The eG Enterprise Logon Simulator for Citrix

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

For years, slow Citrix logons have been the most common complaint in Citrix infrastructures. For a Citrix user, slow logons can lead to frustration, lower productivity and efficiency. For a Citrix administrator, Citrix logon slowness is a complex problem that takes a long time to resolve. There are dozens of steps involved in the Citrix logon process and they involve multiple components – Citrix StoreFront, Citrix Delivery Controller, Active Directory, Profile server, Citrix XenApp/XenDesktop, the Citrix data store and so on. Identifying exactly what is causing the slowdown is often time consuming and laborious.

To ensure great Citrix 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 Citrix 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 a difficult to get a consistent assessment of Citrix 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 Citrix farm, and at those times, it is important to know if Citrix 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 Citrix infrastructures. Using an agentless approach, the eG Citrix Logon Simulator simulates a user logging in to a Citrix StoreFront or NetScaler gateway through a browser, reviewing the list of applications/desktops accessible, clicking on a selected application or desktop, launching it in Citrix Receiver by initiating a session and then logging off. By emulating the exact same process that users go through when they logon to Citrix XenApp or XenDesktop, the eG Citrix Logon Simulator provides a realistic measure of the user experience during Citrix logon. Since every simulation tests the entire Citrix delivery infrastructure (Citrix NetScaler, Citrix StoreFront, Citrix Delivery Controller, Citrix XenApp Server, VDI, etc.), the results represent the cumulative health of all of the tiers supporting Citrix logons.

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

1.1 Pre-requisites for Using eG Enterprise Logon Simulator for Citrix

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

Category	Pre-requisites
Logon Simulator Agent / Simulation Endpoint	• Client Session Simulation 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 on 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 should not be used to monitor any other component in the target environment. • Chrome browser v81x (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 non-start of simulation. Therefore, ensure that the Chrome drivers are also updated whenever the browser is updated to the latest version. • Microsoft .Net 3.5 (or above) should pre-exist on the system hosting the

	logon simulator agent/external agent. • Citrix Receiver version 2.x (also referred to as v12.x) or above should be installed on the system hosting the Logon Simulator Agent. Take care to install the Receiver in the default location only. **Note:** • Ensure that you install the Standard or full version of the Citrix Receiver. Citrix Receiver installed as a plugin is not supported. • Download the latest version of Receiver here: *https://www.citrix.com/go/receiver.html* • 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 / Citrix Receiver. This user should be logged in at all times for the simulator to run continuously. Also, make sure that this session window is **not minimized** because this may cause problems in the logon simulation. **Note:** • The logon simulation will not work if the session is closed. • The logon simulation will not work if the screen is locked on the logon simulation endpoint. • The logon simulator will not work if the screensaver appears on the logon simulation endpoint. • No other ICA session should be connected/running on the simulation endpoint before running the script. Any Receiver processes will be killed, so existing sessions will be disconnected. • If the Citrix Receiver has created a system tray icon on the simulation endpoint, then make sure it is removed.
Citrix XenApp / XenDesktop	• The simulator will only work with Citrix XenApp / XenDesktop 6.x and 7.x environments. • A dedicated Citrix test account is required on Citrix XenApp / Citrix XenDesktop with rights to launch applications/desktops.
Citrix StoreFront / NetScaler	• For Citrix XenApp / XenDesktop 7.x environments, make sure that StoreFront 2.0 or higher or NetScaler Gateway version 9.3 or higher is

	available in your environment. • If a firewall separates the simulation endpoint from StoreFront / NetScaler, then make sure you configure the firewall to allow two-way communication between the endpoint and StoreFront / NetScaler. • When using Citrix XenApp / XenDesktop 7, the desktop or application that the simulator should launch should be included as "Favorites" in the StoreFront or NetScaler web console. When using Citrix XenApp6.x on the other hand, the desktop/application that the simulator should launch should be displayed in the **Main** page of the Citrix Web Interface Management console. • Additionally, for launching desktops published on Citrix XenApp / XenDesktop v6.x or v7.x, set the **autoLaunchDesktop** flag to **false** in the **web.config** file under C:\inetpub\wwwroot\Citrix\<storename>Web folder on the StoreFront server.

Note:

To ensure that all the pre-requisites of the Citrix Logon Simulator is fulfilled, you can execute the **ICALogonSimulatorChecks.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).

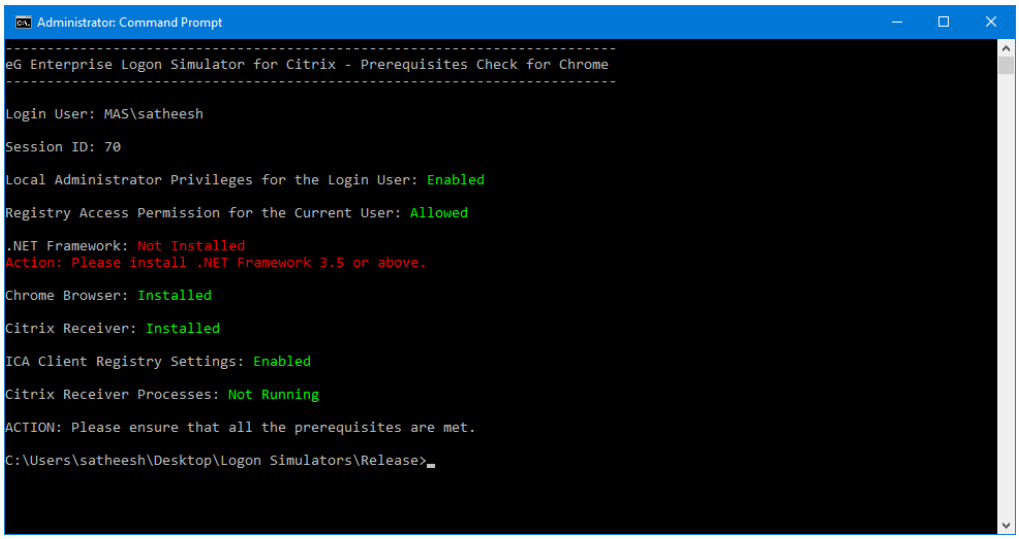

Figure 1.1: Setup script where a pre-requisite has failed

Use the pointers provided in Figure 1.1, just below the failed pre-requisite, to know how to fulfill that requirement. Then, rerun the **ICALogonSimulatorChecks.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.

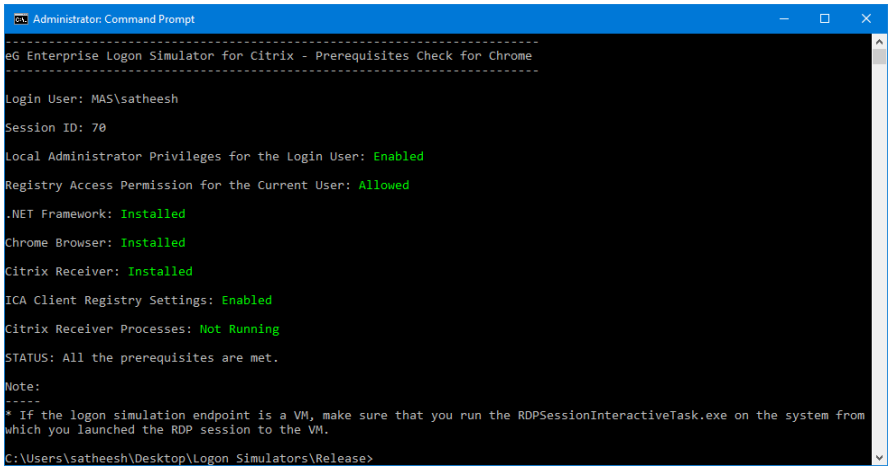

Figure 1.2: All pre-requisites are fulfilled

Caveats:

- Sometimes, the eG agent may not be able to simulate the login session. This may be because of the non interaction of the simulator with the ICA client objects.

  For the simulator to interact with the ICA object and perform the simulation, the following registry entries are needed on the simulator endpoint's registry with DWORD type and value 1.

  - "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\CCM, AllowLiveMonitoring"
  - "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\CCM, AllowSimulationAPI"

- The eG Enterprise Logon Simulator for Citrix can be used to simulate logons to both on-premise Citrix installations and those on the Citrix Cloud or Citrix Workspace. 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. Because of this, the next time the simulator attempts to create a session, it will automatically reconnect to the old session and perform the logon. Metrics reported by the simulator during such sessions may not be representative of the true logon experience. To report a reliable set of metrics each time, the simulator should perform clean application/desktop session logoffs every time.

For simulations that are performed on-premise, you should deploy the light-weight **eG Logoff Helper** software to enable proper application/desktop logoffs. Install the helper software on Citrix ZDC, if a Citrix XenApp Server v6.5 is monitored, or a Citrix Delivery Controller, if Citrix XenDesktop v7.x is monitored. Refer to Section **1.2** topic to know how to install the helper. For simulations performed on the Citrix Workspace or on the Citrix Cloud, the eG Logoff Helper cannot be used for logging off application/desktop sessions. In this case instead, make sure that the **USE ICA** flag of the Citrix Logon Simulator test is set to **Yes**. This setting ensures that session logoffs are performed by the eG agent on the simulation endpoint.

- Sometimes, the user login session may get disconnected. This would primarily happen if the simulation endpoint is rebooted due to automatic updates, scheduled reboots, power failure etc. Every time a session disconnect occurs, 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 ensure that the user is logged in at all times, for the purpose of the simulation, you can automate a user login at the time of a reboot. Refer to the Section **Chapter 4** topic to know how to automate the user logins during reboots.
- **In our environment, logon simulation is performed via RDP sessions. Your pre-requisites specifies that the session window should not be minimized. How should we ensure that the simulation is not impacted if the RDP session is minimized?**

  If the logon simulation is performed via an RDP session, then, you can make sure that the simulation is not impacted even if the RDP session window is minimized. For this, execute the **RDPSessionInteractiveTask.exe** on the system from which the user has launched the RDP session. This executable is available in the **<eG_INSTALL_DIR>\lib** folder. Once you download and extract the package into any location, you will find the RDPSessionInteractiveTask.exe within.

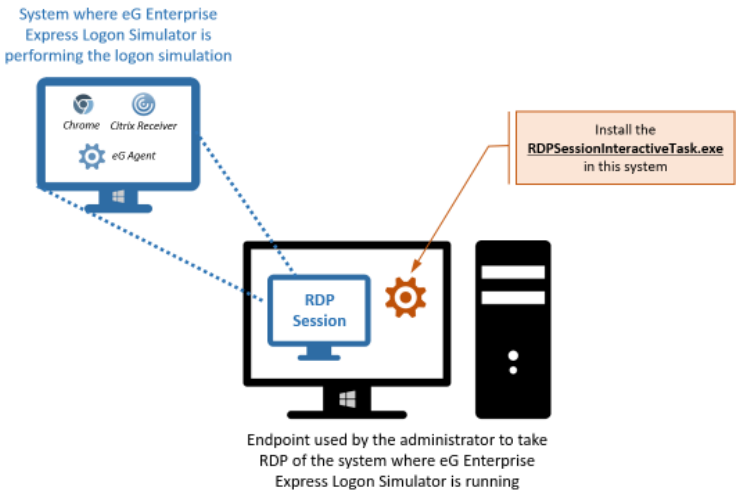

Figure 1.3: Logon Simulation performed via an RDP session

To execute the **RDPSessionInteractiveTask.exe**, do the following:

- Open the command prompt of the system from which the RDP session was launched as an administrator.
- Execute the RPSessionInteractiveTask.exe file. Upon successful execution, a message to that effect will appear.
- Reconnect the RDP session.

- **How do I remove the system tray icon created by the Citrix Receiver?**

  To remove the system tray icon, follow the steps below:

  - Open the Windows Registry Editor on the simulation endpoint.
  - Navigate to the following registry key:

    HKEY_CURRENT_USER\Software\Citrix\Receiver
  - Here, create a new registry entry called **ShowIcon** of type **REG_DWORD**, and set its value to **0**.

1.1.1 Troubleshooting

The logon simulation was being captured well up until a new Chrome browser update. What should I do in my environment to resume logon simulation monitoring using the latest Chrome browser?

Chrome is capable of automatically applying updates and upgrading itself to higher versions. Sometimes, when Chrome auto-upgrades, some drivers that the eG Logon Simulation Agent uses

may suddenly be rendered incompatible with Chrome. This can cause problems in simulation. To avoid this, the Citrix Logon Simulator, 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 The eG Logoff Helper

The eG Enterprise Logon Simulator for Citrix can be used to simulate logons to both on-premise Citrix installations and those on the Citrix Cloud or Citrix Workspace. The simulator simulates a user logging into a Citrix StoreFront or NetScaler gateway through a browser, reviewing the list of applications/desktops accessible, clicking on a selected application or desktop, launching it in Citrix Receiver 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 Citrix 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 Citrix ZDC, if a Citrix XenApp Server v6.5 is monitored, or a Citrix Delivery Controller, if Citrix XenDesktop v7.x is monitored.

In simulations performed on the Citrix Workspace or on the Citrix Cloud on the other hand, you have no control over the monitored Citrix infrastructure. This is why, the eG Logoff Helper cannot be used for logging off application/desktop sessions . In this case instead, make sure that the **USE ICA** flag of the Citrix Logon Simulator test is set to **Yes**. This setting ensures that session logoffs occur using the eG agent on the simulation endpoint.

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

1. Run the **eGLogoffHelper.exe** as an *Administrator* (see Figure 1.4).

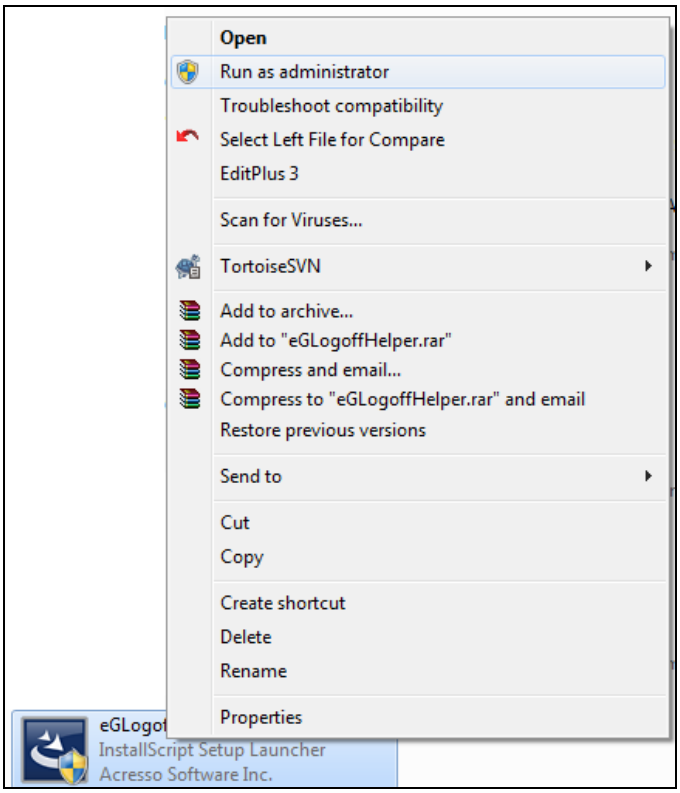

Figure 1.4: Running the eGLogoffHelper.exe as an Administrator

2. Figure 1.5 will then appear. By default, the logoff helper will installed in the C drive. You can change the location of the helper by specify a different install location. For making this change, use the **Browse** button in Figure 1.5. Then, click the **Next** button in Figure 1.5 to proceed.

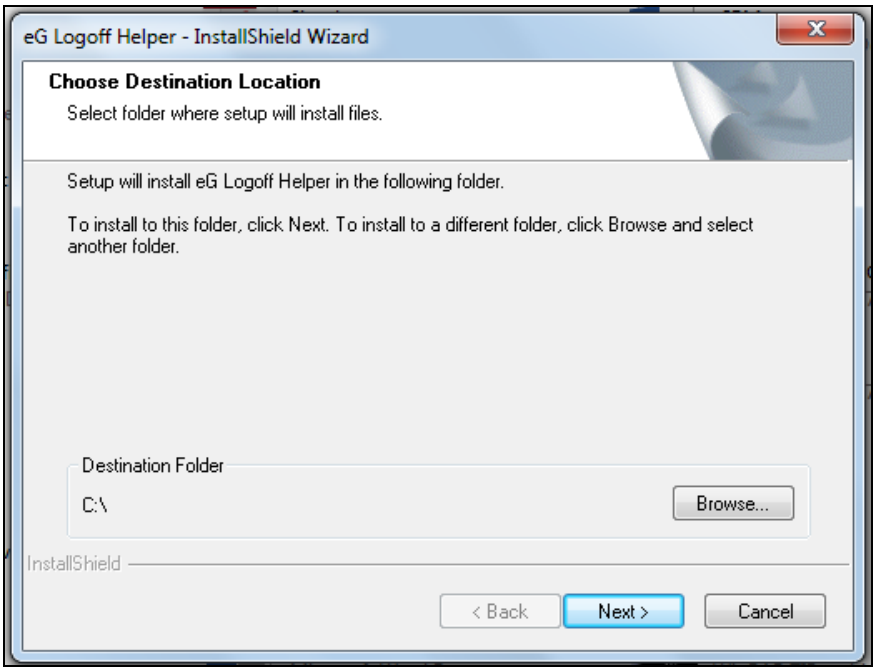

Figure 1.5: Specifying where the logoff helper is to be installed

3. When Figure 1.6 appears, select **Citrix** as the infrastructure and click **Next** to move on.

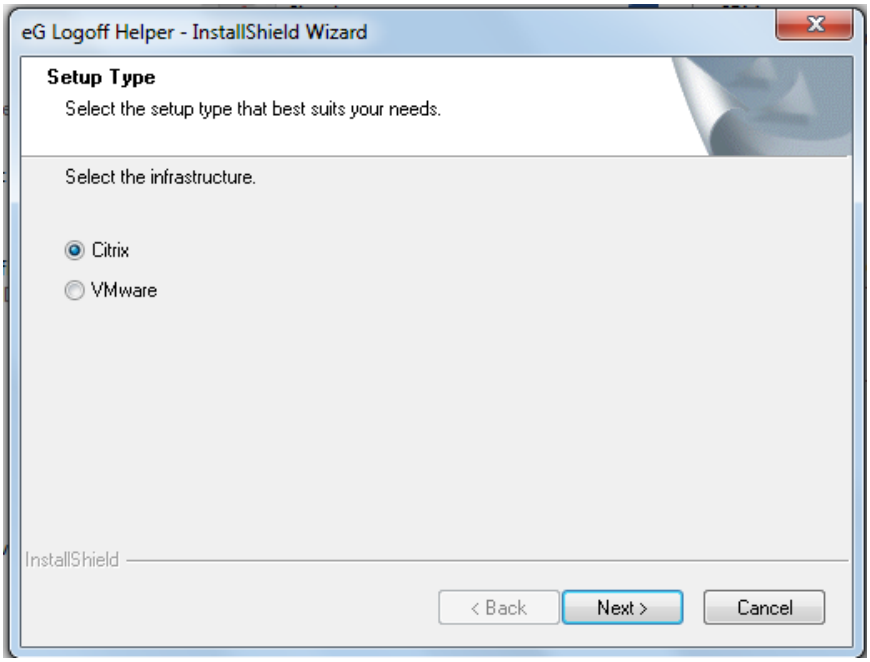

Figure 1.6: Selecting Citrix as the infrastructure

4. In Figure 1.7 that appears next, provide the Citrix Farm/Site administrator's credentials. This is essential for creating and running the eG Logoff Helper Windows service on Citrix ZDC or Citrix Delivery

Controller (as the case may be). **Note that the User Name of the Citrix Farm/Site administrator should be provided in the format, <DomainName>\<UserName>**.

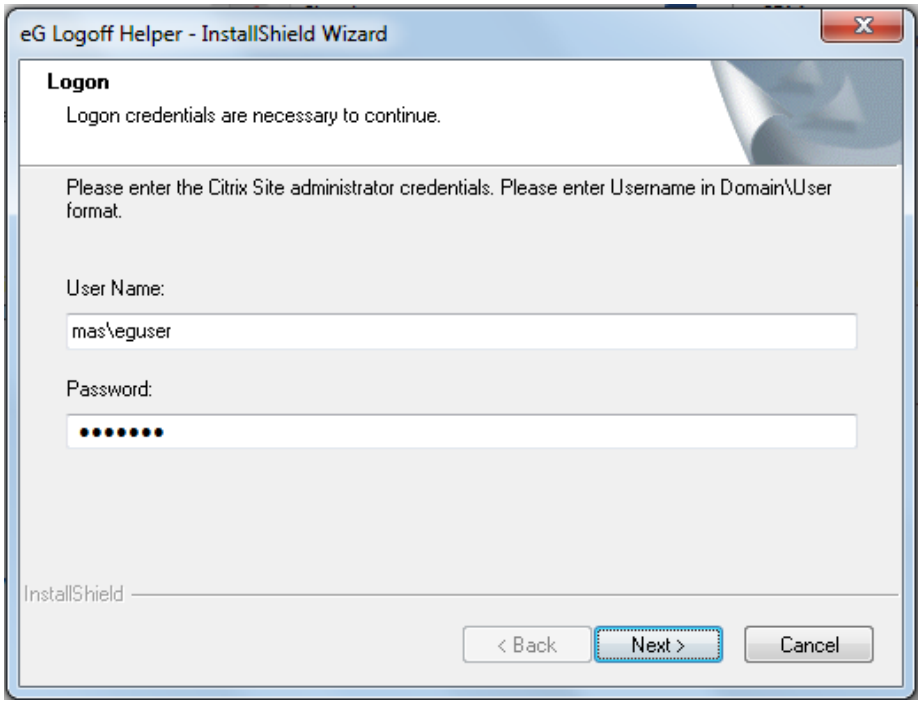

Figure 1.7: Providing the credentials of a Citrix Farm/Site administrator

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.

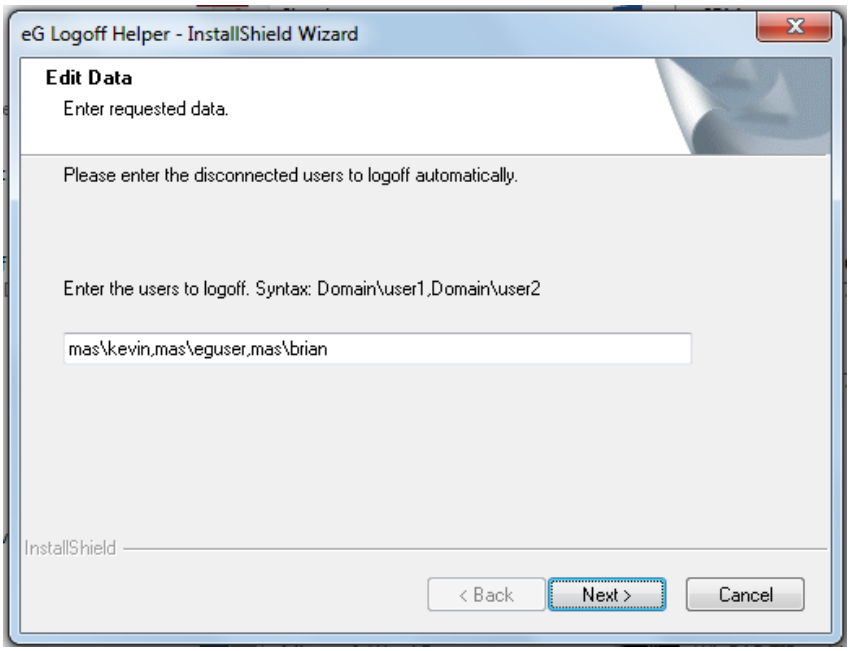

Figure 1.8: Providing a comma-separated list of application/desktop users to logoff

6. Upon successful installation of the helper, a message depicted by Figure 1.9 will appear.

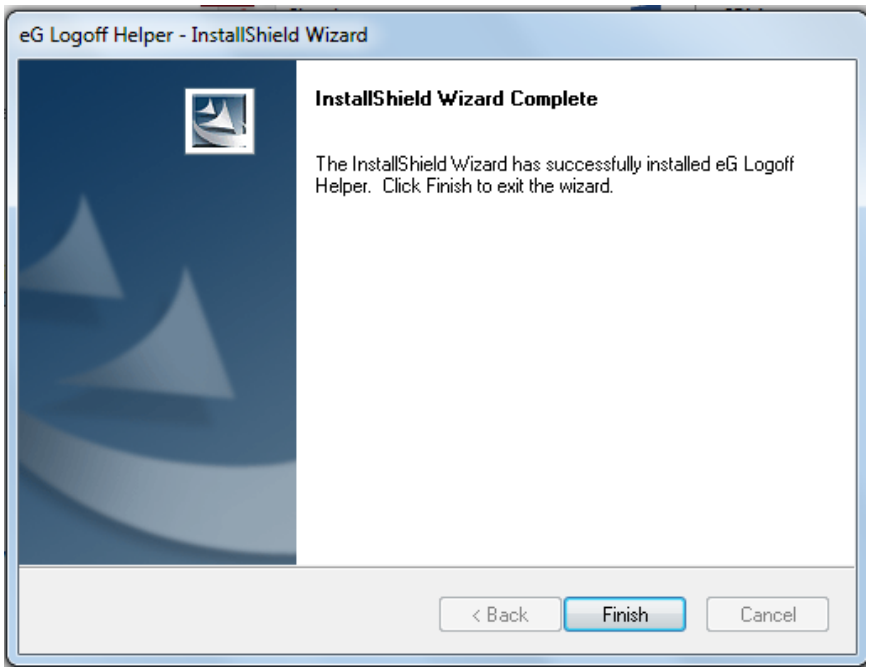

Figure 1.9: Successful installation of the logoff helper

7. Click the **Finish** button in Figure 1.9 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 Citrix farm/site administrator privileges.

1.3 How does the Citrix Logon Simulator Work?

As stated earlier, a dedicated eG external agent drives the logon simulation. This agent periodically runs a **Citrix Logon Simulator** test that emulates the entire process of a user logging into a Citrix 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 StoreFront/NetScaler that it needs to access
- The credentials using which it needs to log into the farm;
- The applications and/or desktops that it needs to launch
- The user account with local administrator rights on the simulation endpoint - i.e., on the system hosting the external agent / Citrix Receiver
- The frequency of the simulation

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 1.10 below.

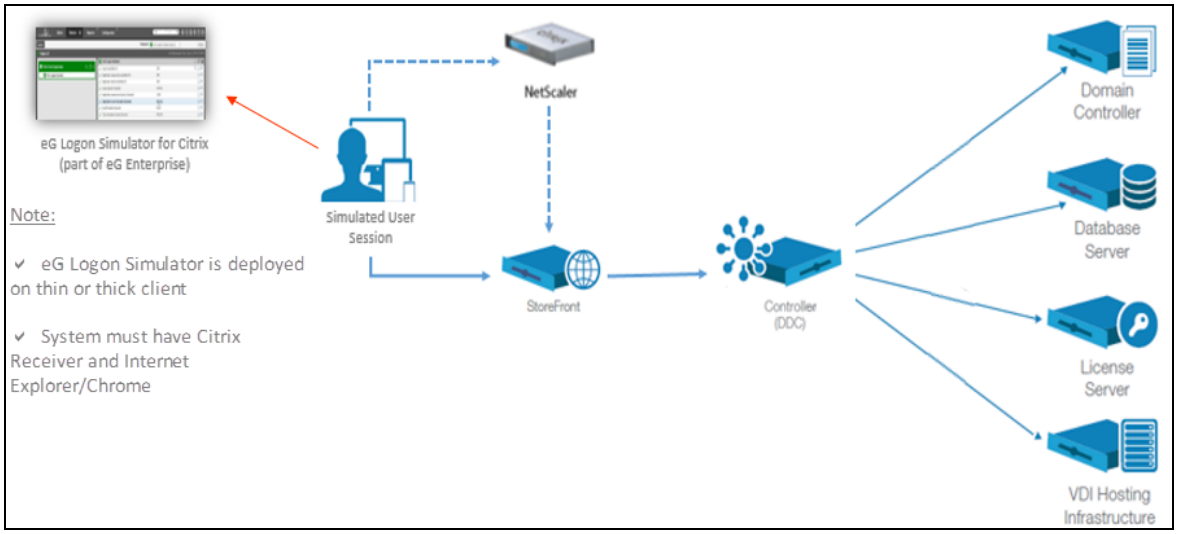

Figure 1.10: How the Citrix Logon Simulator Works

The process depicted by Figure 1.10 is described below:

1. The simulator first opens Chrome and connects to the configured StoreFront/NetScaler 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 lauch was successful.
5. Finally, the simulator closes the application and logs out of the Citrix 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 **Citrix Logon Simulator** component and presents them in the eG monitoring console for analysis. Refer to the **Analyzing the Simulation Results** topic for a detailed discussion on the **Citrix Logon Simulator** model.

Chapter 2: Configuring the Citrix 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).

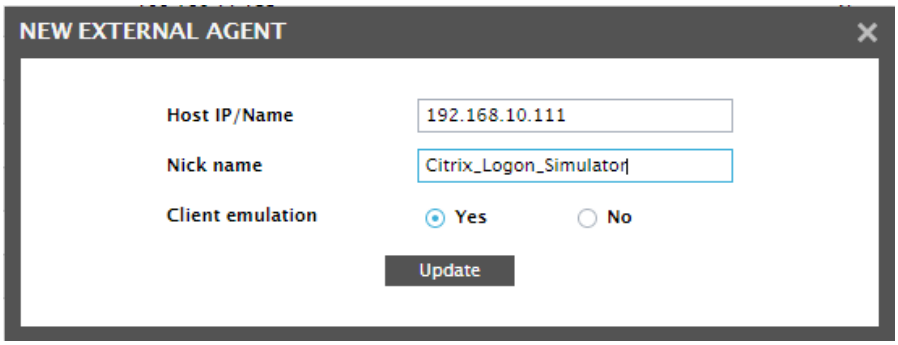

Figure 2.1: Adding a dedicated external agent for the simulation

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

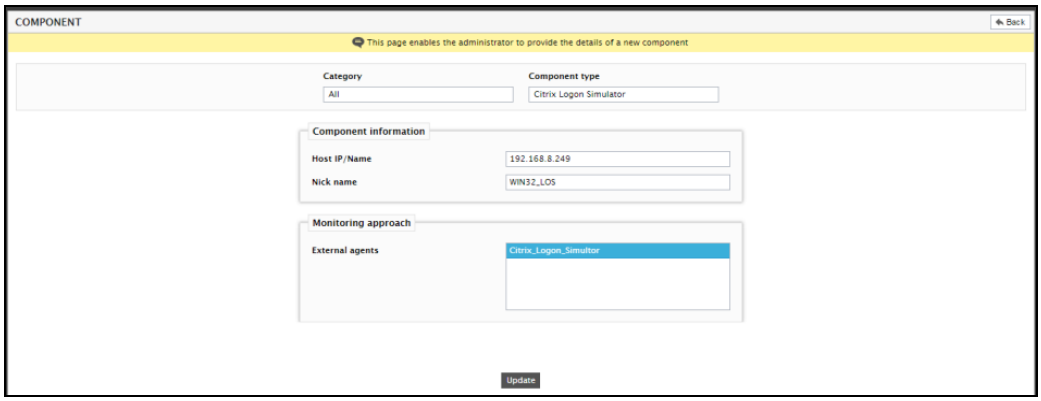

Figure 2.2: Adding a Citrix Logon Simulator

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 **Citrix Logon Simulator** test for this component. Click on the test to configure it.
8. Figure 2.3 will then appear.

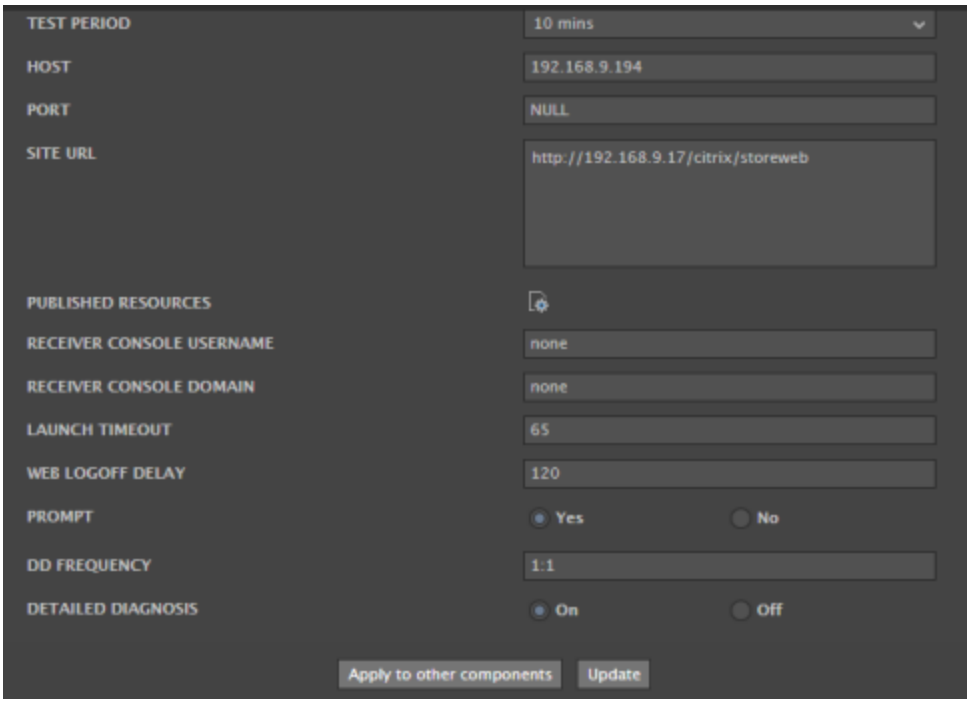

Figure 2.3: Configuring the Citrix Logon Simulator test

9. To know how to configure the test, refer to Section **3.1** .
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 Citrix Logon Simulator test - sends the availability and duration measures it collects to the eG manager. Using a specialized **Citrix Logon Simulator** monitoring model, the eG manager captures these metrics and publishes them in the eG monitoring console for analysis.

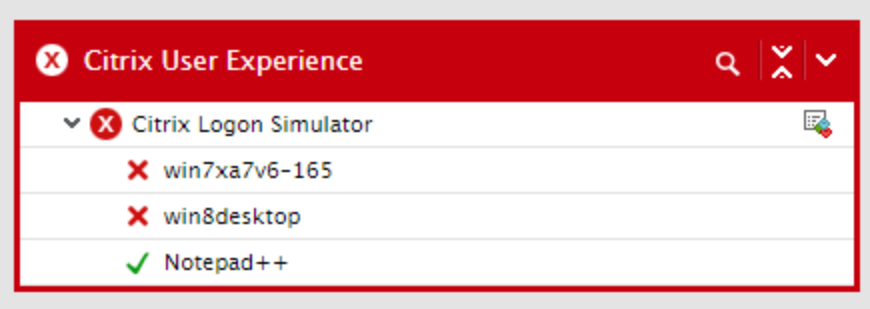

Figure 3.1: The layer model of a Citrix Logon Simulator component

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

3.1 The Citrix Logon Simulator Test

This test emulates a user logging into a Citrix 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, Citrix 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, Citrix administrators are enabled to isolate the probable pain-points of their Citrix delivery infrastructure, even before users begin to actively use applications/desktops.

Target of the test : Citrix XenApp / XenDesktop 6.x or 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 **WEB 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.
   - If the **PROMPT** flag of the test is set to **Yes**: If this is done, then the simulator will be forced to respond to each message prompt that appears during its interaction with the application. This in turn will increase 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 Citrix server
4. **SITE URL** - Specify the URL for connecting to StoreFront / NetScaler. You can provide an HTTP or an HTTPS URL here. Before specifying the URL, ensure the following:

   - Only StoreFront 2.0 (or above) and NetScaler Gateway v9.3 (or above) is supported.

5. **PUBLISHED RESOURCES -** To know how to configure the resources to be monitored, refer to the Section **3.1.1** topic.
6. **RECEIVER 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 Citrix Receiver 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. **WEB 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 5 seconds have elapsed, 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.

9. **PROMPT** - By default, this flag is set to **No**. This means that, by default, the simulator suppresses all message prompts that may appear during the simulation. If for some reason, you want the simulator to view and handle these message prompts, then set this flag to **Yes**.

10. **USE ICA** - By default, this flag is set to **Yes**, indicating that the eG agent itself automatically logs off the simulated sessions. Sometimes however, the eG agent may not be able to perform clean session logoffs. When this happens, simulated 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 Citrix infrastructure, you can avoid such disconnected sessions and ensure clean application/desktop logoffs by deploying the light-weight **eG Logoff Helper** software . To know how to install the software, refer to Section **1.2** topic. Once the helper is

installed, set the **USE ICA** flag to **No**, so that the logoff helper is automatically used for performing session logoffs.

Note:

If the simulation is to performed on the Citrix Cloud or the Citrix Workspace, where you have no control over the Citrix infrastructure, make sure that the **USE ICA** flag is set to **Yes** only.

11. **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.
12. **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

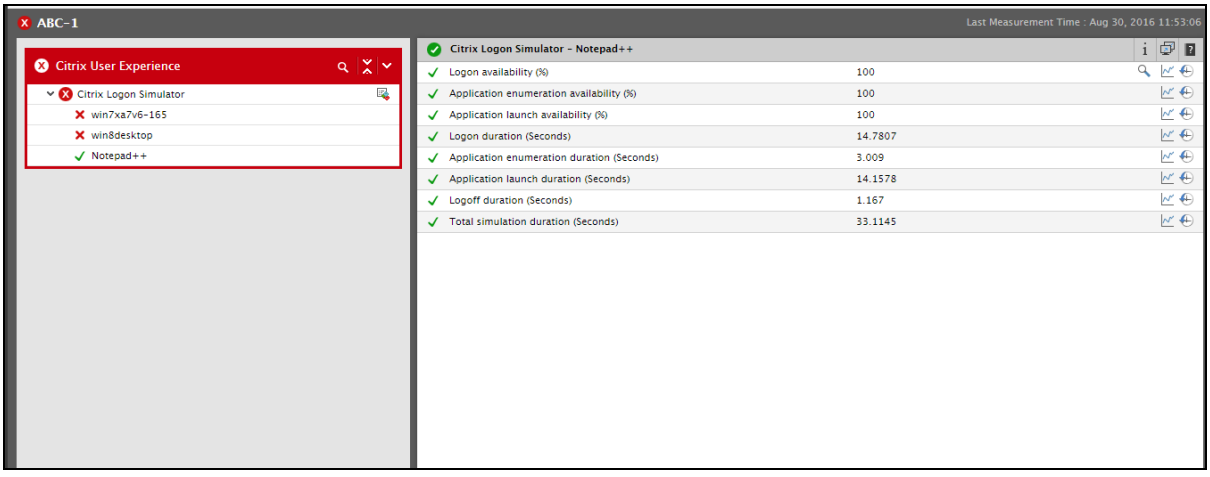

Figure 3.2: The measures reported by the Citrix Logon Simulator test

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 Citrix delivery infrastructure at first glance.
Logon duration	Indicates the time taken by the simulator to login to StoreFront/NetScaler, 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/desktop enumeration availability	Indicates whether/not applications/desktops were successfully enumerated on the StoreFront / NetScaler console, when the simulator attempted to launch this application/desktop.	Percent	The value 100 for this measure indicates that application/desktop enumeration was successful, and the value 0 indicates that enumeration failed.
Application/desktop enumeration duration	Indicates the time taken for application/desktop enumeration to complete, when the simulator attempted to launch this	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

Measurement	Description	Measurement Unit	Interpretation
	application/desktop.		to know where the bottleneck lies - in login authentication? application enumeration? application launch? or log out?
Application/desktop 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/desktop 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 authentication? application enumeration? application launch? or log out?
Logoff duration	Indicates the time taken by the simulator to log out of StoreFront / NetScaler.	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

Measurement	Description	Measurement Unit	Interpretation
			reported by the test to know where the bottleneck lies - in login authentication? application enumeration? application launch? or log out?
Screen refresh latency - avg	Indicates the average time interval measured at the client between the first step (user action) and the last step (graphical response displayed) of this application /desktop's interactions with the endpoint.	Seconds	This is a measurement of the screen lag that is experienced during simulation. In other words, is the latency detected from when the simulator hits a key until the response is displayed. Comparing the value of this measure across simulations will enable administrators to quickly and accurately identify the simulations that are experiencing higher latency.
Data received	Indicates the amount of data received by the simulator to simulate the launch of this application / desktop.	KB	Comparing the value of these measures across simulations will enable administrators to identify the simulation tha had sent/received the maximum amount of data.
Data sent	Indicates the amount of data sent from the simulator to simulate the launch of this application / desktop.	KB	
Frames received	Indicates the number of frames received by the simulator to simulate the launch of this application / desktop.	Number	Comparing the value of these measures across simulations will reveal the simulation that had sent/received the maximum number of frames.
Frames sent	Indicates the number of frames sent from the simulator to simulate the launch of this application / desktop.	Number	

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 Citrix delivery 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.

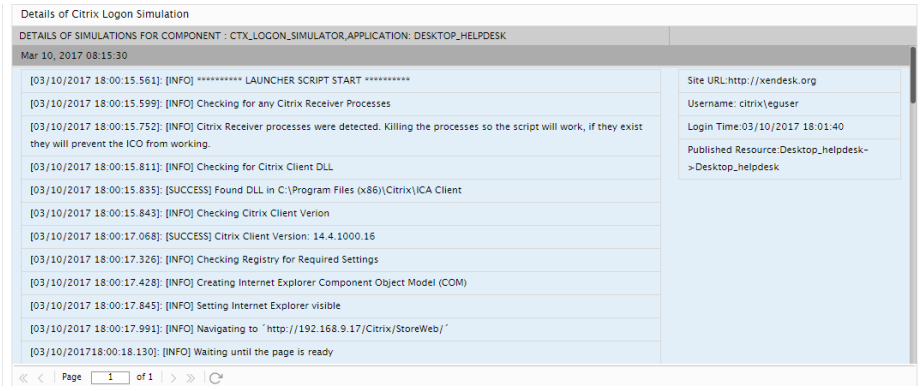

Figure 3.3: The detailed diagnosis of the Logon availability measure

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 Figure 3.4.

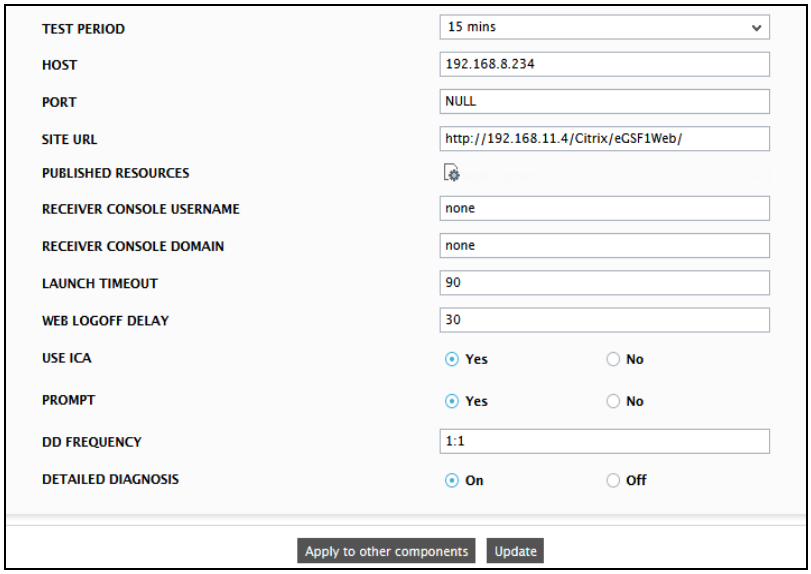

Figure 3.4: The Citrix Logon Simulator Test configuration page

In Figure 3.5 that appears provide a comma-separated list of **Published resources** 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 StoreFront or NetScaler 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. To providea comma-separate list of click on the icon against **Published Resources** in Figure 3.5.

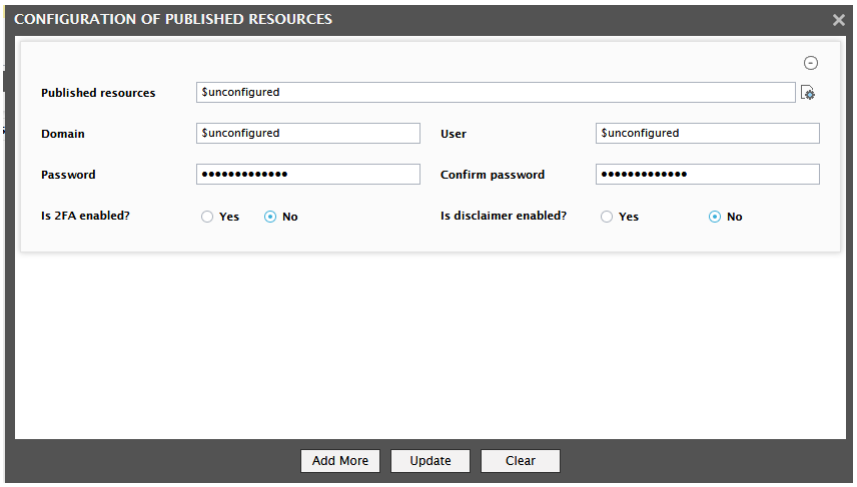

Figure 3.5: Configuration of published resources

Figure 3.5 then appears.

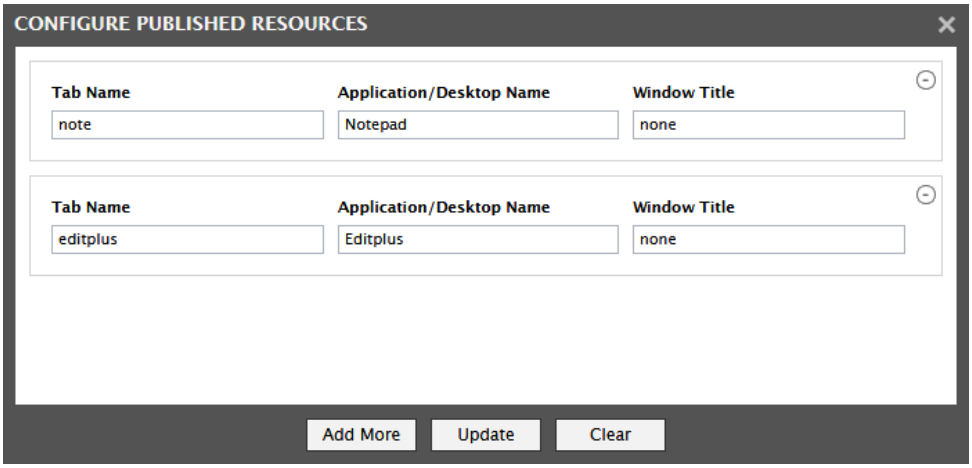

Figure 3.6: Configuring the published resources to be launched

Specify the following in Figure 3.5:

- **Tab Name:** If the simulator is simulating accesses to Citrix XenApp/XenDesktop 7.x, and StoreFront v2.x (or below) is used for the simulation, then the main page of the console will contain two tab pages - Apps and Desktops. The application/desktop that the simulator should launch may be in any of these tab pages. If the application/desktop to be launched is in the tab page that is set as the default landing page, then set the **Tab Name** to *none*. On the other hand, if the application/desktop to be launched is not in the default landing page, then you much specify the exact **Tab Name** of the tab page in which that application/desktop is present.

  Note:

  The **Tab Name** is not case-sensitive.

- **Application/Desktop Name:** Specify the exact name of the Application/Desktop to be launched. When providing the application/desktop name, make sure you provide the same name using which that application/desktop is displayed in the StoreFront or NetScaler web console.

  Note:

  The **Application/Desktop Name** is not case-sensitive.

  Before configuring the names of resources published on Citrix XenApp / XenDesktop 7.x, ensure the following:

  - The desktop or application configured here should be included as "Favorites" in the StoreFront or NetScaler web console.
  - You can auto subscribe users to applications by setting "KEYWORDS:Auto" in the published application's description in the Citrix XenDesktop Broker.
  - Additionally, for launching published desktops, set the **autoLaunchDesktop** flag to **false** in the **web.config** file under C:\inetpub\wwwroot\Citrix\<storename>Web folder on the StoreFront server. You can auto subscribe users to applications by setting "KEYWORDS:Auto" in the published application's description in the Citrix XenDesktop Broker.

  Before configuring the names of resources published on Citrix XenApp / XenDesktop 6.x, make sure that these applications/desktops are available in the **Main** page of the Citrix Web Interface Management console.

- **Window Title:** 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 name in the StoreFront/NetScaler console and the name in the launched window title, then the simulator may wrongly report a successful launch as a failure. To avoid this, where the application/desktop name in the StoreFront/NetScaler console is different from the application/desktop name displayed in the launch window title, use the **Window Title** text box to specify the name thatis displayed for the

configured **Application/Desktop** in the session window's title bar.

Note:

You can specifyeither the partial or exact name that is displayed for the configured Application/Desktop in the session window's title bar.

Finally, click the **Add More** button in Figure 3.5 to add more applications/desktops to be launched. If you do not want to add any more applications/desktops, click the **Update** button in Figure 3.5 to save the changes and exit the **CONFIGURE PUBLISHED RESOURCES** window. You will then return to Figure 3.7, where you can proceed to provide the other details required for the simulation.

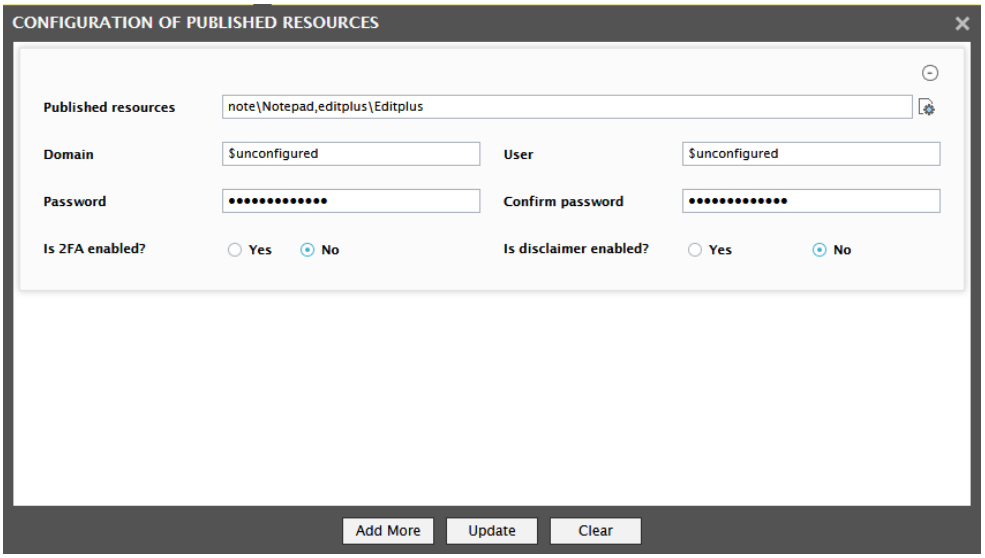

Figure 3.7: Configuring the other credentials

Using Figure 3.7, 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. Using the **Domain**, **User**, **Password**, and **Confirm Password** parameters, configure the credentials of the user who is authorized to launch the configured resources.

   Note:

   If the Storefront server is enabled with two-factor authentication and you have specified the relevant **2FA code**, then, specify *none* against the **Domain** text box.

2. **Is 2FA enabled?:** 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 StoreFront is enabled with two-factor authentication, then to authenticate the specified **User** login, StoreFront 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 StoreFront provides. This is why, if StoreFront is enabled with two-factor 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 StoreFront is not enabled with two-factor authentication, set this flag to **No**. **Note that only static 2FA is supported for user authentication.**

3. **Is disclaimer enabled?:** Some high-security Citrix 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 this 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**.

If you do not want to configure any more resources for launching, then click the **Update** button in Figure 3.7 to save the changes. To add another resource for launching, click the **Add More** button. This will add an empty record to Figure 3.7. 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.

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 3.7.

You can also clear all the configured resources and their launch details at one shot, by clicking the **Clear** button in Figure 3.7.

3.2 Simulator Dashboard

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

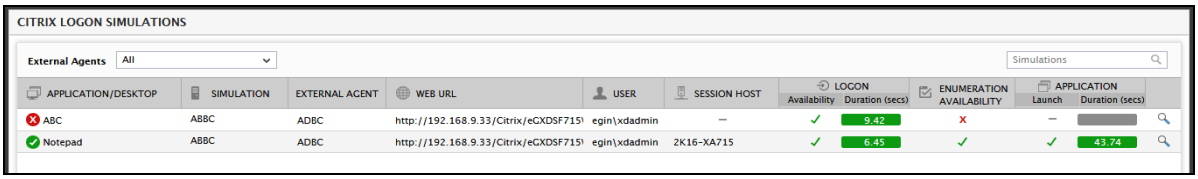

Figure 3.8: The Simulator Dashboard

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.

Figure 3.9: A graphical view of the logon process

You can click on the Details tab page in Figure 3.9 to view the output of the simulation script, scrutinize it, and isolate the failure and problem points of the Citrix delivery infrastructure (see Figure 3.10).

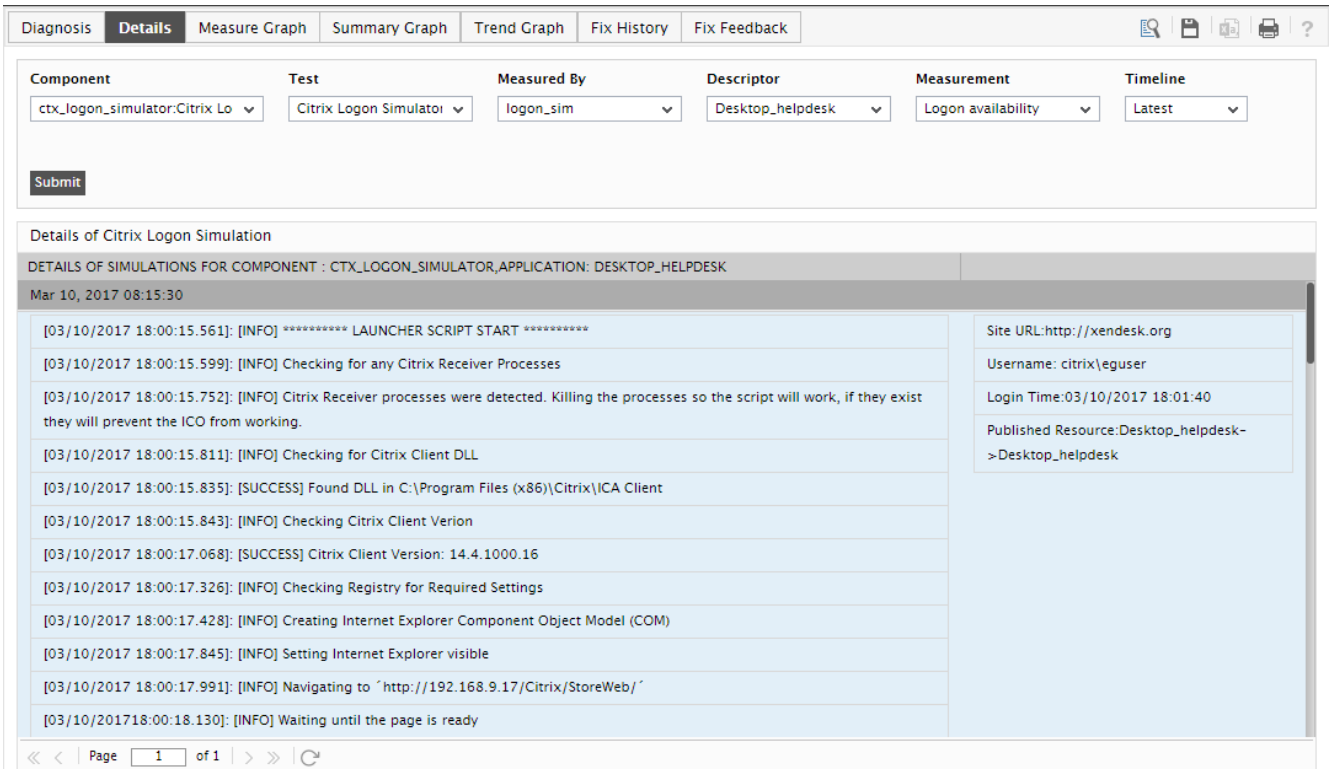

Figure 3.10: The simulation script highlighting the success and failure points of the simulation

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.

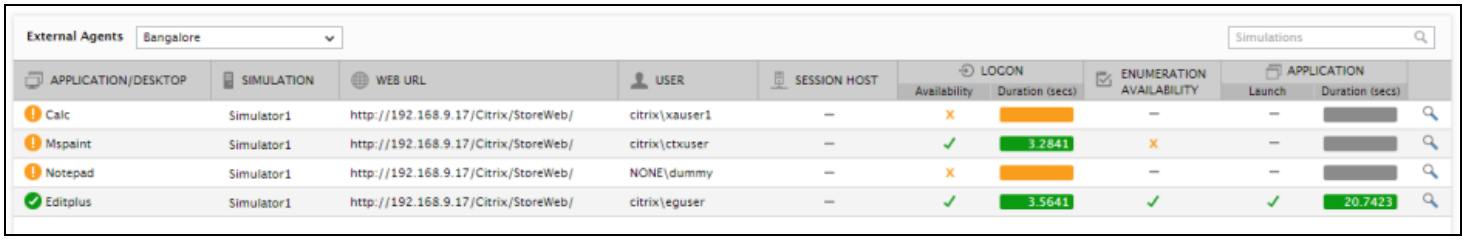

Figure 3.11: Viewing the details of a particular simulator alone

Alternatively, you can filter the dashboard contents on the basis of the *Citrix Logon Simulator* component that you managed. You can specify the whole/part of the component name in the **Simulations** search text box (see Figure 3.12) and click the 'magnifying glass' icon alongside. This will display the details of only those components with names that contain the specified search string.

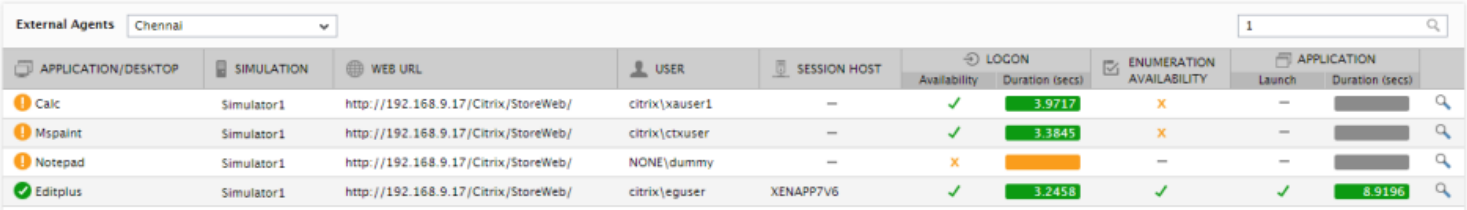

Figure 3.12: Viewing the details of only those simulations that were performed using Citrix Logon Simulator components that match the specified search string

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.

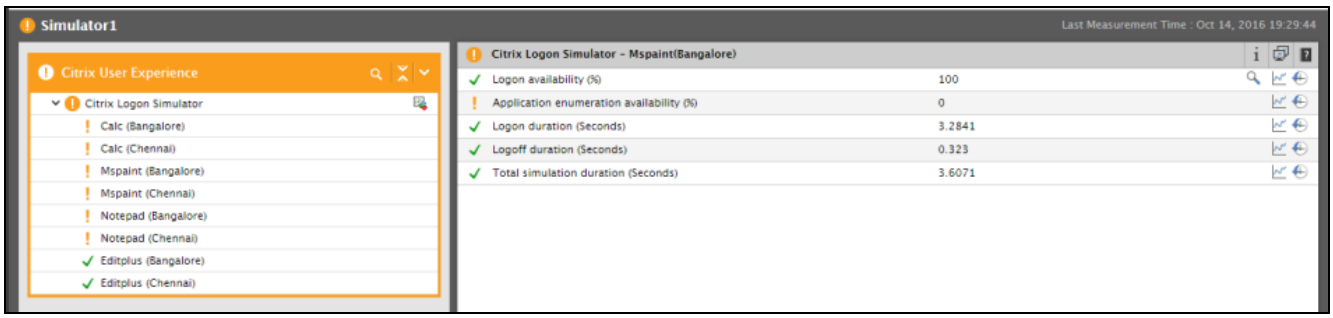

Figure 3.13: The layer model of the Citrix Logon Simulator component that was clicked on

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 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.

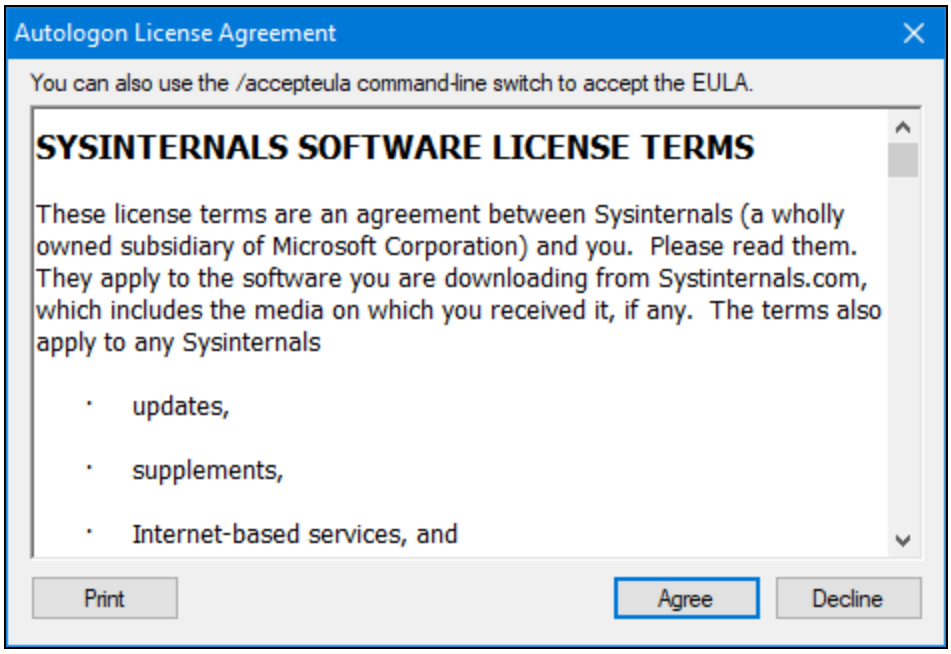

Figure 4.1: Agreeing to the Software License Terms

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

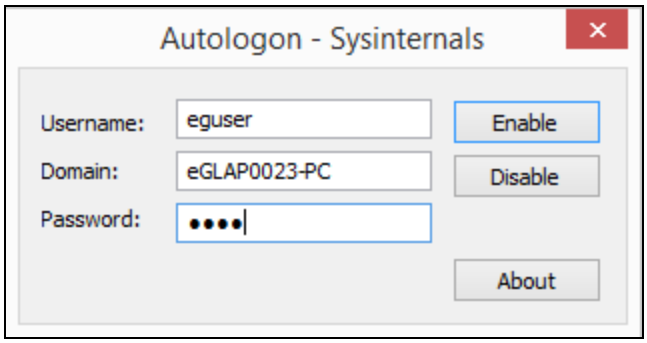

Figure 4.2: Provide the password in this form

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.

Chapter 5: Troubleshooting the eG Citrix Logon Simulator

Sometimes, the simulator may not be able to launch the published application/desktop automatically. Some of the problems that are caused while publishing the applications/desktops, and the means to resolve them are outlined here.

5.1 Unavailable Service Desktop

When the simulator tries to launch the published application / desktop, you may sometimes come across the following message:

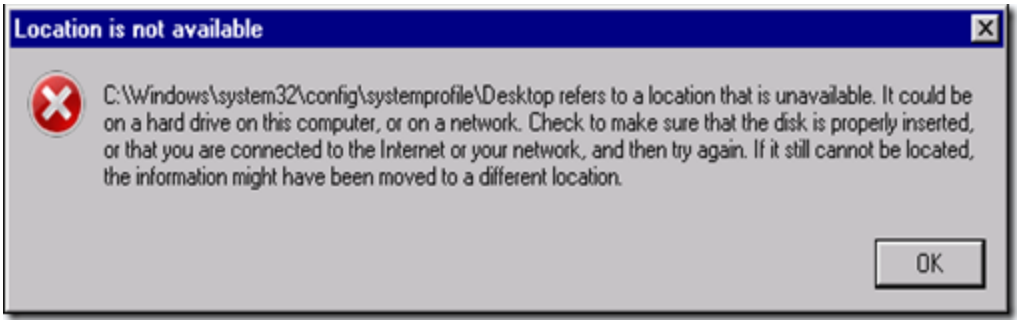

Figure 5.1: A message box indicating that a location is unavailable

To resolve this issue, navigate to C:\Windows\System32\config\systemprofile on the simulation endpoint (i.e., where the external agent and Citrix Receiver are installed) and create a new folder and rename it to “Desktop”.

5.2 Citrix Receiver Not Supporting Selected Encryption

When the simulator tries to launch the published desktop/application, the following error message may sometimes appear, causing the launch to fail:

"This version of Citrix Receiver does not support selected encryption. Please contact your administrator.”

To resolve this issue, follow the steps below:

- Open the Windows Registry.
- Add an entry with the following details to the HKLM\Software\Citrix\ICA Client key:

  Name: VdLoadUnLoadTimeOut

Type: Reg_Dword

Value: 60

5.3 Web Interface Delay Experienced by First User of the Day

When connecting to the Web Interface, there can be a delay before the first page appears. After restarting IIS, or rebooting the Web Interface server, it takes up to 1 minute to load the Welcome page for the first user. If simulation happens during this period, then it will capture and alert administrators to this delay every day, unnecessarily bothering them with an issue, that in fact does not exist. If this is to be avoided, then its best that you ensure that this delay does not occur. For that, do the following:

1. This issue is caused by a CRL check sent to Verisign. If the Web Interface server cannot access the internet, the CRL check fails and times out. To avoid this therefore, first determine the ASP.net version in IIS that is in use with the Web Interface site. Then, open the **ASPNET.CONFIG** file that corresponds to that version from the C:\WINDOWS\Microsoft.NET\Framework\<.Net_framework_version> folder.
2. Add the following lines to your **ASPNET.CONFIG** or **APP.CONFIG** file:

   <?xml version="1.0" encoding="utf-8"?>
   <configuration>
   <runtime>
   <generatePublisherEvidence enabled="false"/>
   </runtime>
   </configuration>

3. Finally, save the file.

5.4 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 5.2 appears.

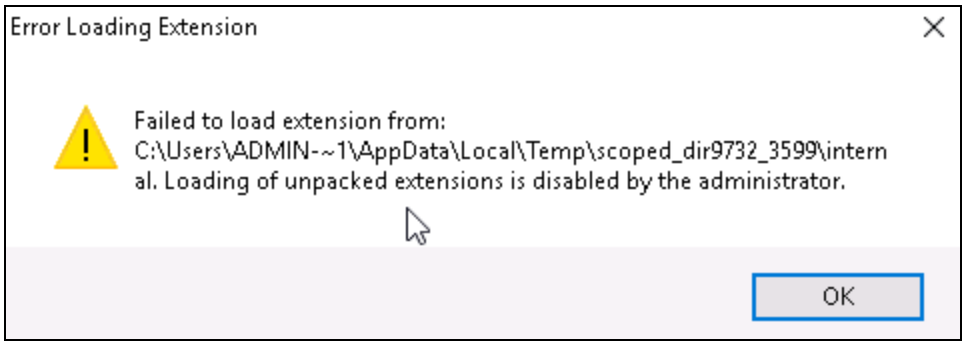

Figure 5.2: Error message that appears when chrome extensions failed to load

For the Citrix 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 Citrix 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.