnsvr.vmware.eginnovations.com
* PUBLISHED RESOURCES	
CONSOLE USERNAME	none
CONSOLE DOMAIN	none
LOGON DELAY	30
LAUNCH TIMEOUT	90
LOGOFF DELAY	30
DD FREQUENCY	1:1
DETAILED DIAGNOSIS	● On ○ Off

Figure 3.4: The VMware Horizon Logon Simulator Test configuration page

Figure 3.5 will then appear.



CONFIGURATION OF PUBLISHED RESOURCES

Published resources	Editplus		
Domain	chn	User	eguser
Password	•••••••	Confirm password	•••••••
Is 2FA enabled?	○ Yes ● No	Is disclaimer enabled?	○ Yes ● No

Published resources	Notepad		
Domain	chn	User	eguser
Password	•••••••	Confirm password	•••••••
Is 2FA enabled?	○ Yes ● No	Is disclaimer enabled?	○ Yes ● No

Figure 3.5: Configuring the published resources to be launched

Using Figure 3.5, you can easily configure multiple resources that you want the simulator to launch and also the valid user credentials for accessing each resource. For this, follow the steps below:

1. Provide a comma-separated list of **Published resource**s to be launched. The resource can be an application / desktop. When providing application/desktop names, make sure you provide the same name using which the applications/desktops are displayed in the Access Point or VMware Horizon Connection Server web console. Also, make sure that the **User** you specify is authorized to launch all the applications/desktops configured in the comma-separated list of **Published resource**s.

   Typically, any application/desktop that is launched opens in a separate window. Sometimes, a different name may be displayed for the launched application/desktop in that window's title bar. If there is a mismatch between the resource name in the Access Point or the VMware Horizon Connection Server console and the resource name in the launched window title, then the simulator may wrongly report a successful launch as a failure. To avoid this, in such circumstances, your Published resources specification should be of the following format: *<Application / Desktop Name as seen in the Access Point / VMware Horizon Connection Server console>:<Application/Desktop Name as displayed in the Window title>*. For example, your specification can be: *winword-Documn:winword.exe,excel-Dev:excel.exe*

   Note:

   ◦ The resources can be specified either in lower case or upper case or a combination of both.

- The display name of the resources should not contain the following special characters:

  `*+=#.|;\"\'<>\/[]{}()?

2. Then, using the **Domain**, **User**, **Password**, and **Confirm Password** parameters, configure the credentials of the user who is authorized to launch the configured resources.

3. Two-factor authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are. If VMware Horizon Connection Server is enabled with two- factor authentication, then to authenticate the specified **User** login, the VMware Horizon Connection Server will require an additional layer of security other than the **Password** you have provided. This can be any piece of information that only the **User** knows or has immediately in hand - such as a verification code that the VMware Horizon Connection Server provides. This is why, if the VMware Horizon Connection Server is enabled with twofactor authentication, you will have to set the **Is 2FA enabled?** flag to **Yes**, and then specify the verification code in the text box that appears alongside. On the other hand, if the server is not enabled with two-factor authentication, set this flag to **No**.

4. Some high- security VMware Horizon environments may have been configured to display a 'disclaimer', whenever a user attempts to login to a server/desktop in the environment. Such disclaimers typically include statements that delimit the scope of access, uphold confidentiality or protect copyright laws, and mitigate the risk of virus infections or data losses that may be caused by unauthorized access. If such a disclaimer is enabled for your environment, then set the **Is disclaimer enabled?** flag to **Yes**. In this case, the simulator will accept the disclaimer and proceed with the simulation. If no such disclaimer has been configured for your environment, set this flag to **No**.

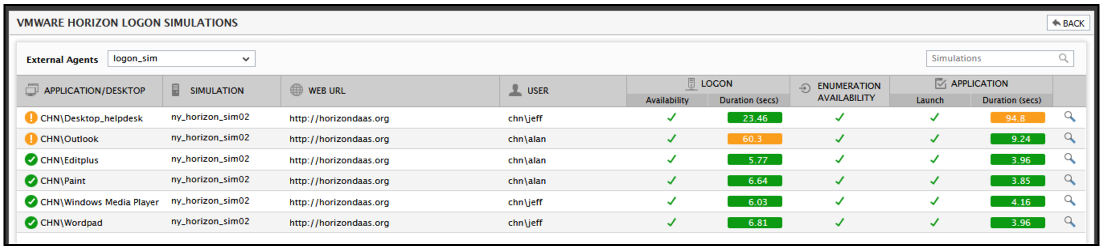
5. If you do not want to configure any more resources for launching, then click the **Update** button in Figure 3.5 to save the changes. To add another resource for launching, click the **Add More** button. This will add an empty record to Figure 3.5. Here, specify the names of more **Published resource**s, and then use the **Domain**, **User**, **Password**, and **Confirm Password** parameters to provide the credentials of a user who is authorized to launch those resources.

6. At any given point in time, you can exclude/delete a resource from the simulation by clicking the ⊖ button corresponding to that resource in Figure 3.5.

7. You can also clear all the configured resources and their launch details at one shot, by clicking the **Clear** button in Figure 3.5.

3.2 Simulator Dashboard

Where two/more VMware Horizon Logon Simulator components are managed, clicking on the *VMware Horizon Logon Simulator* component-type in the **Components At-A-Glance** section of the Monitor dashboard automatically opens the **Simulator Dashboard**.



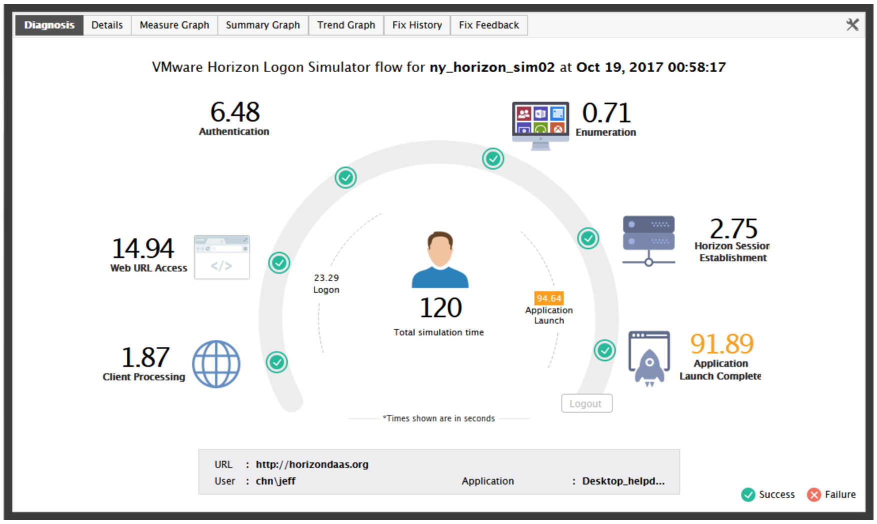
VMWARE HORIZON LOGON SIMULATIONS

External Agents: logon_sim

APPLICATION/DESKTOP	SIMULATION	WEB URL	USER	LOGON		ENUMERATION AVAILABILITY	APPLICATION		
				Availability	Duration (secs)		Launch	Duration (secs)	
! CHN\Desktop_helpdesk	ny_horizon_sim02	http://horizondaas.org	chn\jeff	✓	23.46	✓	✓	94.8	🔍
! CHN\Outlook	ny_horizon_sim02	http://horizondaas.org	chn\alan	✓	60.3	✓	✓	9.24	🔍
✓ CHN\Editplus	ny_horizon_sim02	http://horizondaas.org	chn\alan	✓	5.77	✓	✓	3.96	🔍
✓ CHN\Paint	ny_horizon_sim02	http://horizondaas.org	chn\alan	✓	6.64	✓	✓	3.85	🔍
✓ CHN\Windows Media Player	ny_horizon_sim02	http://horizondaas.org	chn\jeff	✓	6.03	✓	✓	4.16	🔍
✓ CHN\Wordpad	ny_horizon_sim02	http://horizondaas.org	chn\jeff	✓	6.81	✓	✓	3.96	🔍

Figure 3.6: The Simulator Dashboard

By default, the dashboard displays all the simulations performed by all the simulators configured in an environment. For each simulation, the dashboard displays the applications accessed and metrics captured by that simulation. This way, the simulations that failed and the precise failure points - whether login, enumeration, application launch, or logoff - of each simulation can be instantly and accurately isolated. You can even click on the 'magnifying glass' icon corresponding to a simulation for a graphical view of the logon process. Using this graphical representation, administrators can clearly identify which step of the logon process has caused slowness.

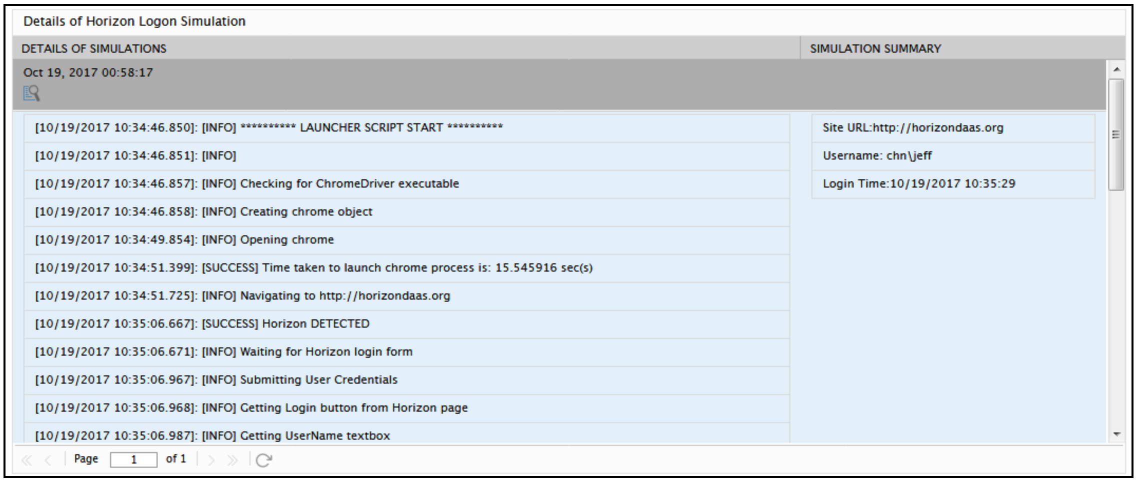


VMware Horizon Logon Simulator flow for **ny_horizon_sim02** at **Oct 19, 2017 00:58:17**

URL : **http://horizondaas.org**
User : **chn\jeff** Application : **Desktop_helpd...**

Figure 3.7: A graphical view of the logon process

You can click on the Details tab page in Figure 3.7 to view the output of the simulation script, scrutinize it, and isolate the failure and problem points of the VMware Horizon infrastructure (see Figure 3.8).



Details of Horizon Logon Simulation

DETAILS OF SIMULATIONS

Oct 19, 2017 00:58:17

```
[10/19/2017 10:34:46.850]: [INFO] ********** LAUNCHER SCRIPT START **********
[10/19/2017 10:34:46.851]: [INFO]
[10/19/2017 10:34:46.857]: [INFO] Checking for ChromeDriver executable
[10/19/2017 10:34:46.858]: [INFO] Creating chrome object
[10/19/2017 10:34:49.854]: [INFO] Opening chrome
[10/19/2017 10:34:51.399]: [SUCCESS] Time taken to launch chrome process is: 15.545916 sec(s)
[10/19/2017 10:34:51.725]: [INFO] Navigating to http://horizondaas.org
[10/19/2017 10:35:06.667]: [SUCCESS] Horizon DETECTED
[10/19/2017 10:35:06.671]: [INFO] Waiting for Horizon login form
[10/19/2017 10:35:06.967]: [INFO] Submitting User Credentials
[10/19/2017 10:35:06.968]: [INFO] Getting Login button from Horizon page
[10/19/2017 10:35:06.987]: [INFO] Getting UserName textbox
```

SIMULATION SUMMARY

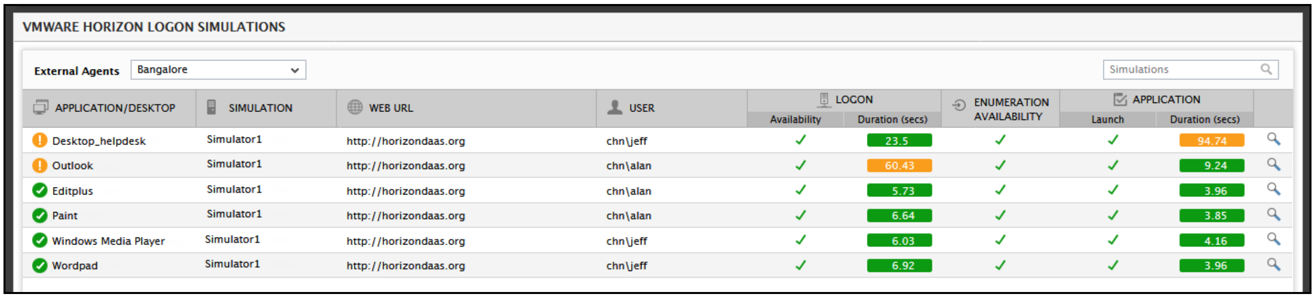
Site URL:http://horizondaas.org

Username: chn\jeff

Login Time:10/19/2017 10:35:29

Figure 3.8: The simulation script highlighting the success and failure points of the simulation

You can even filter the details displayed in the dashboard by picking the simulator for which you want to view the details. This can be achieved by picking a particular external agent from the **External Agents** drop-down.



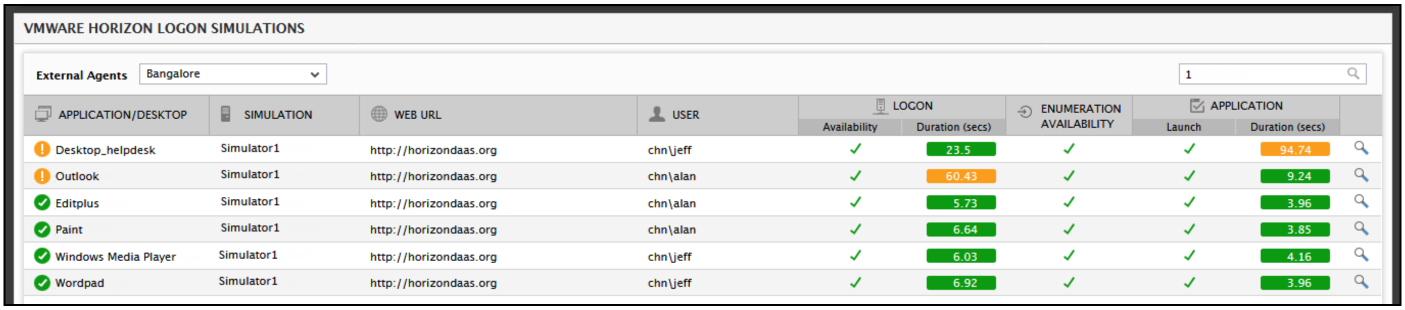
VMWARE HORIZON LOGON SIMULATIONS

External Agents: Bangalore

APPLICATION/DESKTOP	SIMULATION	WEB URL	USER	LOGON		ENUMERATION AVAILABILITY	APPLICATION	
				Availability	Duration (secs)		Launch	Duration (secs)
Desktop_helpdesk	Simulator1	http://horizondaas.org	chn\jeff	✓	23.5	✓	✓	94.74
Outlook	Simulator1	http://horizondaas.org	chn\alan	✓	60.43	✓	✓	9.24
Editplus	Simulator1	http://horizondaas.org	chn\alan	✓	5.73	✓	✓	3.96
Paint	Simulator1	http://horizondaas.org	chn\alan	✓	6.64	✓	✓	3.85
Windows Media Player	Simulator1	http://horizondaas.org	chn\jeff	✓	6.03	✓	✓	4.16
Wordpad	Simulator1	http://horizondaas.org	chn\jeff	✓	6.92	✓	✓	3.96

Figure 3.9: Viewing the details of a particular simulator alone

Alternatively, you can filter the dashboard contents on the basis of the *VMware Horizon Simulator* component that you managed. You can specify the whole/part of the component name in the **Simulations** search text box (see Figure 3.10) and click the 'magnifying glass' icon alongside. This will display the details of only those components with names that contain the specified search string.



VMWARE HORIZON LOGON SIMULATIONS

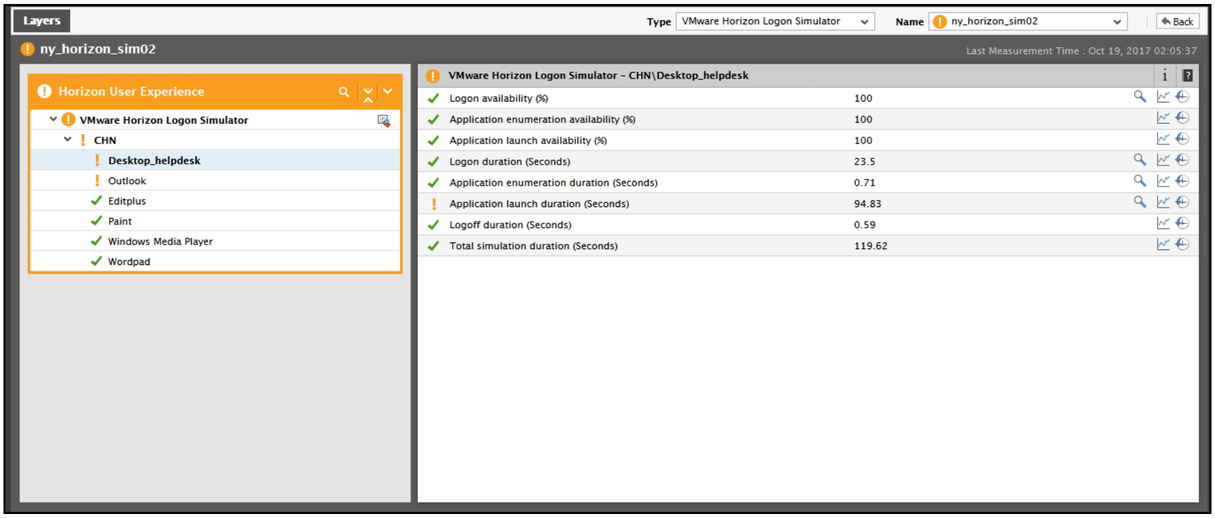
External Agents: Bangalore

Search: 1

APPLICATION/DESKTOP	SIMULATION	WEB URL	USER	LOGON		ENUMERATION AVAILABILITY	APPLICATION		
				Availability	Duration (secs)		Launch	Duration (secs)	
! Desktop_helpdesk	Simulator1	http://horizondaas.org	chn\jeff	✓	23.5	✓	✓	94.74	🔍
! Outlook	Simulator1	http://horizondaas.org	chn\alan	✓	60.43	✓	✓	9.24	🔍
✓ Editplus	Simulator1	http://horizondaas.org	chn\alan	✓	5.73	✓	✓	3.96	🔍
✓ Paint	Simulator1	http://horizondaas.org	chn\alan	✓	6.64	✓	✓	3.85	🔍
✓ Windows Media Player	Simulator1	http://horizondaas.org	chn\jeff	✓	6.03	✓	✓	4.16	🔍
✓ Wordpad	Simulator1	http://horizondaas.org	chn\jeff	✓	6.92	✓	✓	3.96	🔍

Figure 3.10: Viewing the details of only those simulations that were performed using VMware Horizon Logon Simulator components that match the specified search string

Clicking on any simulation in the dashboard will lead you to the **Layers** tab page, where you can view the metrics reported by the simulation and the current state of each metric.



Type: VMware Horizon Logon Simulator   Name: ny_horizon_sim02

ny_horizon_sim02   Last Measurement Time : Oct 19, 2017 02:05:37

Horizon User Experience
- VMware Horizon Logon Simulator
  - CHN
    - ! Desktop_helpdesk
    - ! Outlook
    - ✓ Editplus
    - ✓ Paint
    - ✓ Windows Media Player
    - ✓ Wordpad

VMware Horizon Logon Simulator – CHN\Desktop_helpdesk

	Measure	Value
✓	Logon availability (%)	100
✓	Application enumeration availability (%)	100
✓	Application launch availability (%)	100
✓	Logon duration (Seconds)	23.5
✓	Application enumeration duration (Seconds)	0.71
!	Application launch duration (Seconds)	94.83
✓	Logoff duration (Seconds)	0.59
✓	Total simulation duration (Seconds)	119.62

Figure 3.11: The layer model of the VMware Horizon Logon Simulator component that was clicked on

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*.

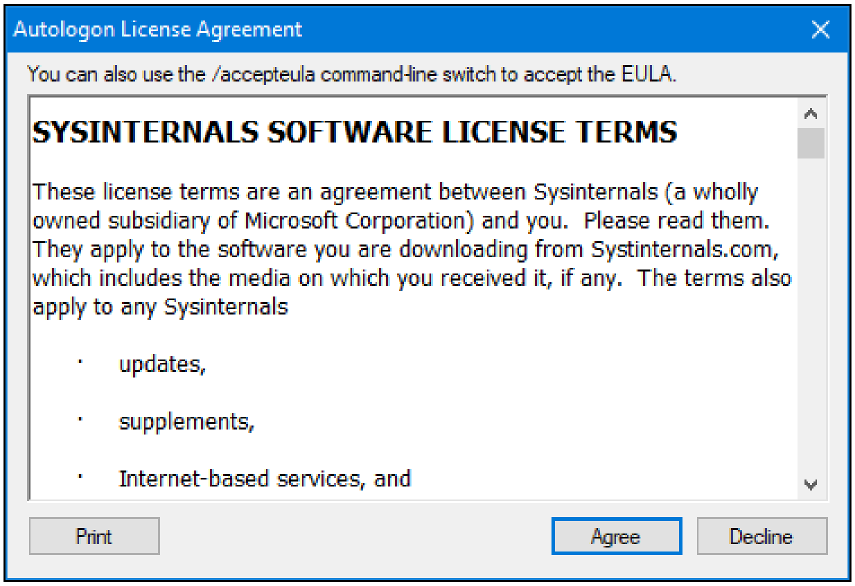
4.1 Fine-tuning the simulation using Autologon.exe

If you wish to automate the user logon using 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.



Autologon License Agreement

You can also use the /accepteula command-line switch to accept the EULA.

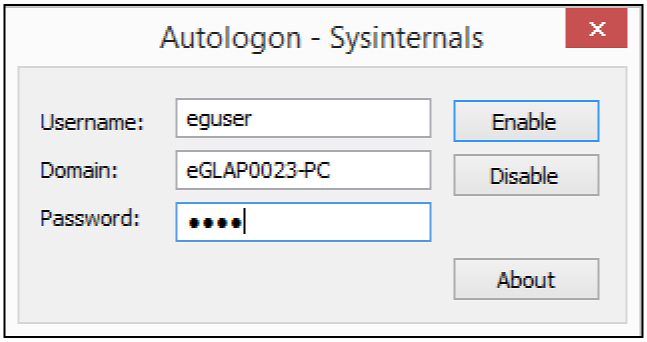
SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services, and

Figure 4.1: Agreeing to the Software License Terms

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



Autologon - Sysinternals

Username: eguser

Domain: eGLAP0023-PC

Password: ••••

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

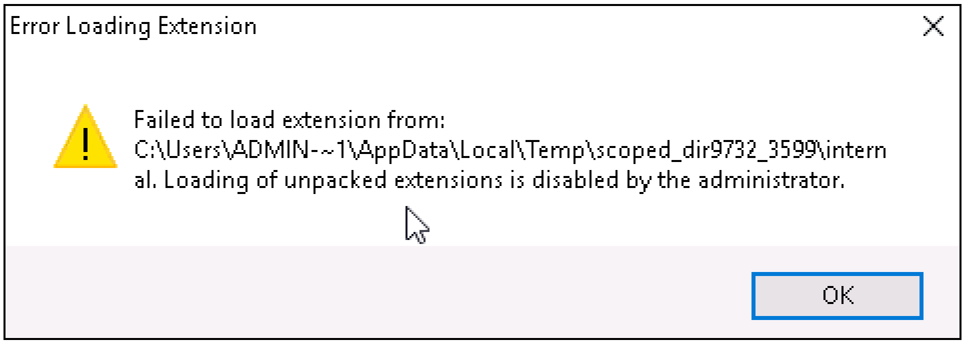
3. In this registry entry, add the following REG_SZ string values:

   - **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.

4.3 Browser launch hindered due to disabled chrome extensions

In highly secure environments, administrators may not want to load the chrome extensions on the Chrome browser for all users. In such cases, a group policy may be applied to disable these chrome extensions from loading on the Chrome browser. If simulation happens in such environments, the Chrome browser may not be launched and an error message as shown in Figure 4.3 appears.



Error Loading Extension

Failed to load extension from:
C:\Users\ADMIN-~1\AppData\Local\Temp\scoped_dir9732_3599\intern
al. Loading of unpacked extensions is disabled by the administrator.

Figure 4.3: Error message that appears when chrome extensions failed to load

For the VMWare Horizon Logon Simulator to launch the Chrome browser by overriding the group policy settings that disabled the extensions, do the following:

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

   HKLM\Software\Policies\Google\Chrome\ExtensionInstallBlacklist

   In this registry entry, delete all keys and values.
3. Locate the following registry entry:

   HKCU\Software\Policies\Google\Chrome\ExtensionInstallBlacklist

   In this registry entry, delete all keys and values.
4. Finally, restart the eG agent.

Ensure that the group policy is disabled on the simulation endpoint so that the Chrome browser can be launched by the VMware Horizon Logon Simulator at periodic intervals.

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.