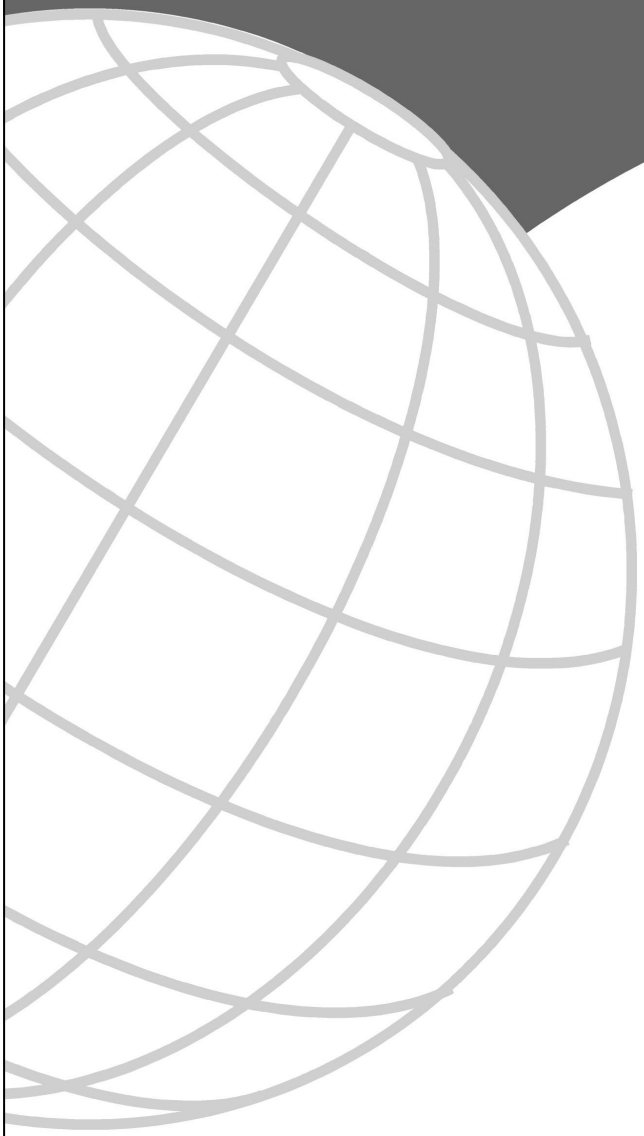

Enabling Service Excellence

The eG Citrix Logon Simulator

Table of Contents

Table of Figures

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 Internet Explorer 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 the Citrix Logon Simulator

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

- The eG license should enable the **Client Emulation** capability.
- A dedicated eG external agent is required for the purpose of this simulation. This implies that the external agent should only be used as the Citrix Logon Simulator. You should not use the same agent to perform external monitoring of your servers/devices or to perform client emulation using Tevron's Citra Test / Itexis AppsMon.
- The eG external agent used for the simulation should run only on the English version of a Windows 2008/7/8/10/2012/2016 operating system.
- The Windows system hosting this eG external agent should use only a static IP address.
- .Net 3.5 should pre-exist on the external agent host.
- The simulator will only work with Citrix XenApp / XenDesktop 6.x and 7.x environments.
- 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.
- The Citrix AppController cannot be used for the simulation.
- When using Citrix StoreFront, make sure that the **Authentication mode** of StoreFront is set to **Explicit**.
- Also, when using Citrix StoreFront, check if the Citrix StoreFront store that you want to set as the **SITE URL** allows access from both internal and external networks. If so, then make sure *Domain Pass-through* is disabled for that store. The steps in this regard are as follows:
  - Login to the Citrix StoreFront console.
  - Click on **Stores** in the left panel of the console to view the stores on StoreFront (see Figure 1).

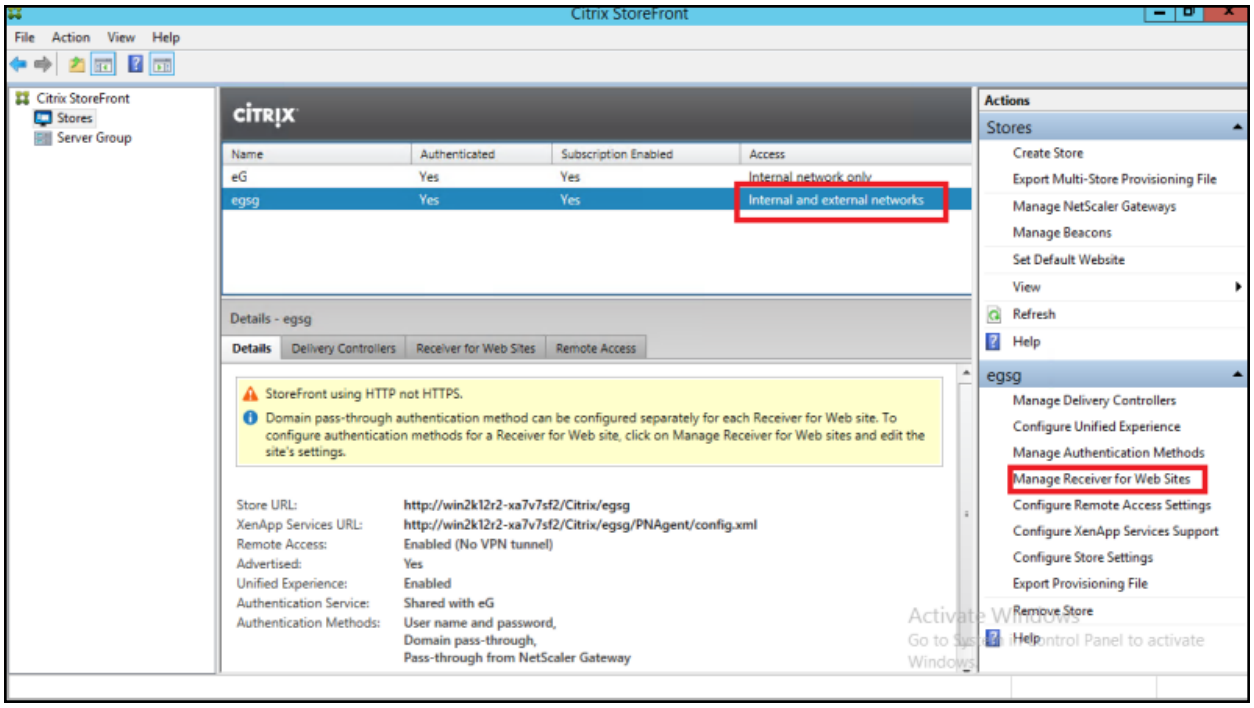

Figure 1.1: Checking the Access method of the stores

- Browse the list of stores in the right panel to locate the store containing the resources (i.e., applications/desktops) that your simulator should launch.
- Once you find the store, check the **Access** setting of that store - i.e., check the entry in the **Access** column of that store. If it reads, Internal and external networks, you can confirm that the store allows access from both internal and external networks. In this case, select the store and then click the **Manage Receiver for Websites** option from the list of **Actions** for that store.
- From the list of **Web sites** that appears, select the URL that has been set as the **SITE URL**. Then, click **Configure**.

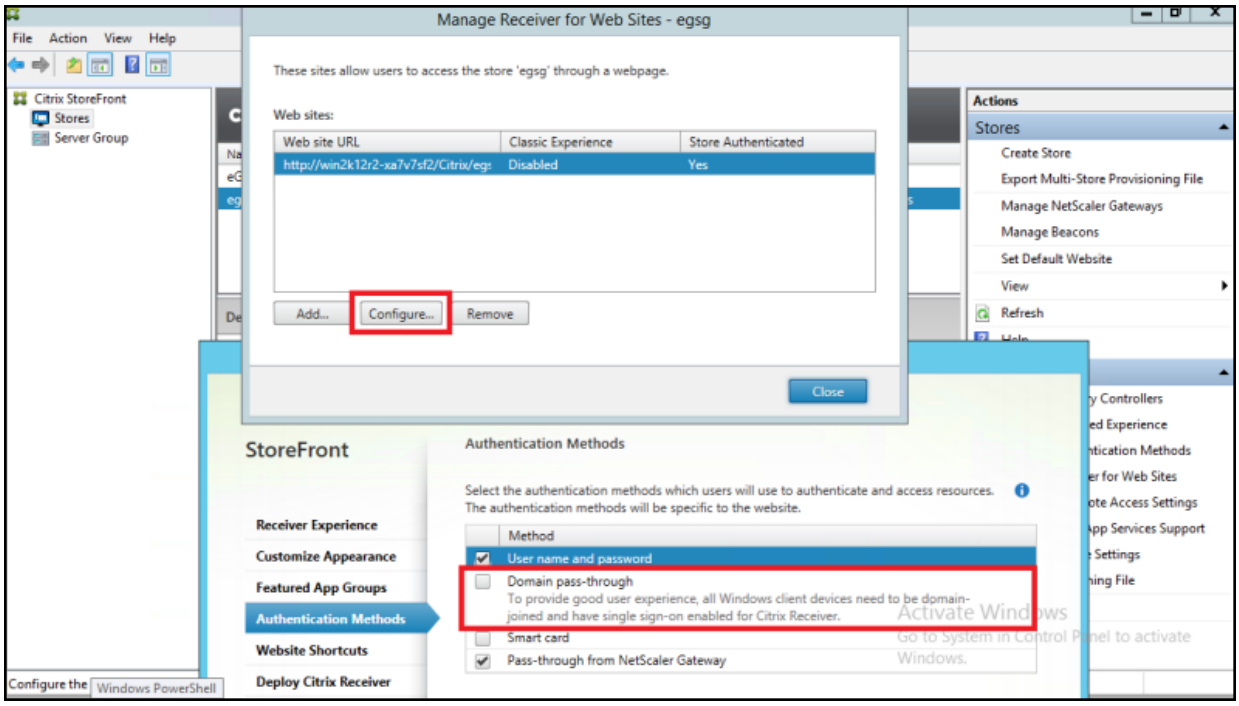

Figure 1.2: Disabling Domain pass-through

- When the **Authentication Methods** are listed, deselect the **Domain pass-through** check box in the list and save the changes.

- Citrix Receiver 4.0 (or above) should be installed on the system hosting the external agent that performs this simulation. Take care to install the Receiver in the default location only.
- The simulator requires a dedicated Citrix test account with rights to launch applications/desktops.
- When monitoring 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. You can auto subscribe users to applications by setting "KEYWORDS:Auto" in the published application's description in the Citrix XenDesktop Broker.

  When monitoring 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. To achieve this, do the following:

  - Login to the Citrix Web Interface.
  - When the Citrix Web Interface Management console opens, select **XenApp Web Sites** node from the **Citrix Web Interface** tree in the left panel of the console (see Figure 1.3).

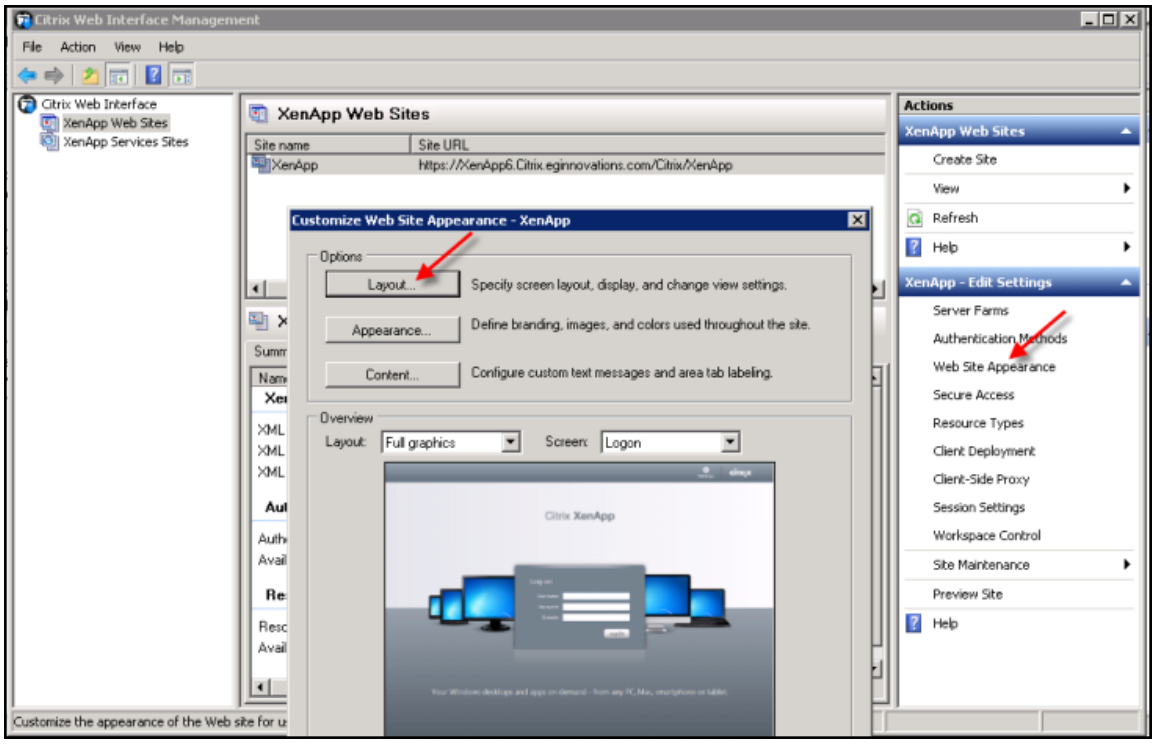

Figure 1.3: The Citrix Web Interface Management console

- From the list of XenApp sites displayed in the right panel of Figure 1.3, select the site to which the simulator should log on.
- Then, from the **Actions** pane, select the **Web Site Appearance** option indicated by Figure 1.3.
- This will open the **Customize Web Site Appearance - XenApp** dialog box of Figure 1.3. Click on the **Layout** button in this dialog box.
- Figure 1.4 will then appear.

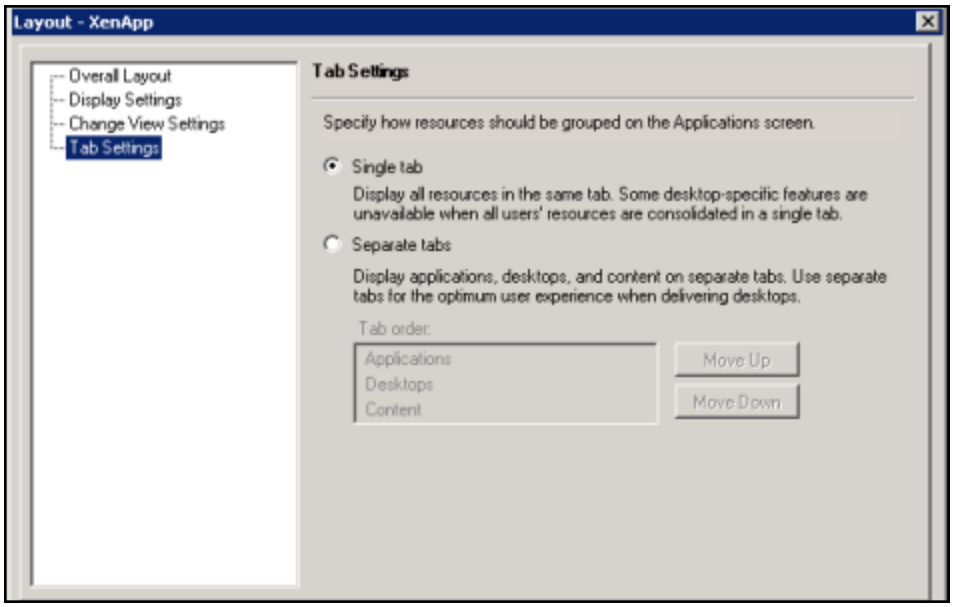

Figure 1.4: Indicate how the resources should be grouped

- Select the **Single tab** option from Figure 1.4 so that all published resources appear in a single Main page, as depicted by Figure 1.5.

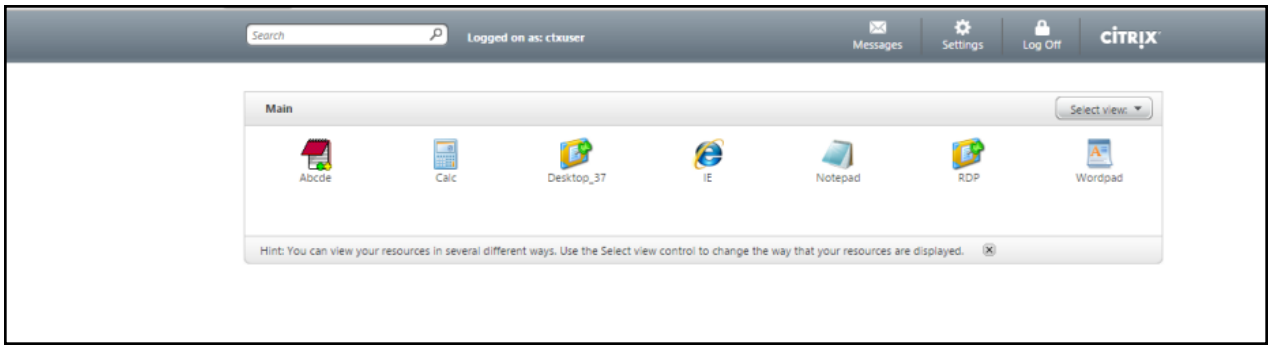

Figure 1.5: The Main page displaying all published resources

- Additionally, for launching desktops published on Citrix XenApp / XenDesktop 7, set the **autoLaunchDesktop** and **pluginAssistant** flags to **false** in the **web.config** file under C:\inetpub\wwwroot\Citrix\<storename>Web folder on the StoreFront server.
- The simulator also requires a user account with local administrator rights on the simulation endpoint - i.e., on the system hosting the external agent / Citrix Receiver. This user should be logged in at all times for the simulator to run continuously.
- No other 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.
- Make sure that **User Account Control** is disabled at the system-level on the simulation endpoint.

- If the Citrix Receiver has created a system tray icon on the simulation endpoint, then make sure it is removed. To remove this 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**.
- The simulator mandates the presence of Internet Explorer 11. No other browser (including Edge) supports this simulation.
- 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.
- The **SITE URL** that you want to configure for the simulation should first be added as a trusted site in Internet Explorer. For that, follow the steps below:
  - Open Internet Explorer, and browse the Tools -> Internet options menu sequence. Then, click on the Security tab page in the Internet Options dialog that appears. Figure 1.6 will then appear.

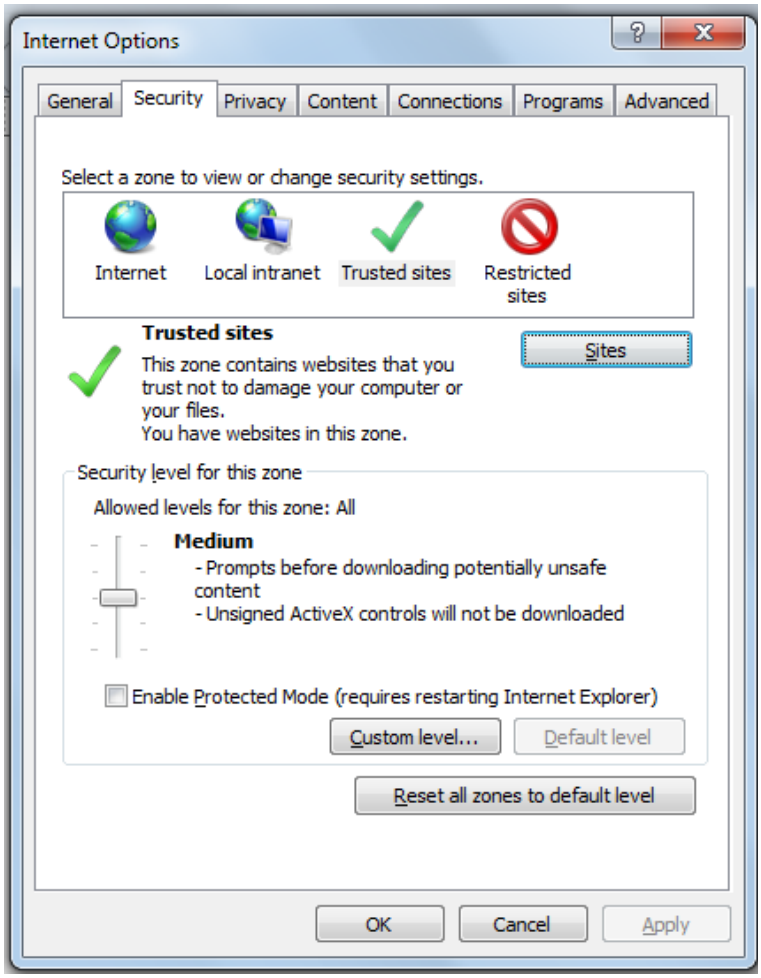

Figure 1.6: The Internet Options dialog box

- Click on the **Trusted Sites** option inFigure 1.6. This will open Figure 1.7.

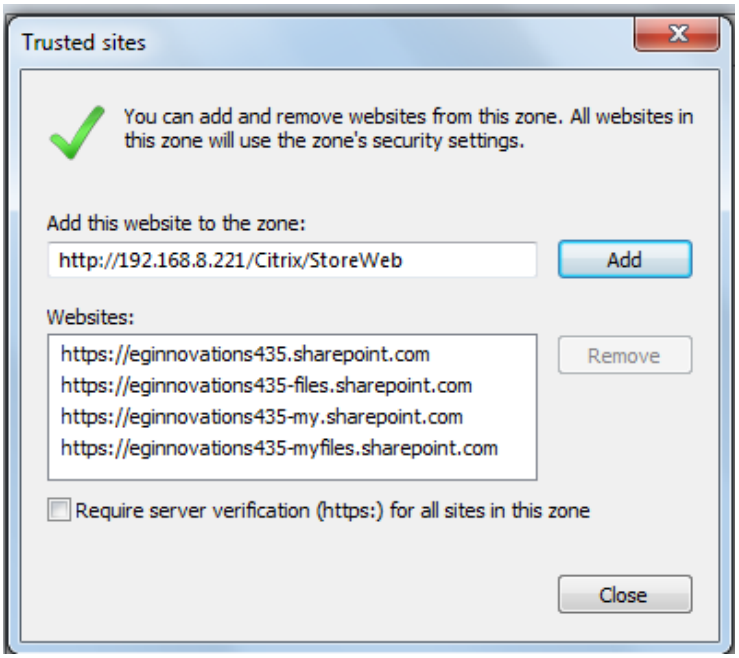

Figure 1.7: Adding the Site URL as a trusted site

- In the **Add this website to the zone** text box, type the URL of the site that you want to use for the simulation.
- If the URL you entered is not an HTTPS URL, then uncheck the **Require server verification...** check box in Figure 1.7.
- Then, click the **Add**button to add the site URL to the list of trusted sites. This will add the URL to the **Websites** list box. Then, click the **Close** button.

- Make sure that the **Trusted sites** zone of Internet Explorer is assigned the **Medium-low** security level. To achieve this, do the following:
  - Open Internet Explorer, and browse the Tools -> Internet options menu sequence. Then, click on the **Security** tab page in the **Internet Options** dialog that appears. Figure 1.8 will then appear.

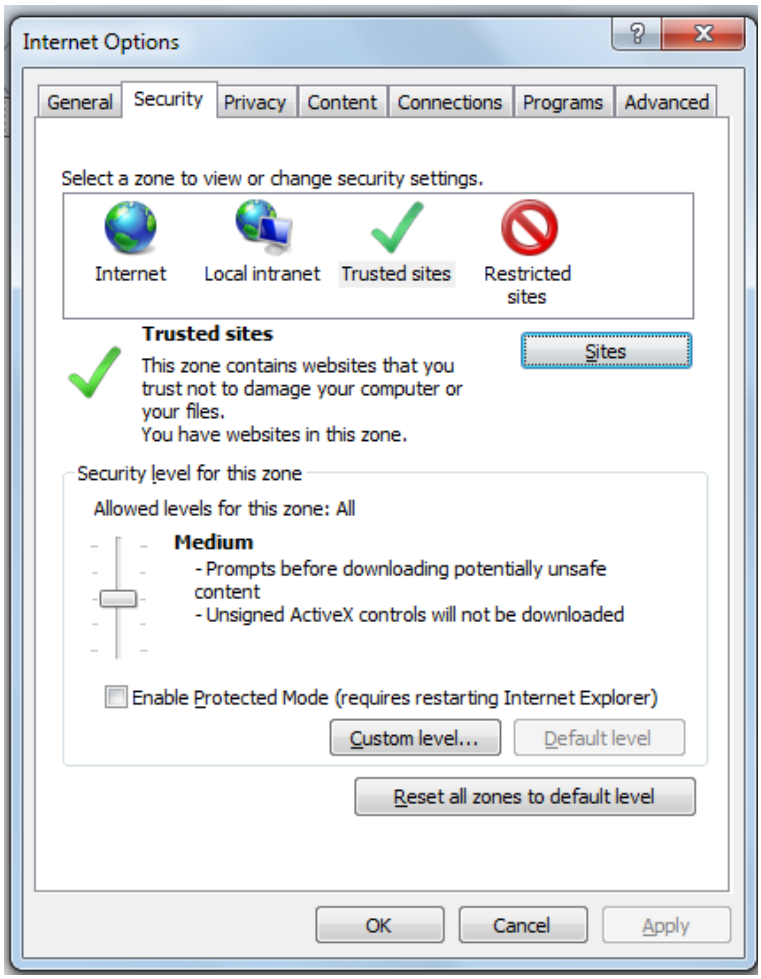

Figure 1.8: The Internet Options dialog box

- Click on the **Trusted sites**zone in Figure 1.8. This will open Figure 1.9.

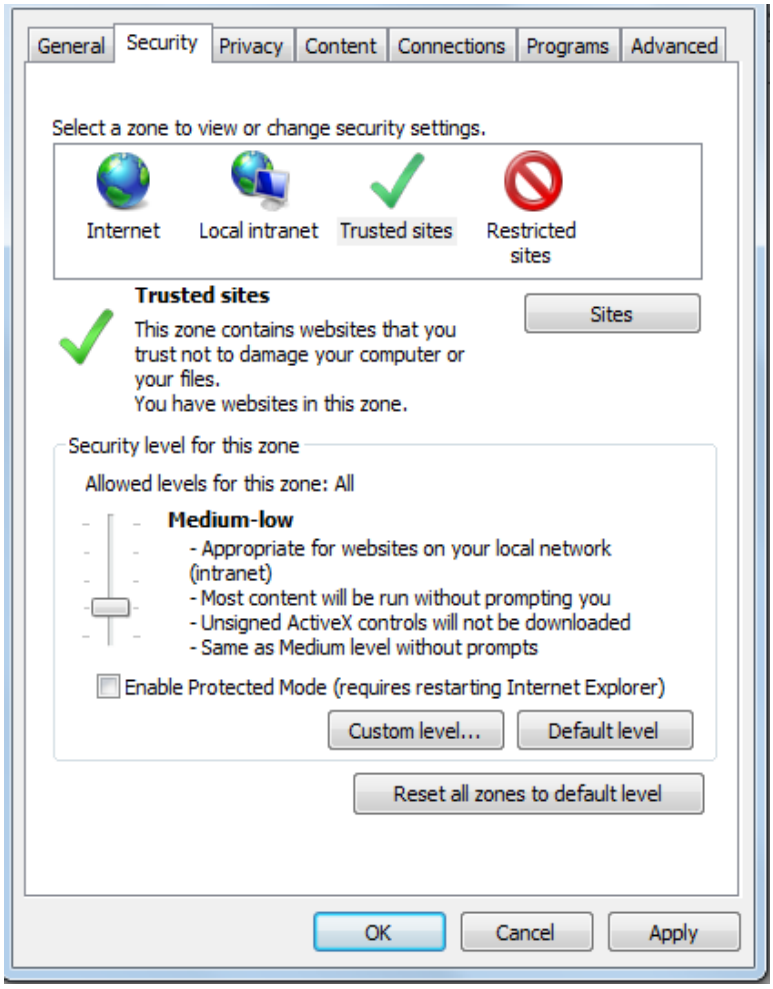

Figure 1.9: Setting the security level of Trusted sites zone to Medium-low

- Use the slider control in the **Security level for this zone** section to set the security level to **Medium-low**.
- Finally, click the **Apply** and **OK** buttons to save the changes.

- Configure Internet Explorer to not prompt for saving/remembering the password, as this may hinder simulation. To disable this prompt, do the following:
  - Open Internet Explorer, and browse the Tools -> Internet options menu sequence. Click on the **Content** tab page in the **Internet Options** dialog that appears (see Figure 1.10).

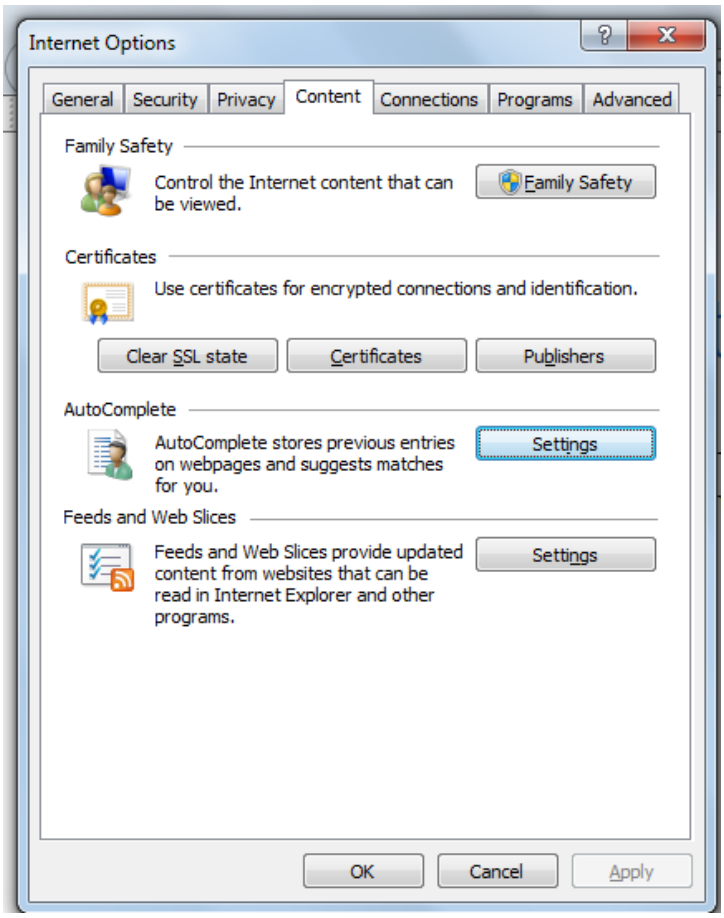

Figure 1.10: The Content tab page of the Internet Options dialog box

- Click the **Settings** button in the **AutoComplete** section. This will open Figure 1.11.

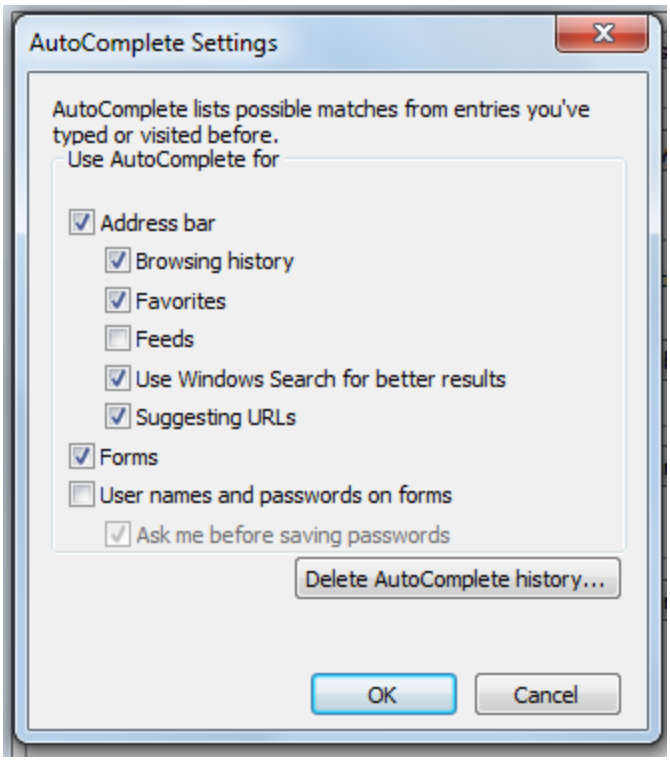

Figure 1.11: Disabling the password prompt

- Here, uncheck the **User names and passwords on forms** check box.
- Finally, click the **OK** button.

- Ensure that the Internet Explorer browser is enabled to run JavaScripts. For this, follow the steps below:
  - Open Internet Explorer, and browse the Tools -> Internet options menu sequence. Click on the **Security** tab page in the **Internet Options** dialog that appears (see Figure 1.12).

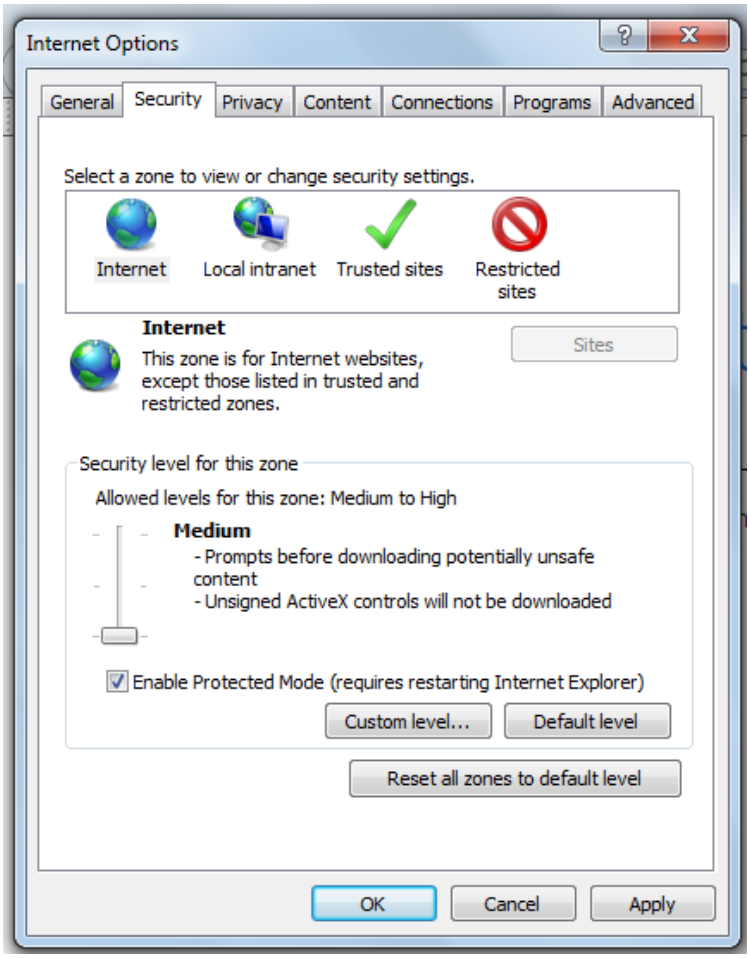

Figure 1.12: The Security tab page of the Internet Options dialog box

- Select the Internet zone from the **Select a zone . . .** section, and then click the **Custom Level** button in the **Security** level for this zone section. This will open Figure 1.13.

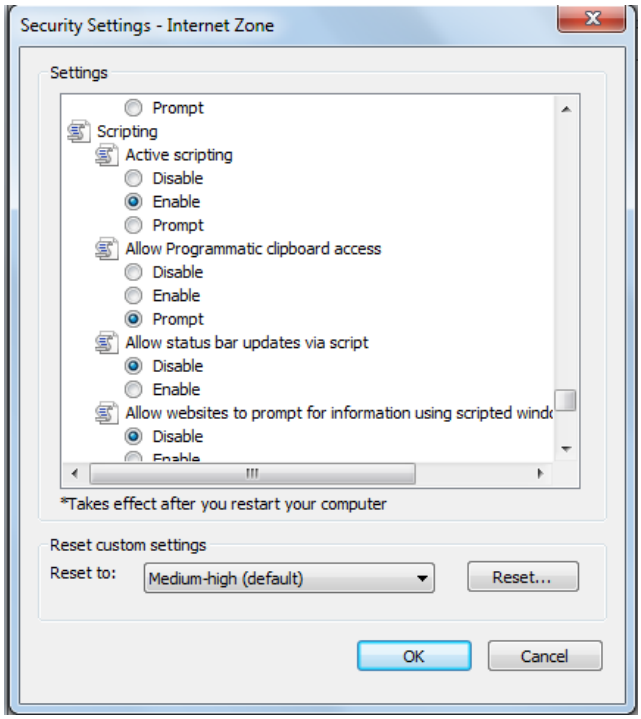

Figure 1.13: Enabling JavaScript

- Scroll down the **Settings** list in Figure 1.13 until you find the **Scripting** section.
- In this section, choose the **Enable** option of **Active scripting**, and click the **OK** button in Figure 1.13.

1.2 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 **Configuring the Citrix Logon Simulator** 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 1.14 below.

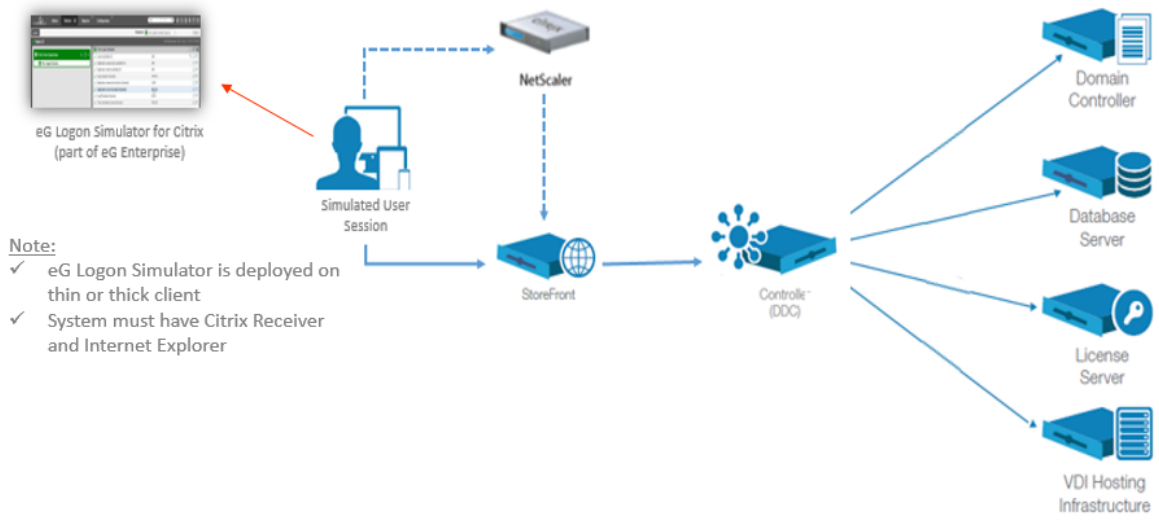

Figure 1.14: How the Citrix Logon Simulator Works

The process depicted by Figure 1.14 is described below:

1. The simulator first opens Internet Explorer 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.

2

Configuring the Citrix Logon Simulator to Perform the Simulation

Once the pre-requisites outlined 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).

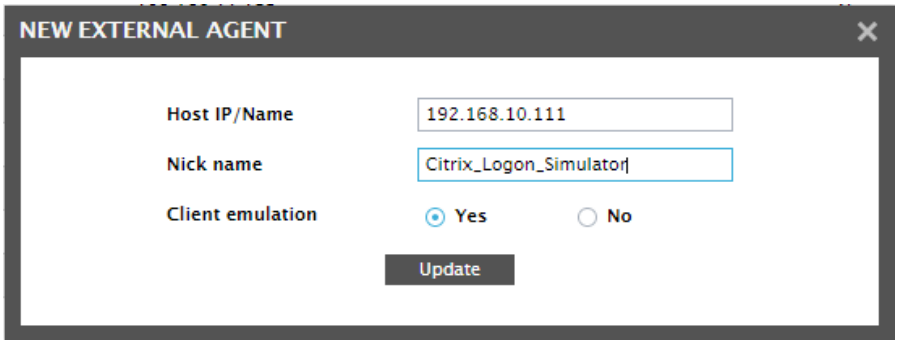

Figure 2.1: Adding a dedicated external agent for the simulation

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.

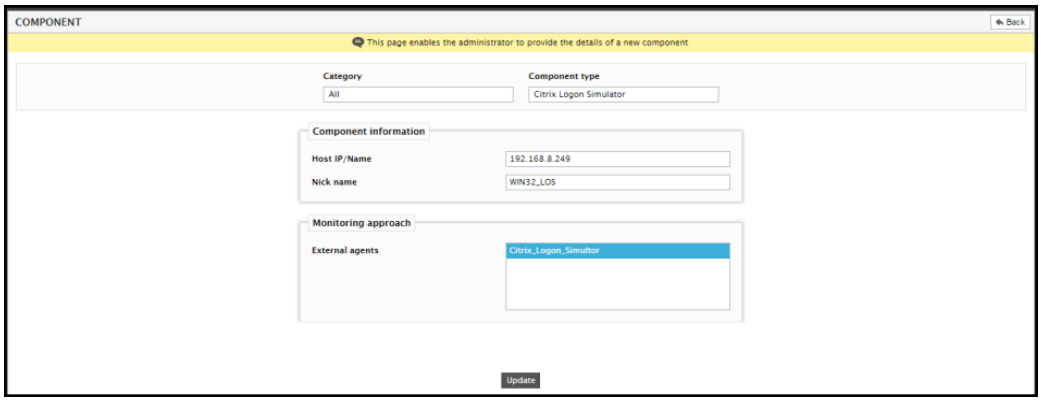

Figure 2.2: Adding a Citrix Logon Simulator

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.

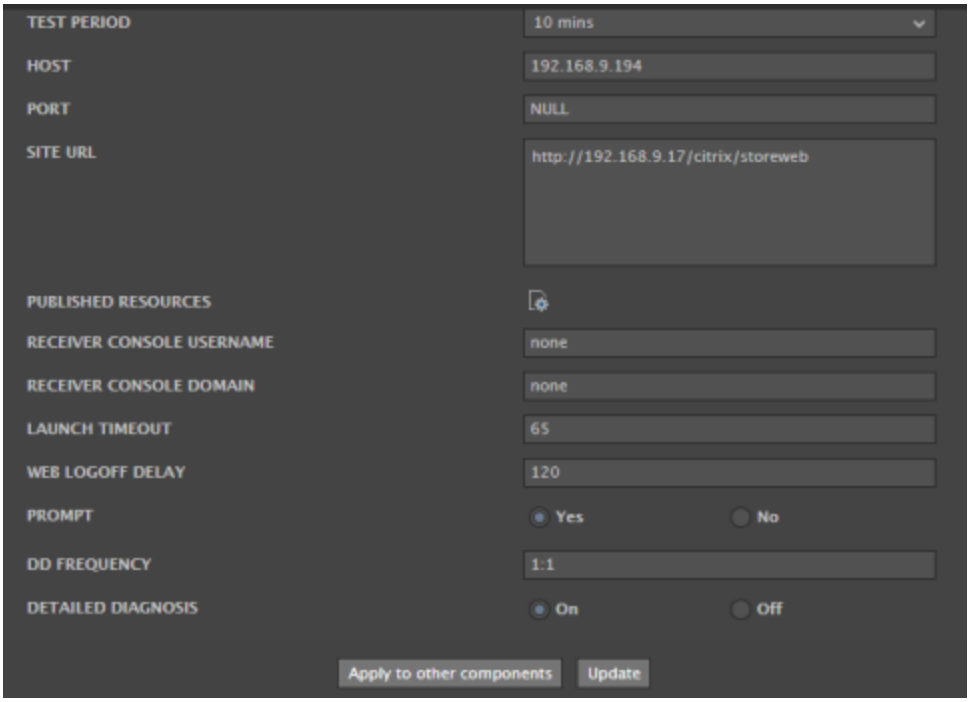

Figure 2.3: Configuring the Citrix Logon Simulator test

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

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.

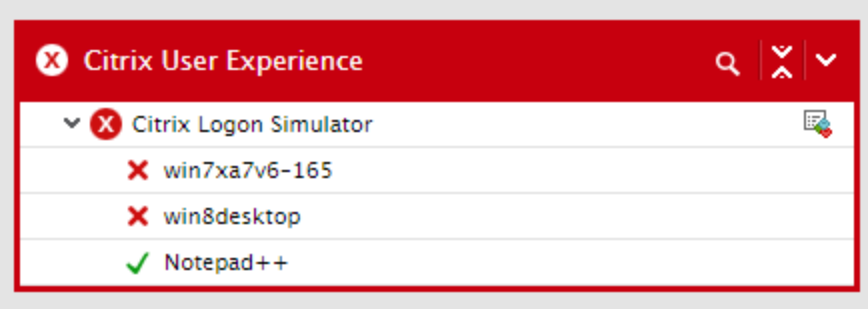

Figure 3.1: The layer model of a Citrix Logon Simulator component

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.
   - The URL should be added to the **Trusted Sites** zone of Internet Explorer. To know how, refer to the **Pre-requisites for Using the Citrix Logon Simulator**.
   - The **Trusted Sites** zone should be assigned the **Medium-low** security level. To know how, refer to the **Pre-requisites for Using the Citrix Logon Simulator**.
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. **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 **Y**es.

10. **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.

11. **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

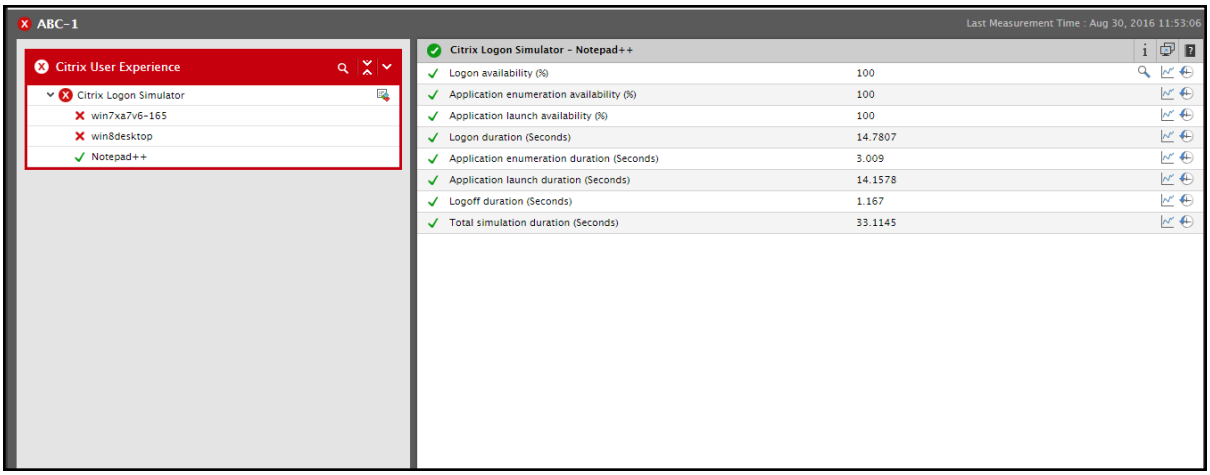

Figure 3.2: The measures reported by the Citrix Logon Simulator test

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?

Measurement	Description	Measurement Unit	Interpretation
Application 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 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 authentication? application enumeration? application launch? or log out?
Logoff duration:	Indicates the time taken by	Secs	If the *Total simulation duration* for an

Measurement	Description	Measurement Unit	Interpretation
	the simulator to log out of StoreFront / NetScaler.		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 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.

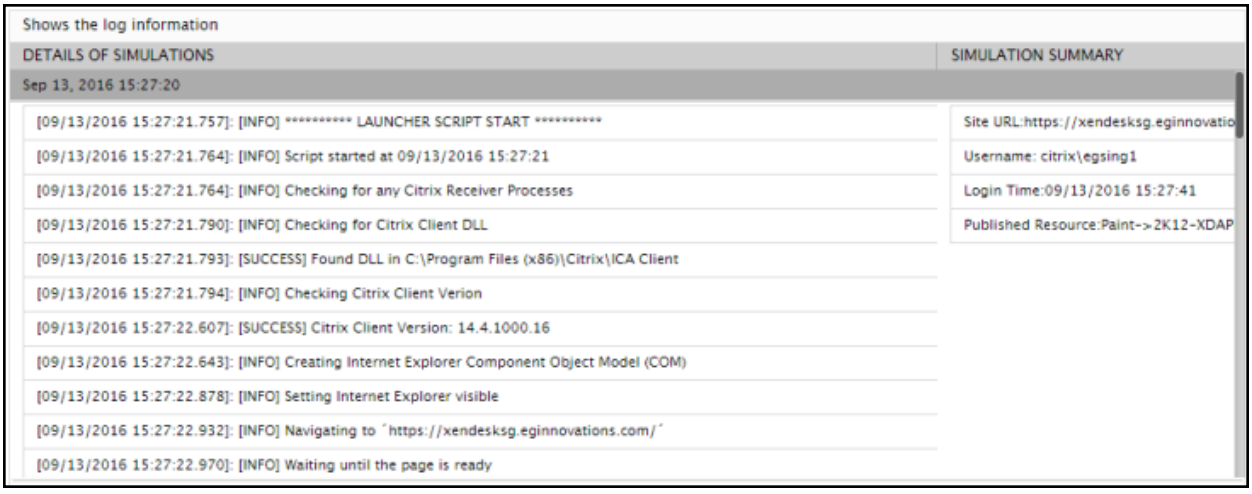

Figure 3.3: The detailed diagnosis of the Logon availability measure

3.2 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**.

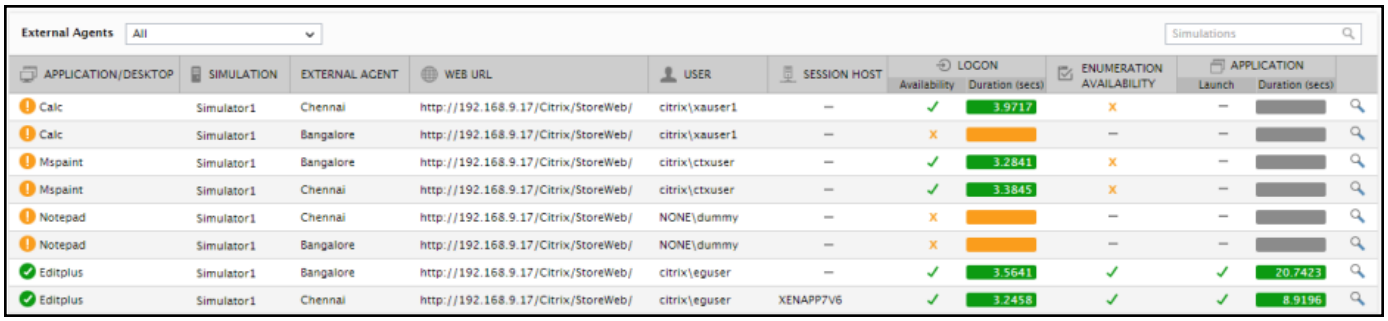

Figure 3.4: The Simulator Dashboard

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 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.

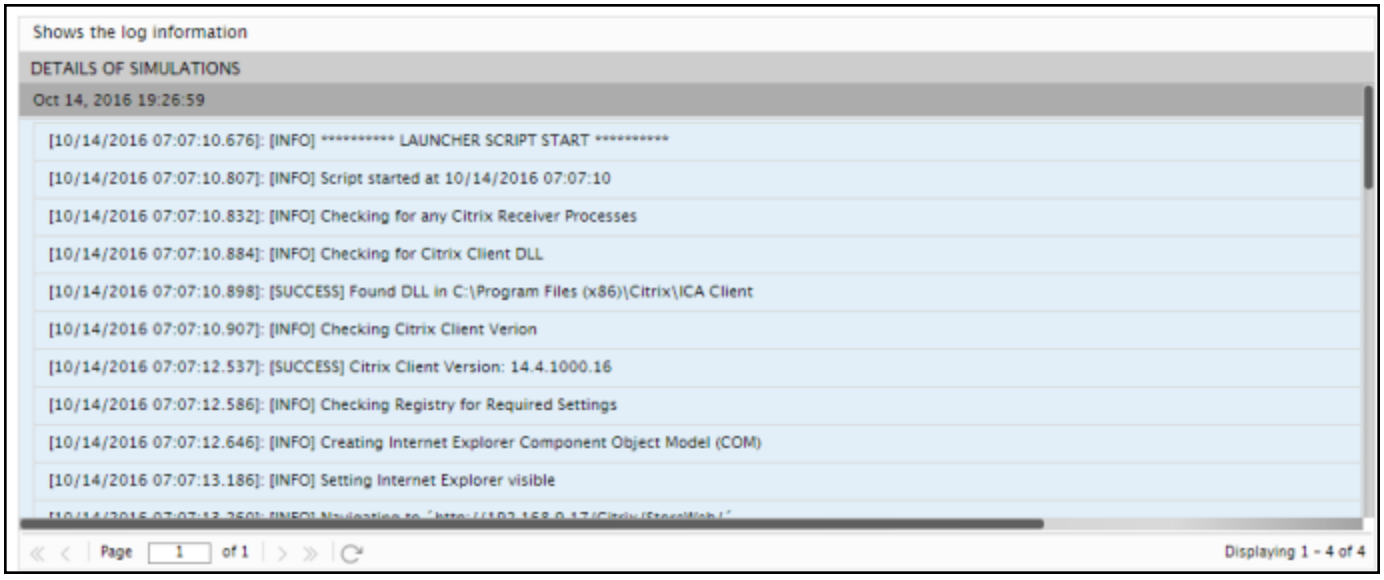

Figure 3.5: The simulation script highlighting the success and failure points of the simulation

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 3.6: 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 3.7) and click the 'magnifying glass' icon alongside. This will display the details of only those components with names that contain the specified search string.

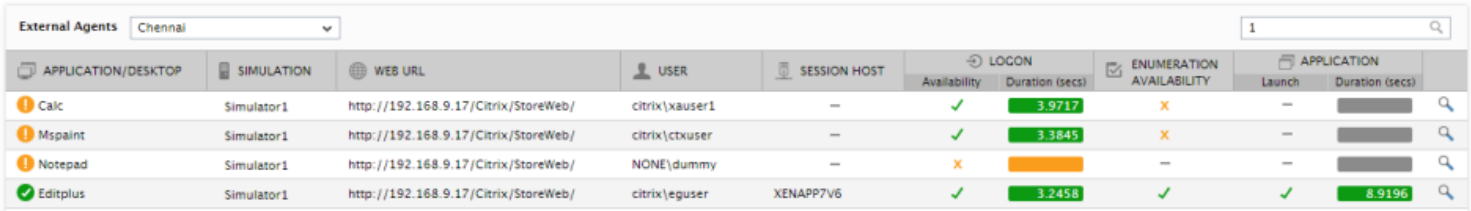

Figure 3.7: Viewing the details of only those simulations that were performed using Citrix Logon Simulator components that match the specified search string

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.

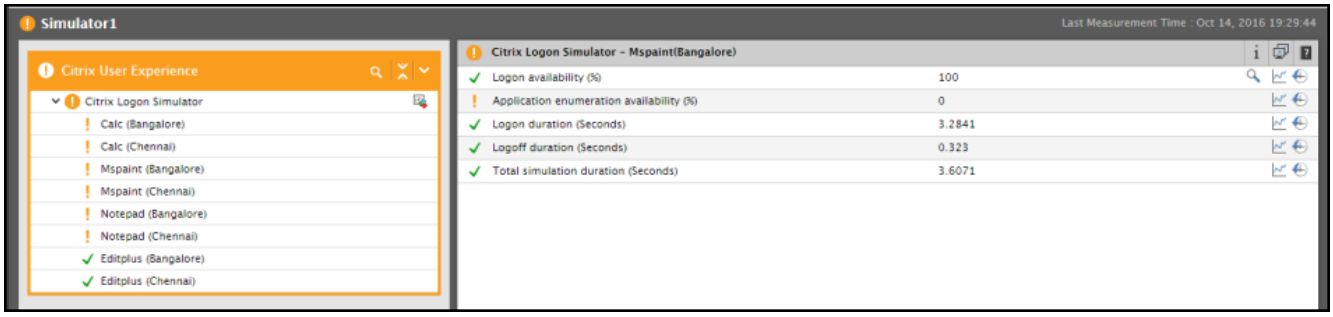

Figure 3.8: The layer model of the Citrix Logon Simulator component that was clicked on

4

Troubleshooting the eG Citrix Logon Simulator

Sometimes, the simulator may not be able to launch the published application/desktop automatically. More often than not, this could be due to the security settings applied in Microsoft Internet Explorer. Some of these settings, the problems they may cause, and the means to resolve them are outlined here.

4.1 Troubleshooting the Inability of IE to Open the ICA File Automatically

Sometimes, when the simulator tries to launch an application / desktop, Internet Explorer will throw the following error message:

Figure 4.1: The error message that appears if IE is unable to open an ica file automatically

There can be a number of reasons for the issue including but not limited to:

- The *.ica file on the client needs to be associated with a required installation of the Citrix Receiver.
- The Internet Explorer browser option "Do not save encrypted data to disk" is selected in the Internet Settings on the Advanced tab.
- A lockdown issue occurring after an upgrade of the current Internet Explorer browser version is preventing the launch.
- The Web Interface server is not configured with the proper address routing or network address translation setting causing the launch.ica file to render with the incorrect local network IP address or https/SSL WAN address location.
- Third party web browser based applications, known as Adware, or password caching shopping based programs installed on a client's machine have been known to be the cause of this prompt.

There can be a number of resolutions to the issue including but not limited to the following:

- **Install the Latest Version of Citrix Receiver**

  Make sure that the latest version of Citrix Receiver is installed on the eG external agent host. If you do not have the latest version installed, then download the latest version from https://www.citrix.com/downloads/citrix-receiver.html , and install it.

- **Add Website to Trusted Sites**

  Ensure that the **SITE URL** that is configured for the **Citrix Logon Simulator** test is added to the **Trusted sites** zone of Internet Explorer. To know how to add a URL to the **Trusted sites** zone, refer to the Pre-requisites for Using the Citrix Logon Simulator.

- **Remove or Disable Third Party Browser Adware**

  Remove or disable any third party browser based Adware software that could be interfering with the successful launch of the ICA file. Restart the browser after removing these software and try again.

- **Clear the "Do not save encrypted data to disk" Option**

  The “Do not save encrypted data to disk.” option should be cleared because the dynamic files are stored in the Temporary Internet Files folder. When applications are clicked, a file is downloaded to the folder, then launched using MIME type. If access to the folder is disabled or not available, the process cannot occur successfully.

  To disable the “Do not save encrypted data to disk.” option, follow the steps below:

  - Open Internet Explorer and follow the Tools -> Internet Options menu sequence.
  - Select the **Advanced** tab page in the **Internet Options** dialog box that appears next. Keep scrolling down the contents of the tab page until you find the **Security** section. Then, deselect the check box alongside “Do not save encrypted data to disk” in that section.

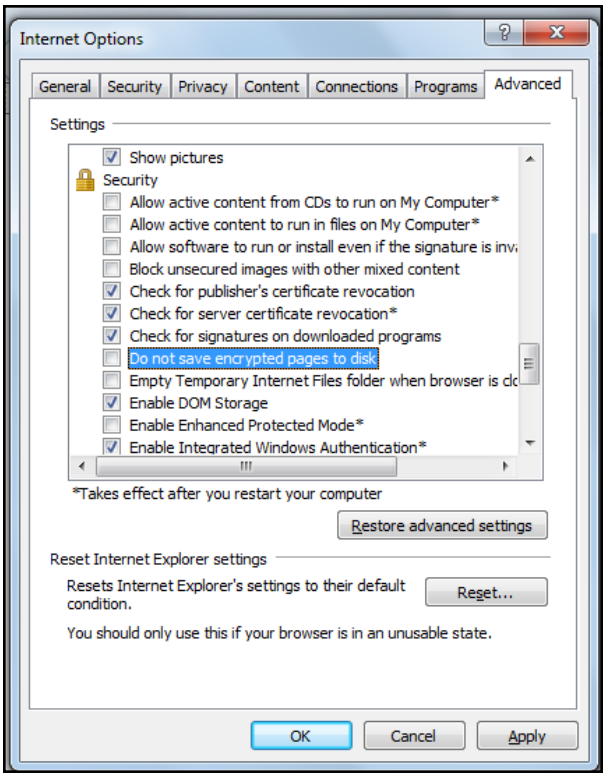

Figure 4.2: Clearing the “Do not save encrypted data to disk" option

- Finally, click the **Apply** and **OK** buttons in 4.1

- **Automatically Open ICA Files**

  You need to enable Internet Explorer to automatically open ICA files. For this, right-click on the downloaded file and uncheck the option **Always ask before opening this type of file**.

- **Associate .ica File Type With Citrix Connection Manager**

  To achieve this, follow the steps below:

  - On Windows computers, go to Control Panel > Programs > Default Programs > Associate a file type or protocol with a program.
  - Under **Name**, find .ica file type.
  - Ensure that the current default is set to **Citrix Connection Manager**. If not, click **Change program** and choose **Citrix Connection Manager**.

- **Disable ActiveX**

  Configure Internet Explorer as follows to allow successful application launching:

1. Disable ActiveX filtering feature for the Web Interface site, using either of the following methods:

   - Disable ActiveX filtering globally: For this, Click **Gear** icon, select **Safety**, de-select **ActiveX Filtering**(see Figure 4.3). Alternatively, press Alt key and click Tools menu (ActiveX filtering is enabled if a "tick" appears next to it and is disabled if the "tick" disappears).

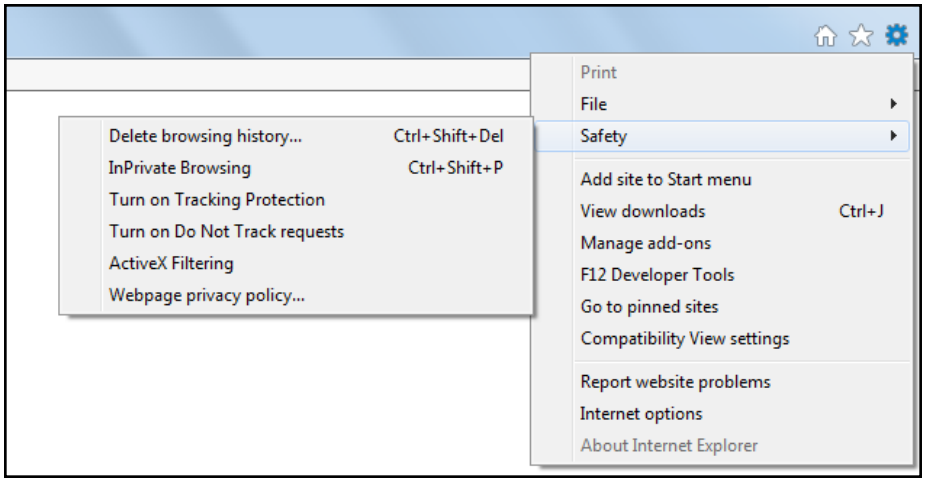

Figure 4.3: Disabling ActiveX filtering globally

   - Disable ActiveX filtering for an individual site when ActiveX filtering is enabled globally: For this, do the following:

     - Log on to the Web Interface site and attempt to launch an application. At the end of the address bar a blue warning sign appears, indicating filtered content.

Figure 4.4: Blue warning sign in address bar

     - Click the blue warning sign and select **Turn off ActiveX Filtering**.

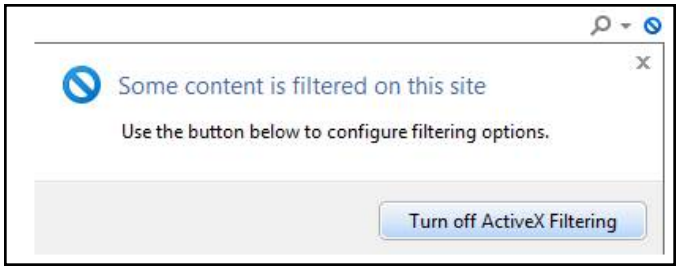

Figure 4.5: Disabling ActiveX Filtering for an individual site

2. Enable ICA launch using one of the following options:

- In the **Security** tab of **Internet Options**, add the Web Interface site to **Trusted Sites** list to allow the use of the ActiveX ICA client object for the launch.
- Rename the following registry key: HKEY_CLASSES_ROOT\PROTOCOLS\Filter\application/x-ica

3. Log off and close window then restart the browser after making this change.

After applying all the above steps, if the issue is still not resolved, please change the security settings of trusted sites zone from Medium to "Medium-low". The related steps are available in Pre-requisites for Using the Citrix Logon Simulator.htm.

4.2 Internet Explorer's 'Save Password' Prompt

When the simulator tries to authenticate the user credentials, the following prompt may sometimes appear in the Internet Explorer:

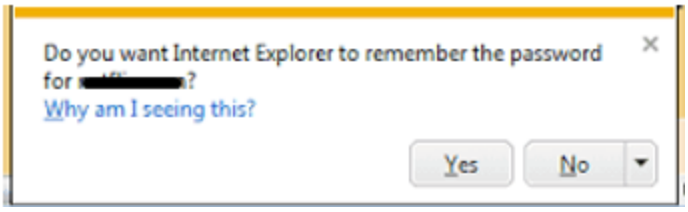

Figure 4.6: Internet Explorer prompting you to confirm whether/not to remember the password

Such a prompt will cause the simulation to fail. To avoid the prompt therefore, follow the steps detailed in the Pre-requisites for Using the Citrix Logon Simulator topic.

4.3 Unavailable Service Desktop

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

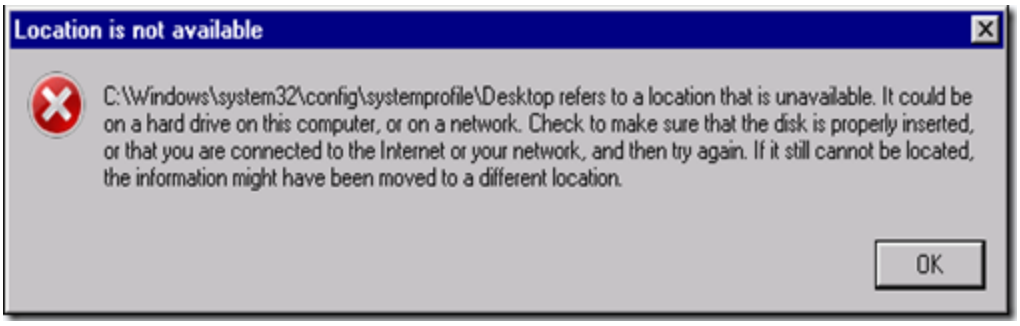

Figure 4.7: A message box indicating that a location is unavailable

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".

4.4 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

4.5 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

Conclusion

Using the eG Citrix Logon Simulator, you can proactively isolate the following problem conditions:

- Slow session logon
- Session disconnect after logon
- Logon authentication failure
- Slow application enumeration
- Citrix session not starting after logon
- Application unavailability

For more details about the eG Citrix Logon Simulator, feel free to contact sales@eginnovations.com.

We will be adding new measurement capabilities into the future versions of eG Enterprise. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.