



The eG Enterprise Express Logon Simulator for Citrix XenApp and XenDesktop

eG Innovations Product Documentation

www.eginnovations.com



Table of Contents

CHAPTER 1: AN OVERVIEW OF THE EG ENTERPRISE EXPRESS LOGON SIMULATOR FOR CITRIX XENAPP AND XENDESKTOP	1
1.1 Challenges in Troubleshooting User Logon Performance Issues in Citrix Environments	1
1.2 The eG Enterprise Express Logon Simulator for Citrix	1
1.3 How does the eG Enterprise Express Logon Simulator for Citrix Work?	2
1.4 Pre-requisites for the eG Enterprise Express Logon Simulator for Citrix	4
1.5 Installing and Configuring the eG Enterprise Express Logon Simulator for Citrix	8
1.6 Subscribe to the Simulation Service	8
1.7 Configure the Simulation	11
1.7.1 Generating Secret Key for TOTP based User Authentication	15
1.8 Download and Install the Logon Simulator Agent	24
1.8.1 Enabling the Logon Simulator Agent to communicate with the Logon Simulator Portal via a Proxy server	27
1.9 Installing the eG Logoff Helper	28
1.10 Fine-tuning the Simulation	32
1.10.1 Fine-tuning the simulation using Autologon.exe	33
1.10.2 Fine-tuning the simulation by editing the windows registry	34
1.11 Browser launch hindered due to disabled chrome extensions	34
1.12 Viewing and Interpreting the Simulation Results	35
1.13 Enabling Email Notifications for Issues	44
1.14 Benefits of the eG Enterprise Express Logon Simulator for Citrix	45
1.15 Going Beyond the eG Enterprise Express Logon Simulator for Citrix	46
ABOUT EG INNOVATIONS	48

Chapter 1: An Overview of the eG Enterprise Express Logon Simulator for Citrix XenApp and XenDesktop

This document provides an overview of the eG Enterprise Express Logon Simulator for Citrix XenApp and XenDesktop (popularly known as the eG Enterprise Express Logon Simulator for Citrix), its capabilities, and how it works, and also discusses the broad steps to be followed to install and configure it.

1.1 Challenges in Troubleshooting User Logon Performance Issues in Citrix Environments

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. Here are the reasons why:

- **N-tier logon process makes root-cause isolation difficult:** 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.
- **Collection of logon metrics challenging:** 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 be collected from the different tiers involved. Even then, it is 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.

1.2 The eG Enterprise Express Logon Simulator for Citrix

The eG Enterprise Express Logon Simulator for Citrix, is a free cloud-based, on-demand service that delivers proactive visibility into the logon performance in Citrix infrastructures. This simulator

emulates the exact same process that users go through when they logon to Citrix XenApp or XenDesktop, and measures user experience during Citrix logon.

Using the metrics reported by this free simulator, Citrix users and administrators can:

- Receive a consistent, true picture of Citrix logon performance, whether or not users are logged into the Citrix farm;
- Proactively capture potential logon slowness;
- Monitor the logon process end-to-end, across the different tiers involved in the process, and accurately isolate where the process is bottlenecked;

If users to your Citrix delivery infrastructure are frequently complaining of slowness or failures when accessing their applications/desktops, and such complaints are impacting your bottomline, affecting productivity, and are a troubleshooting nightmare, you no longer have to wait for days to procure and setup a monitoring system that can ease your troubleshooting pains. With the eG Enterprise Express Logon Simulator for Citrix, you can have your monitoring system up, running, reporting metrics, and pinpointing delivery bottlenecks in no time, without investing even a dime on the hardware and resources required for configuring a full-fledged monitoring infrastructure.

1.3 How does the eG Enterprise Express Logon Simulator for Citrix Work?

A light-weight eG Logon Simulator Agent drives the logon simulation. You only have to register with a web-based Logon Simulator portal, download and install this agent on any Windows host in your environment, and configure it to simulate accesses to an application/desktop. The agent then periodically emulates the entire process of a user logging into a Citrix farm and launching an application / desktop. Since the agent 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 two-factor authentication code, if StoreFront is enabled with two-factor authentication

Once the simulator is configured, it runs at a pre-configured frequency. Every time it runs, it simulates the logon process as depicted by Figure 1.1 below.

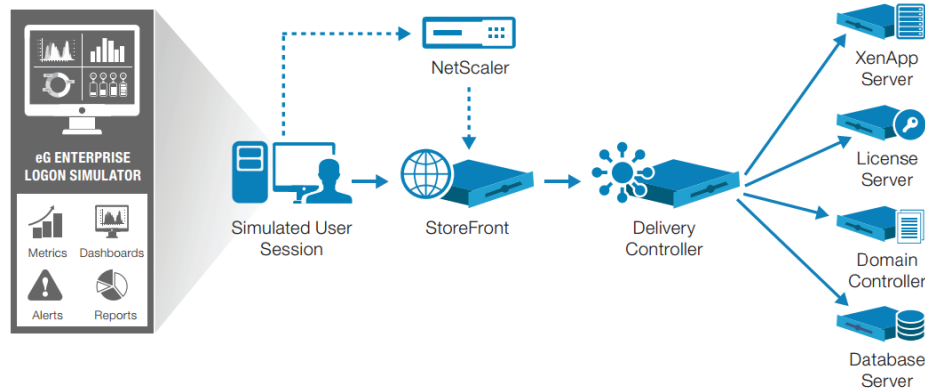


Figure 1.1: How the free eG Enterprise Logon Simulator for Citrix works

The process depicted by Figure 1.1 is described below:

1. The simulator first opens the Chrome browser 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 launch 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 automatically reports the metrics to a cloud-hosted eG management server, which publishes the metrics on the Logon Simulator portal. The communication between the simulator (i.e., the Logon Simulator Agent) and the eG management server is over the secure, web-based HTTP/S protocol. The other key features of this communication are as follows:

- **One-way communication:** The Logon Simulator Agent does not listen on any TCP port and initiates all communication to the eG management server; this minimizes the security risk to the systems hosting the agent.
- **Firewall-friendly architecture:** Since all the communication is web-based, and since the agent initiates all communications to the manager, as long as users within your network can browse the

web from the systems on which the agents are deployed, the agents will be able to communicate with the management server without needing any additional firewall configuration.

- **Monitoring support for multiple private networks:** Since the Logon Simulator Agent initiates all the communications, it can even be installed on systems that are assigned private IP addresses, and on networks that are behind network address translation (NAT) devices. That is, you do not have to have your agents on the Internet to use this service - the agents can be in your Intranet.
- **Multi-tenancy support:** Support for multi-tenancy is built in. Users receive personalized logins and they can monitor the logon performance of only their Citrix delivery infrastructure.
- **Does not carry business-sensitive information:** This free simulator does not monitor business-related information (credit card information, etc.), and the information transmitted between the agent and the manager can be audited by the IT administrators at any time, using packet sniffers.
- **Secure, authenticated access:** Your data is securely maintained and all accesses to the service are authenticated. You only have access to metrics, alerts, and reports from your infrastructure.

1.4 Pre-requisites for the eG Enterprise Express Logon Simulator for Citrix

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

Category	Pre-requisites
Logon Simulator Agent / Simulation Endpoint	<ul style="list-style-type: none"> • The Logon Simulator Agent should be installed on a dedicated endpoint. The dedicated endpoint should only run on an English version of Windows operating system. • No other eG agent should exist on the same host on which the Logon Simulator Agent has been installed. • .Net Framework 4.5 (or above) should pre-exist on the system hosting the Logon Simulator Agent. • Citrix Receiver version 2.x (also referred to as v12.x) and above or Citrix Workspace App should be installed on the system hosting the Logon Simulator Agent. Take care to install the Receiver/Workspace App in the default location only. <p>Note:</p>

- Ensure that you install the Standard or full version of the Citrix Receiver/Citrix Workspace App. Citrix Receiver/Citrix Workspace App installed as a plugin is not supported.
- The simulator requires a dedicated Citrix test account with rights to launch applications/desktops.
- The simulator also requires a user account with local administrator rights on the simulation endpoint - i.e., on the system hosting the Logon Simulator Agent / Citrix Receiver / Citrix Workspace App. 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.

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 bundled into the logon simulator agent package. Once you download and extract the package into any location, you will find the RDPSessionInteractiveTask.exe within.

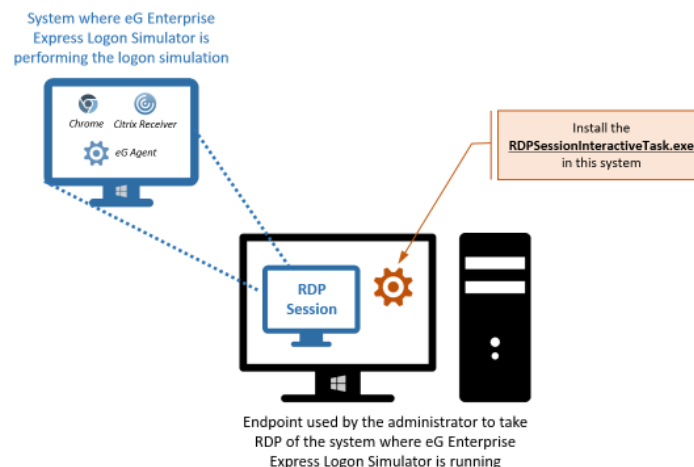


Figure 1.2: Logon Simulation performed via an RDP session

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

	<p>execution, a message to that effect will appear.</p> <ul style="list-style-type: none"> • Reconnect the RDP session. <p>Note:</p> <ul style="list-style-type: none"> • 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/Workspace App processes will be killed, so existing sessions will be disconnected. • If the Citrix Receiver/Citrix Workspace App has created a system tray icon on the simulation endpoint, then make sure it is removed.
Environment	<ul style="list-style-type: none"> • The simulator will only work with Citrix XenApp / XenDesktop 6.x and 7.x environments and Citrix Cloud. • 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. • The eG Enterprise Logon Simulator for Citrix can be used to simulate logons to both on-premises Citrix installations and those on the Citrix Cloud or Citrix Workspace. Typically, 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/Citrix Workspace App 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-premises, 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 used for the simulation, or the Citrix Delivery

	<p>Controller, if Citrix XenDesktop v7.x is used.</p> <p>In simulations performed on the Citrix Workspace or on the Citrix Cloud on the other hand, the eG Logoff Helper is not required. In this case, the eG agent itself automatically logs off the simulated application/desktop sessions.</p> <ul style="list-style-type: none"> • 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. You can auto subscribe users to applications by setting "KEYWORDS:Auto" in the published application's description in the Citrix XenDesktop Broker. 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. • 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.
Browser	<p>The eG Enterprise Express Logon Simulator for Citrix mandates the presence of the Chrome browser v98 (and above). No other browser supports this simulation.</p> <p>Note:</p> <p>Chrome is capable of automatically applying updates and upgrading itself to higher versions. Sometimes, when Chrome auto-upgrades, some drivers that the eG Logon Simulator Agent uses may suddenly be rendered incompatible with Chrome. This can cause problems in simulation. To avoid this, the eG Enterprise Express Logon Simulator for Citrix, by default, prevents Chrome upgrades/updates (both automatic and manual) from being applied at the simulation endpoint.</p> <p>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</p>

	<p>simulation endpoint allows Chrome upgrades. To achieve this, before manually upgrading Chrome, follow the steps below:</p> <ul style="list-style-type: none"> • 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: <p>ChromeUpgradeHandler.exe enable</p>
--	--

Caveat:

Users can access their Citrix environments through different means. Users within the Citrix environment use the Citrix StoreFront to access the Citrix hypervisors and applications whereas users accessing the Citrix environment from remote/external locations use the Citrix NetScaler. Some Citrix environments may also use F5 load balancers through which the users can access their environments. Citrix NetScaler can be integrated with additional authentication mechanisms (single sign-on systems) such as OKTA, Azure AD, AD FS. The Citrix Logon Simulator is capable of simulating the transactions when the Citrix NetScaler is integrated with authentication mechanisms such as Microsoft Azure AD and AD FS.

1.5 Installing and Configuring the eG Enterprise Express Logon Simulator for Citrix

To install and configure the eG Enterprise Express Logon Simulator for Citrix, follow the broad steps below:

1. [Subscribe to the Simulation Service](#)
2. [Configure the Simulation](#)
3. [Download and install the Logon Simulator Agent](#)
4. If your simulation is performed on-premises, then [deploy the light-weight eG Logoff Helper](#) software to enable proper application/desktop logoffs.

The sections that follow will discuss each of these steps elaborately.

1.6 Subscribe to the Simulation Service

For this, first connect to <https://logonsimulator.eginnovations.com>. Figure 1.3 will appear.

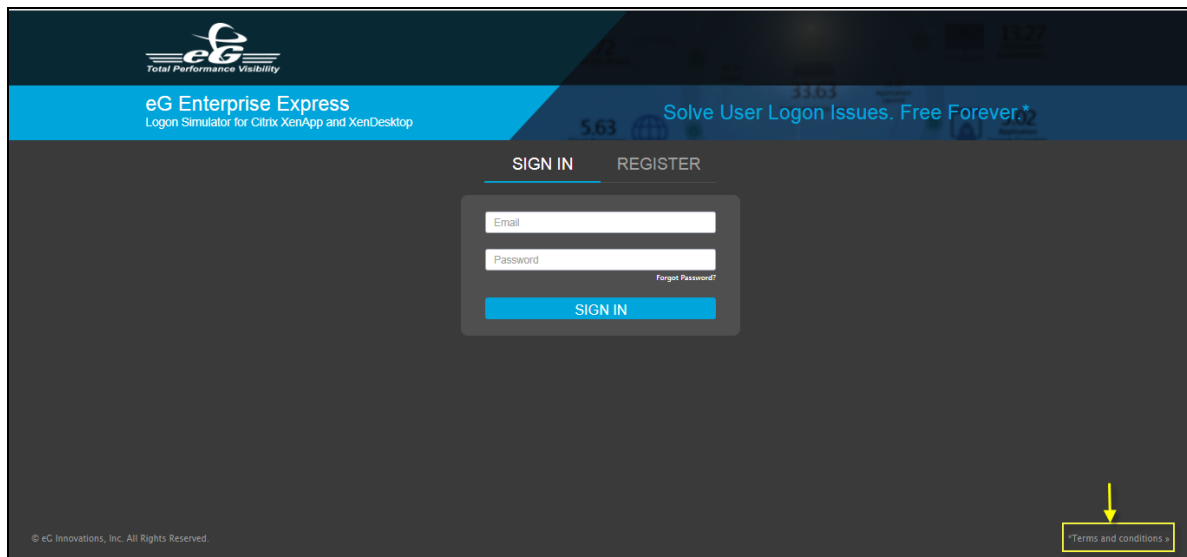


Figure 1.3: Connecting to the URL: logonsimulator.eginnovations.com

If you are an existing subscriber to the service, you can sign in using the **Email ID** and **Password** you provided at the time of registering. If you are a first time user and want to subscribe to the service, first take a look at the terms and conditions of the service by clicking the **Terms and conditions** link at the bottom right corner of the **SIGN IN** page (as indicated by Figure 1.3). Figure 1.4 will then appear.

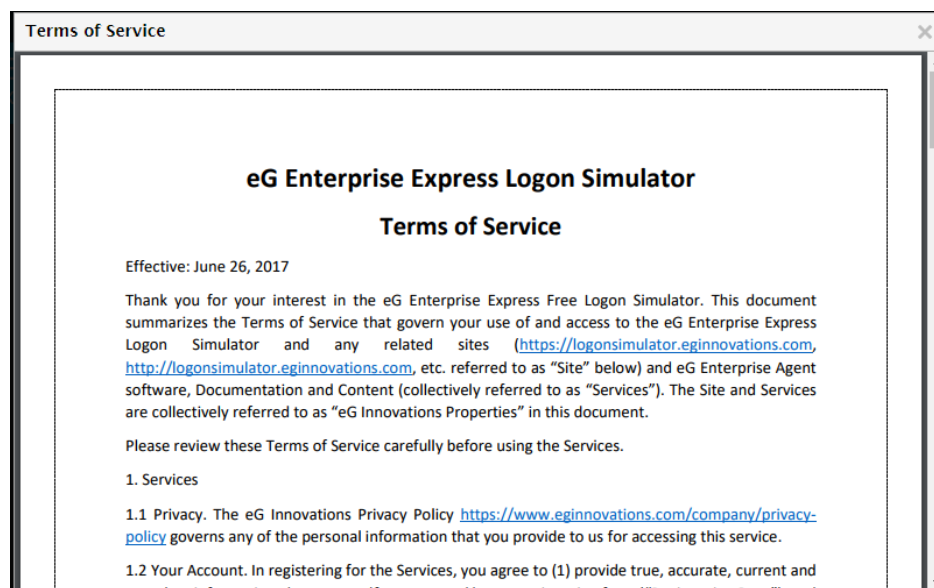


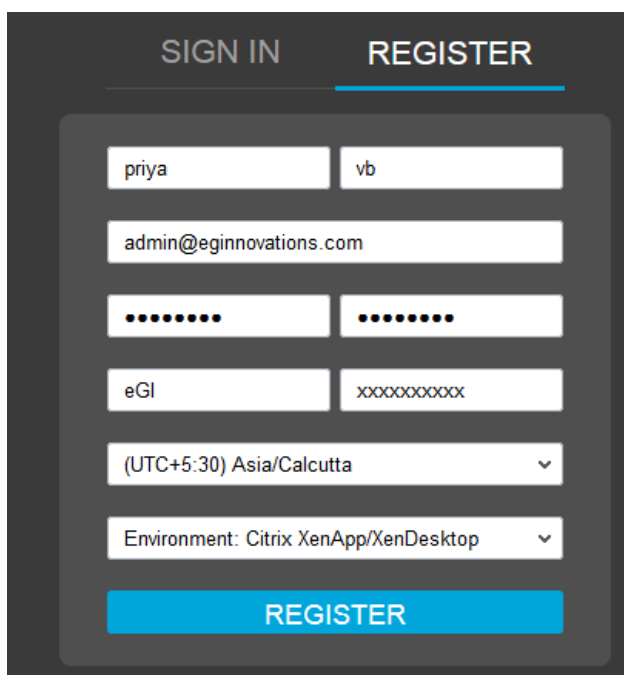
Figure 1.4: Terms and conditions of service

After reading the terms and conditions of service, close the window and return to the **SIGN IN** page of Figure 1.3. Then, to register, click on the **REGISTER** link in Figure 1.3. When Figure 1.5 appears, provide your First name, Last name, your valid Email ID and a unique password for logging in.

Note:

For using eG Enterprise Express Logon Simulator for Citrix, a valid corporate email address should be used during registration. The free logon simulator service will accept registrations of up to three (3) unique email addresses per email domain. Not more than three (3) unique user accounts can be created per valid corporate email domain.

Also, specify your company name, pick a Time zone, and enter your phone number. eG Enterprise offers eG Enterprise Express Logon Simulator for both Citrix XenApp/XenDesktop and VMware Horizon. Select the environment for which you wish to configure the simulations from the **Environment for Logon Simulation** list. In our case you need to choose **Environment: Citrix XenApp/XenDesktop** from this list. Finally, click **REGISTER** to subscribe to the free service.



The image shows a registration form with a dark background. At the top, there are two tabs: "SIGN IN" and "REGISTER", with "REGISTER" being the active tab. Below the tabs, there are several input fields: a first name field containing "priya", a last name field containing "vb", an email field containing "admin@eginnovations.com", two password fields each containing seven dots, a company name field containing "eGI", and a phone number field containing "xxxxxxxxxx". Below these fields are two dropdown menus: the first shows "(UTC+5:30) Asia/Calcutta" and the second shows "Environment: Citrix XenApp/XenDesktop". At the bottom of the form is a large blue button labeled "REGISTER".

Figure 1.5: Signing up to use the eG Enterprise Express Logon Simulator for Citrix

A Verification code will be sent to the email address you specified in Figure 1.5. Upon receipt of the code, copy and paste it in Figure 1.6 and click **Verify**.

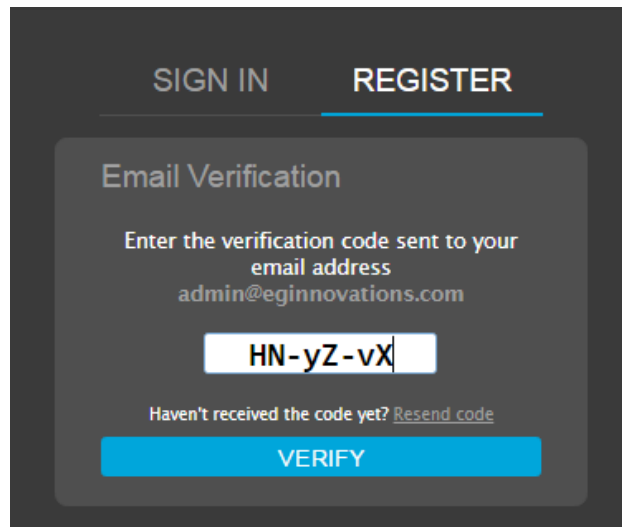


Figure 1.6: Specifying the verification code sent by email

Once the code is successfully verified, Figure 1.7 will appear, detailing the next steps for using this simulator.



Figure 1.7: Home page of the eG Enterprise Express Logon Simulator for Citrix portal

1.7 Configure the Simulation

For this, click **Configure** in Figure 1.7 . Figure 1.8 will then appear.

The screenshot shows the 'LOGON SIMULATOR' window with three tabs: 'Choose Simulator', 'Configure Simulation' (active), and 'Download Agent'. The 'Configure Simulation' tab contains the following fields and options:

- Simulator:** A dropdown menu showing 'Citrix Logon Simulator'.
- Site URL:** A text box containing 'http://192.168.11.4/Citrix/SIMWeb'.
- Is this service hosted on Citrix Cloud?:** Radio buttons for 'Yes' and 'No', with 'No' selected.
- Application/Desktop:** A text box containing 'notepad.notepad' with a gear icon to its right.
- Domain:** A text box containing 'egin'.
- User:** A text box containing 'xenadmin'.
- Password:** A text box with masked characters '*****'.
- Confirm Password:** A text box with masked characters '*****'.
- Is 2FA enabled?:** Radio buttons for 'Yes' and 'No', with 'Yes' selected.
- Is disclaimer enabled?:** Radio buttons for 'Yes' and 'No', with 'Yes' selected.


At the bottom of the window are three buttons: 'Add More', 'Update', and 'Clear'.

Figure 1.8: Configuring the simulation

Provide the following inputs in Figure 1.8:

1. **Site URL:** The URL of the StoreFront/NetScaler/Web interface that it needs to access

Note:

- The eG Enterprise Express Logon Simulator for Citrix supports only up to one (1) Citrix farm URL
 - Only StoreFront 2.0 (or above) and NetScaler Gateway v9.3 (or above) are supported.
2. **Is this service hosted on Cloud?:** If your Citrix environment is hosted on a Citrix Cloud (Citrix WorkSpace), then, set this flag to **Yes**. By default, this flag is set to **No**.
 3. **Application/Desktop:** The names of the applications/desktops to be launched. To provide the application/desktop names, click the  icon alongside the **Application/Desktop** text box. Figure 1.9 will then appear.

Tab Name	Application/Desktop Name	Window Title
none	notepad	notepad
Apps	winword	winword

Buttons: Add More, Update, Clear

Figure 1.9: Configuring the names of applications/desktops to be launched

Specify the following in Figure 1.9:

- 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 must specify the exact **Tab Name** of the tab page in which that application/desktop is present.
- Application/Desktop Name:** Specify the 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:

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 that will be displayed for the configured **Application/Desktop** in the session window's title bar.

Finally, click the **Add More** button in Figure 1.9 to add more applications/desktops to be launched. A maximum of three applications/desktops can only be configured for the simulation. If you do not want to add any more applications/desktops, click the **Update** button in Figure 1.9 to save the changes and exit the **CONFIGURE APPLICATION/DESKTOP** window. You will then return to Figure 1.8, where you can proceed to provide the other details required for the simulation.

4. **Domain, User, Password, and Confirm Password:** Provide the credentials of a user who is authorized to launch the configured applications/desktops.

Note:

- The eG Enterprise Express Logon Simulator for Citrix supports a maximum of only three (3) users for logon simulation.
 - 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.
5. **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 and TOTP - based dynamic 2FA is supported for user authentication. If dynamic 2FA (TOTP) is used for user authentication, then, you may need to specify the secret key obtained while registering the logon simulation endpoint device as a TOTP device against the text box that appears when you set this flag to **Yes**. Once the device is registered, during every simulation, the logon simulator will automatically generate the TOTP code based on the specified secret key. To know how to register the Logon simulation endpoint device and obtain the secret key for generating TOTP automatically, refer to **Section 1.7.1**.

6. **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**.

Click **Add More** if you want to configure more simulations. However, the eG Enterprise Express Logon Simulator for Citrix supports a maximum of three (3) **Users** only for the logon simulation. Likewise, a maximum of only three applications/desktops can be launched by the eG Enterprise Express Logon Simulator. At any point in time, click **Update** to save the changes.

1.7.1 Generating Secret Key for TOTP based User Authentication

In order to generate a secret key for TOTP-based dynamic 2FA, you need to first register your logon simulation endpoint on a Citrix NetScaler Gateway or Citrix Workspace or Citrix NetScaler Gateway/Citrix Workspace integrated with Microsoft Azure AD. Let us now discuss elaborately on how to register your logon simulation endpoint and generate the secret key using Citrix NetScaler Gateway, Citrix Workspace and Microsoft Azure AD in the forthcoming sections.

1.7.1.1 Registering the Logon Simulation Endpoint on Citrix NetScaler Gateway

To register your logon simulation endpoint on on-premises Citrix NetScaler Gateway and generate a secret key, follow the instructions mentioned below:

1. Open any browser and navigate to the URL: `https://<Fully Qualified Domain Name of the Citrix NetScaler ADC>/manageotp`. For example, your URL can be: `https://xendesk7v1912.eginnovations.com/manageotp`. Figure 1.10 will then appear.

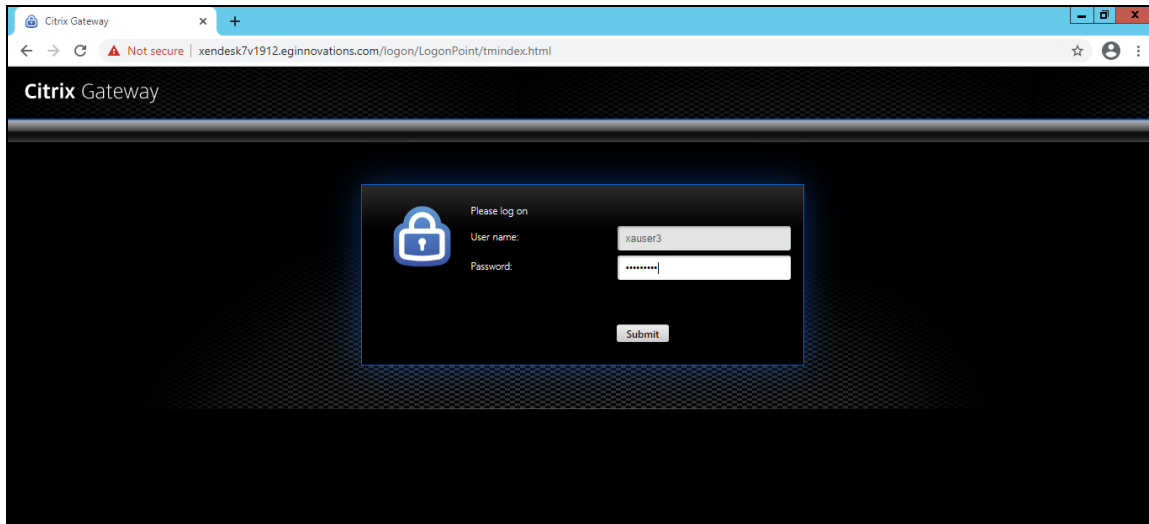


Figure 1.10: Logging in through the on-premises Citrix NetScaler Gateway

2. In Figure 1.10, specify the credentials of the user who is authorized to perform the logon simulation and click the **Submit** button. Figure 1.11 then appears.

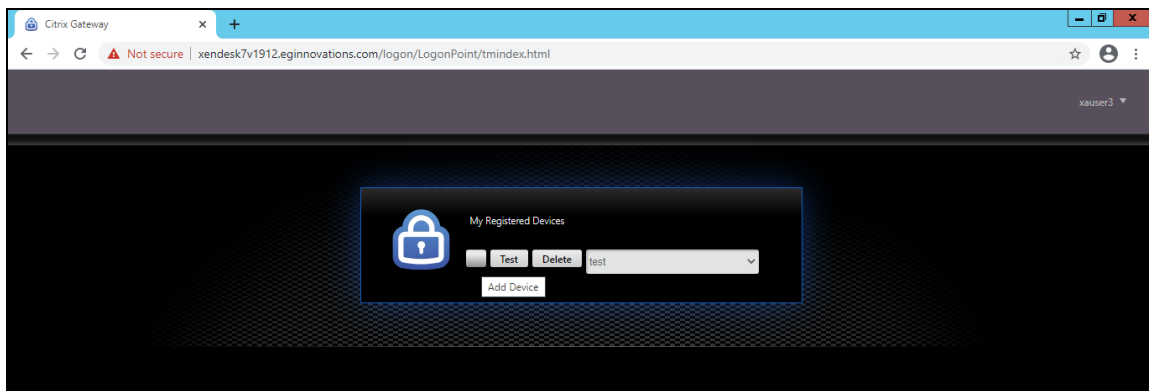


Figure 1.11: The Add Device button

3. Clicking the **Add Device** button in Figure 1.11 will reveal Figure 1.12. Here, specify the name of the device i.e., the name of the logon simulation endpoint that you wish to register in the text box that appears alongside the **Go** button.

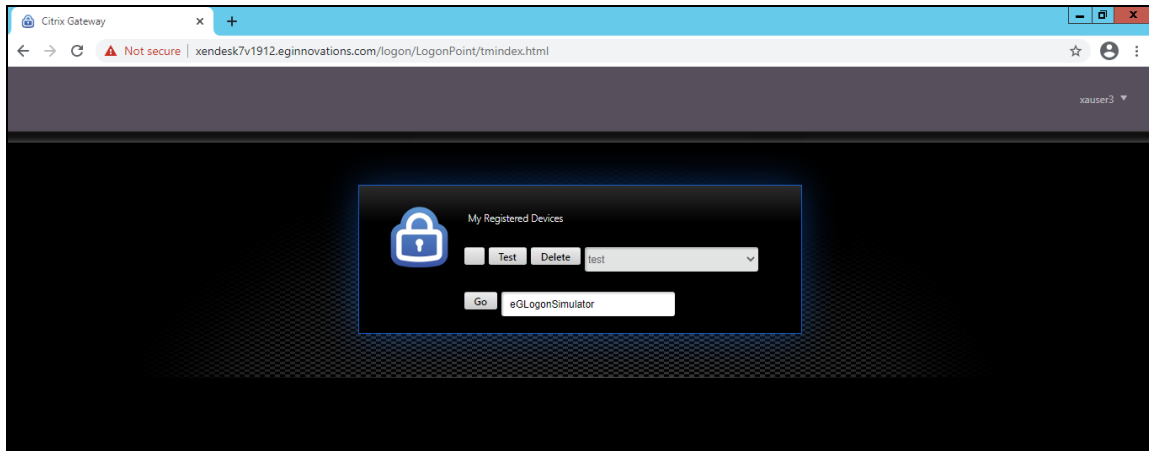


Figure 1.12: Specifying the name of the device that is to be registered

- Once you have specified the name of the device, click the **Go** button. A 16 digit secret key along with a QR code will appear as shown in Figure 1.13. Ensure that you note down this secret key as this should later be specified in the text box that appears when you set the **Is 2FA enabled?** flag to **Yes** while configuring the simulation.

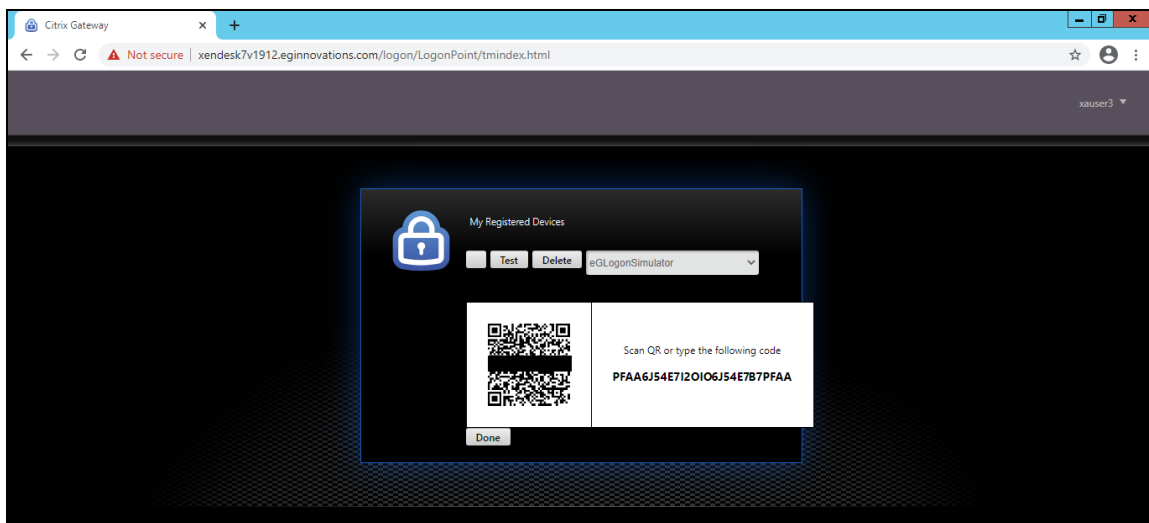


Figure 1.13: QR code and Secret Key displayed for the registered endpoint

- Clicking the **Done** button in Figure 1.13 will ensure that your device has been successfully registered with the Citrix NetScaler Gateway.

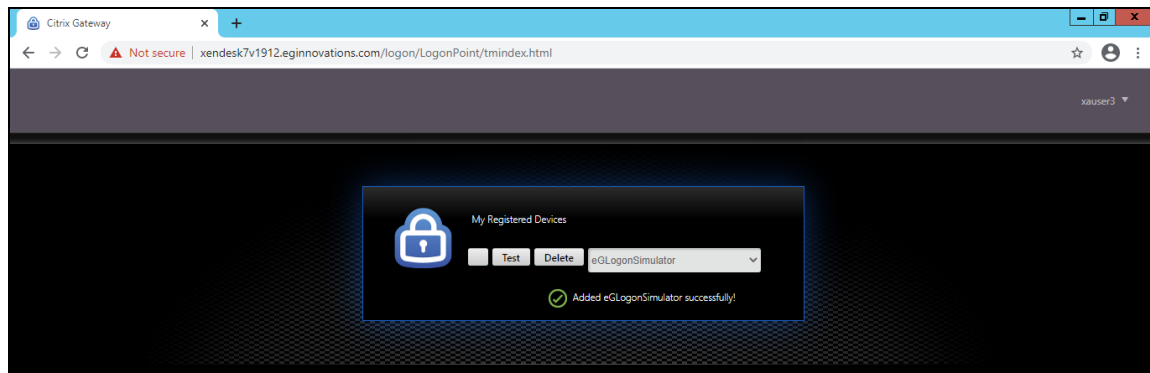


Figure 1.14: A message stating that the registration is successful

1.7.1.2 Registering the Logon Simulation Endpoint on Citrix Workspace

To register your logon simulation endpoint on Citrix Workspace and generate a secret key, follow the instructions mentioned below:

1. Open any browser and hit the site URL of the Citrix Workspace in your environment. Figure 1.15 then appears. To register the logon simulation endpoint on Citrix Workspace, the user who is authorized to perform logon simulation should possess a valid token. To generate this token, click on the **Don't have a token?** link in Figure 1.15.

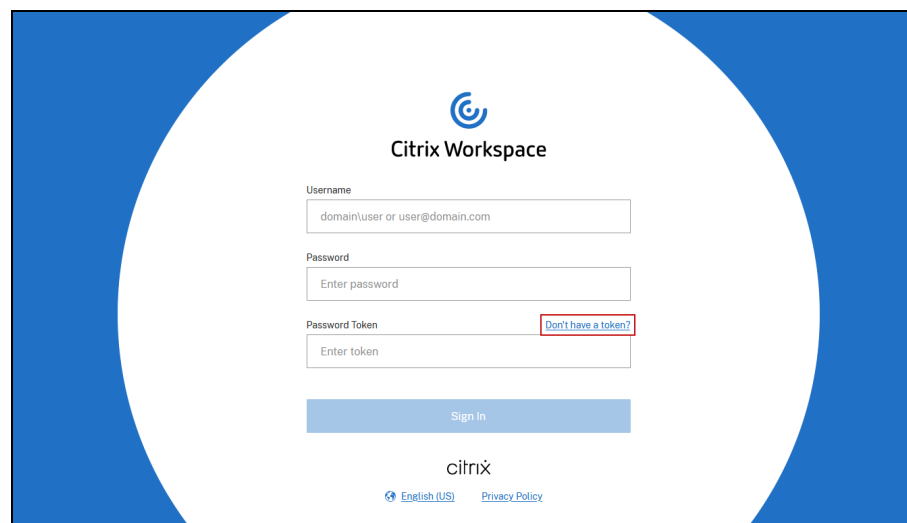


Figure 1.15: Proceeding to generate a Password Token

2. In Figure 1.16 that appears, specify the name of the user who is authorized to perform logon simulation in the **Username** text box. As soon as the **Next** button is clicked, a verification code

will be sent to the email ID of the specified user.

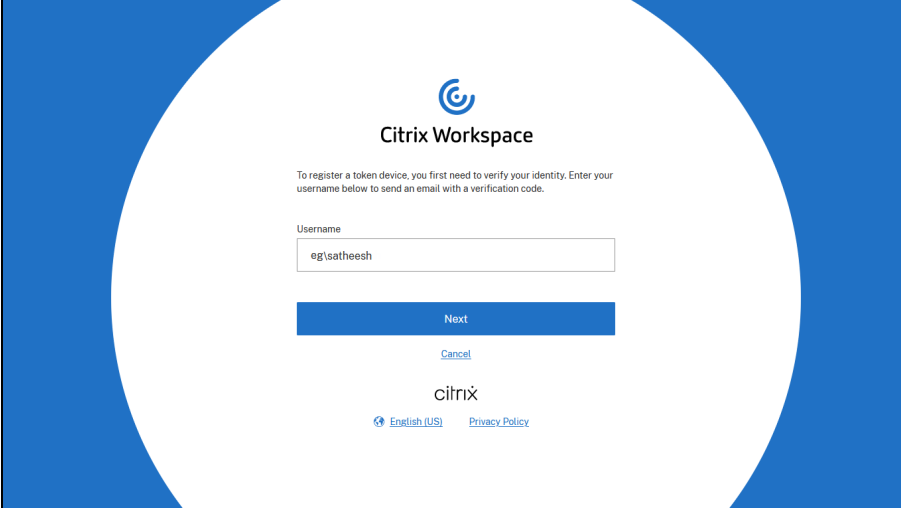
The image shows the Citrix Workspace registration interface. At the top, the Citrix logo is displayed above the text "Citrix Workspace". Below this, a message states: "To register a token device, you first need to verify your identity. Enter your username below to send an email with a verification code." There is a text input field labeled "Username" containing the text "eg@satheesh". Below the input field is a blue "Next" button. A "Cancel" link is positioned below the "Next" button. At the bottom, the Citrix logo is shown again, along with links for "English (US)" and "Privacy Policy".

Figure 1.16: Specifying the name of the user who is authorized to perform logon simulation

3. In Figure 1.17 that appears, specify the **Verification Code** received by email and the password corresponding to the user who is authorized to perform the simulation.

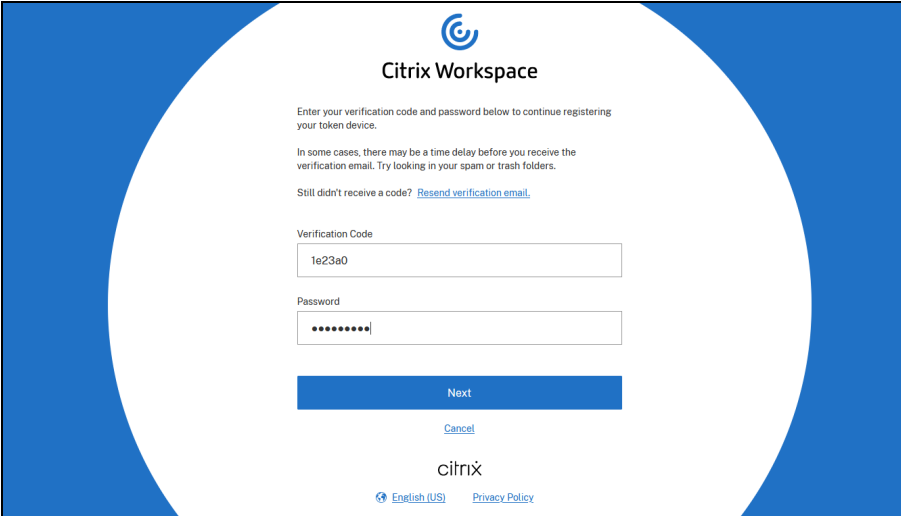
The image shows the Citrix Workspace registration interface for the verification step. At the top, the Citrix logo is displayed above the text "Citrix Workspace". Below this, a message states: "Enter your verification code and password below to continue registering your token device." A second message reads: "In some cases, there may be a time delay before you receive the verification email. Try looking in your spam or trash folders." Below these messages is a link: "Still didn't receive a code? [Resend verification email.](#)". There are two input fields: "Verification Code" containing "1e23e0" and "Password" containing "*****". Below the input fields is a blue "Next" button. A "Cancel" link is positioned below the "Next" button. At the bottom, the Citrix logo is shown again, along with links for "English (US)" and "Privacy Policy".

Figure 1.17: Specifying the Verification Code and Password

4. Clicking the **Next** button will lead you to Figure 1.18 which reveals the QR code and the secret key for the registered logon simulation endpoint. Ensure that you note down this secret key as this should later be specified in the text box that appears when you set the **Is 2FA enabled?** flag to **Yes** while configuring the simulation.

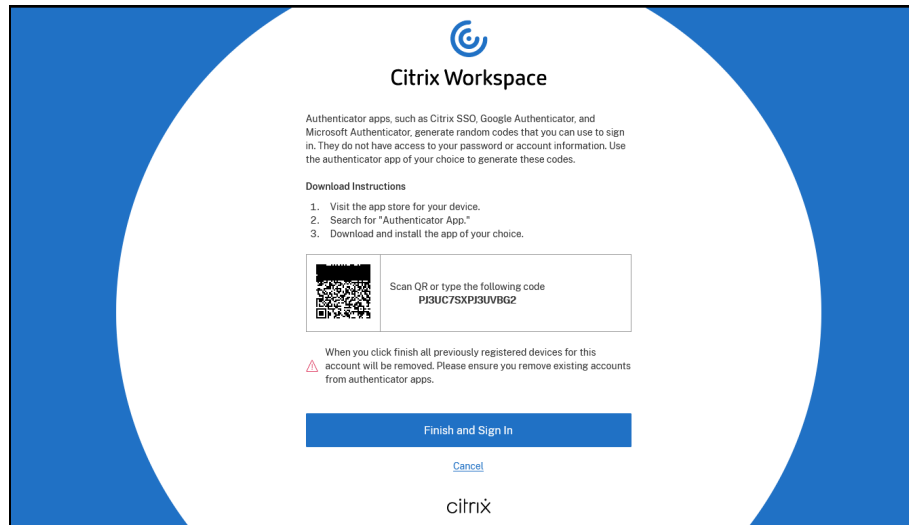


Figure 1.18: QR code and secret key displayed for the registered endpoint

5. Clicking the **Finish and Sign In** button will ensure that your logon simulation endpoint is registered and is ready for monitoring.

1.7.1.3 Registering the Logon Simulation Endpoint as an Application to generate OATH Soft token in Microsoft Azure AD

Prior to registering the logon simulation endpoint, you need to download and install an Authenticator App (for e.g., Microsoft Authenticator, Google Authenticator, Citrix SSO) on your mobile from Android Play Store or Apple Store based on the operating system of your mobile.

If the user who is authorized to perform logon simulation belongs to Microsoft Azure Active Directory, then, you may need to follow the steps mentioned below to register the logon simulation endpoint and generate a secret key/code.

1. Log in to the URL: **https://<Fully Qualified Domain Name of Microsoft Office 365 site in your environment>/securityinfo** with the credentials of the user who is authorized to perform logon simulation. Figure 1.19 then appears.

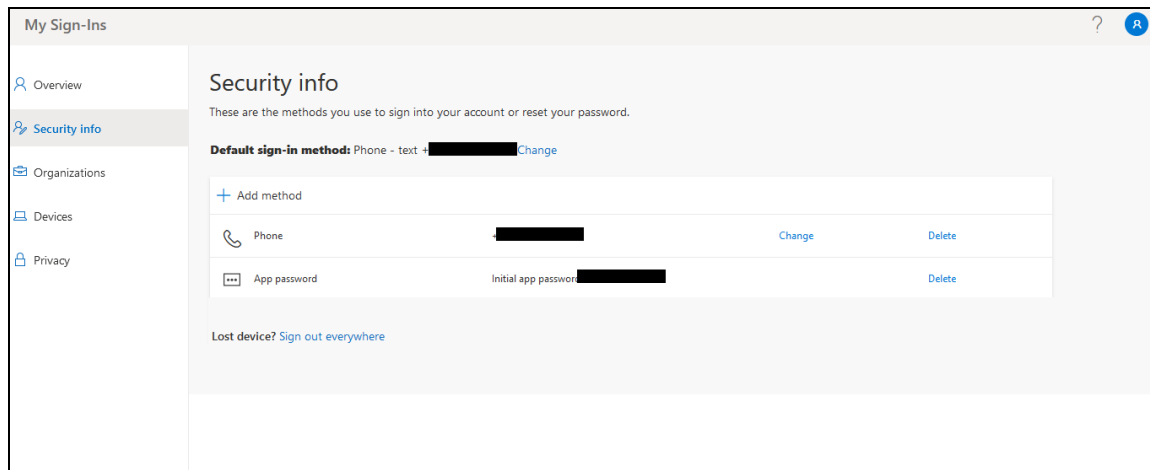


Figure 1.19: Logging into the Microsoft Office 365 site URL

2. In Figure 1.19, click the Add method. This will invoke the Add a method pop up window as shown in Figure 1.20.

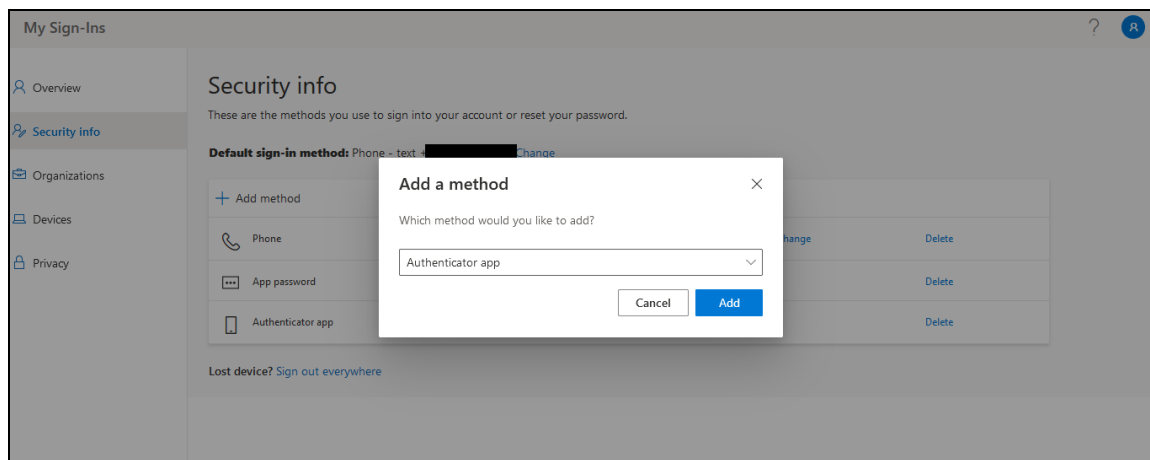


Figure 1.20: The Add a method pop up window

3. In Figure 1.20, choose **Authenticator App** from the **Which method would you like to add?** drop-down list and click the Add button. Figure 1.21 then appears.

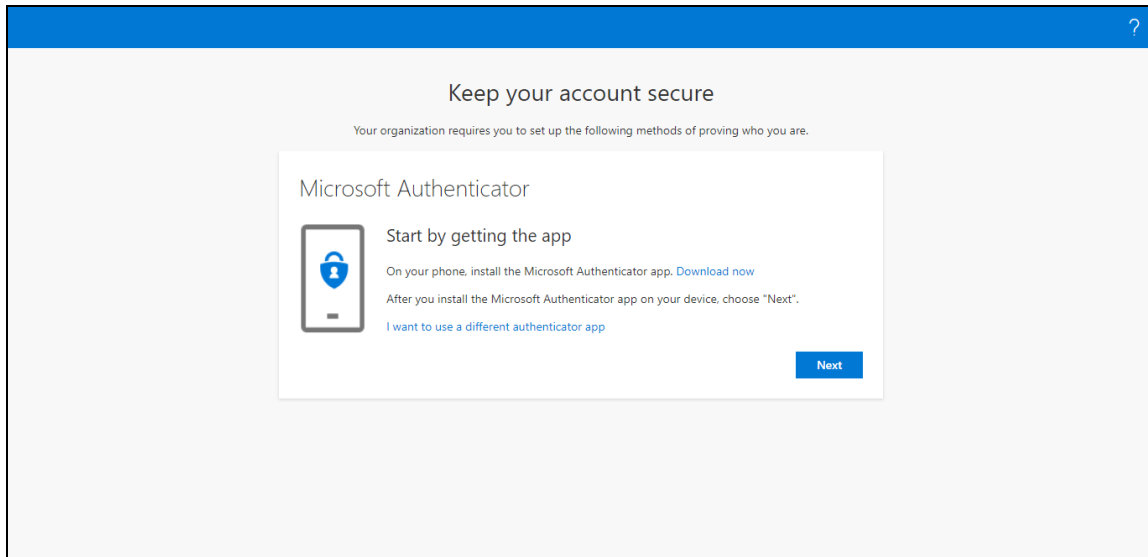


Figure 1.21: Choosing to use a different authenticator app

4. In Figure 1.21, click the **I want to use a different authenticator app** link and click the **Next** button. This will start setting up the account for the authenticator app.

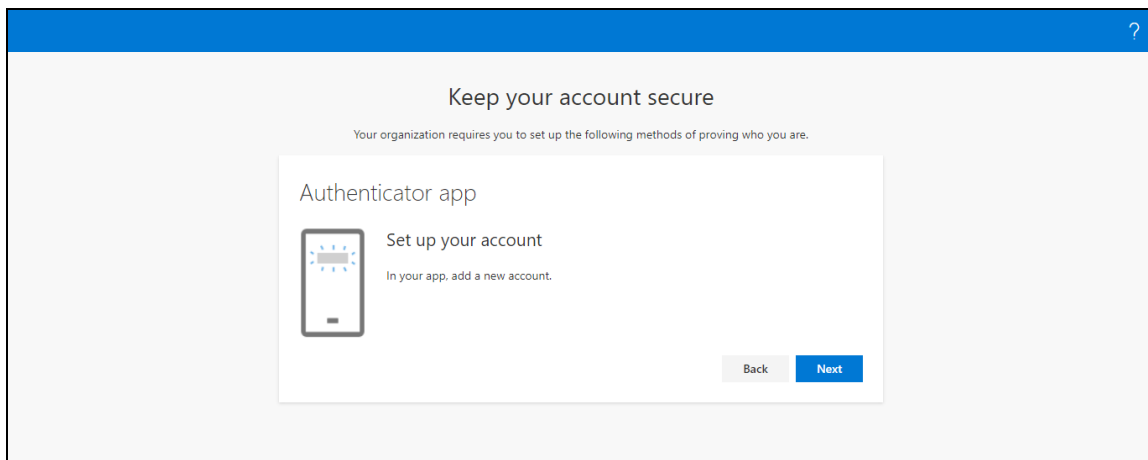


Figure 1.22: Setting up your account for a different authenticator app

5. Clicking the **Next** button in Figure 1.22 will reveal the QR code and secret key as shown in Figure 1.23. Ensure that you note down this secret key as this should later be specified in the text box that appears when you set the **Is 2FA enabled?** flag to **Yes** while configuring the simulation.

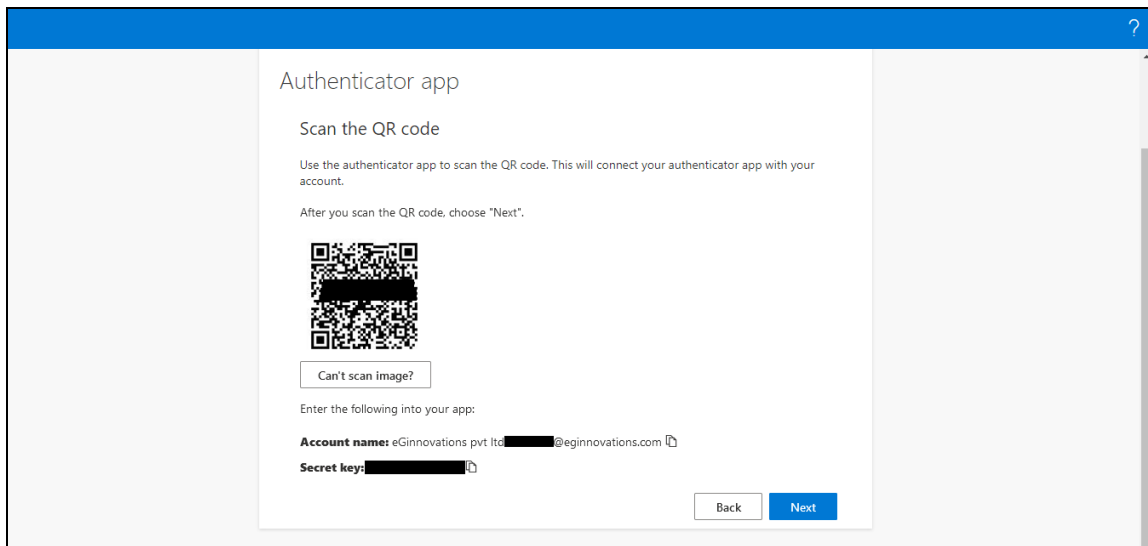


Figure 1.23: QR code and secret key displayed for the registered endpoint

6. Clicking the **Next** button will lead you to Figure 1.24 where you will be required to enter the passcode generated on your Authenticator App. This is an additional layer of security that is required for registering the logon simulation endpoint. In our example, to generate the passcode, the QR code/Secret Key shown in Figure 1.23 is scanned using/entered in the Microsoft Authenticator App.

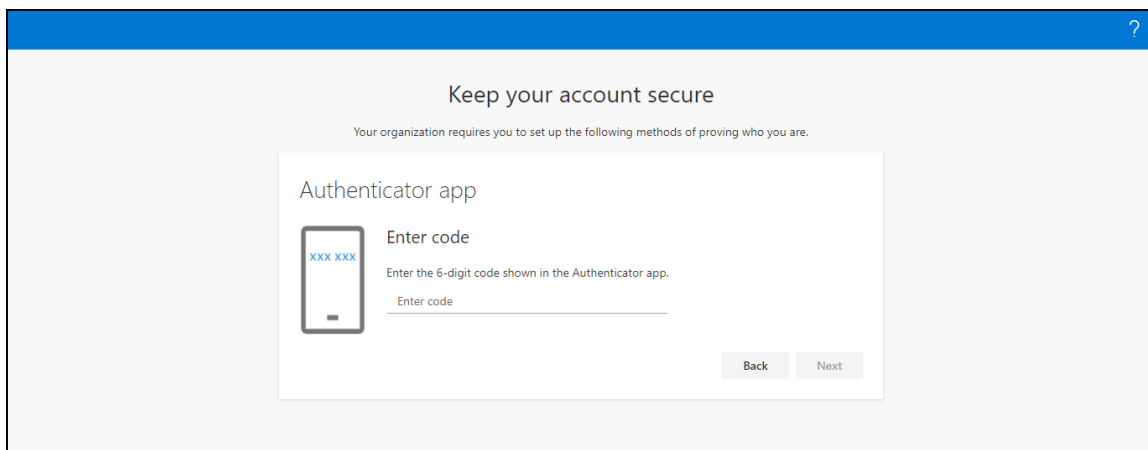


Figure 1.24: Authenticating the user credentials with a passcode from the Authenticator App

7. Once the code is specified in Figure 1.24, clicking the **Next** button will ensure that your logon simulation endpoint is successfully registered as shown in Figure 1.25.

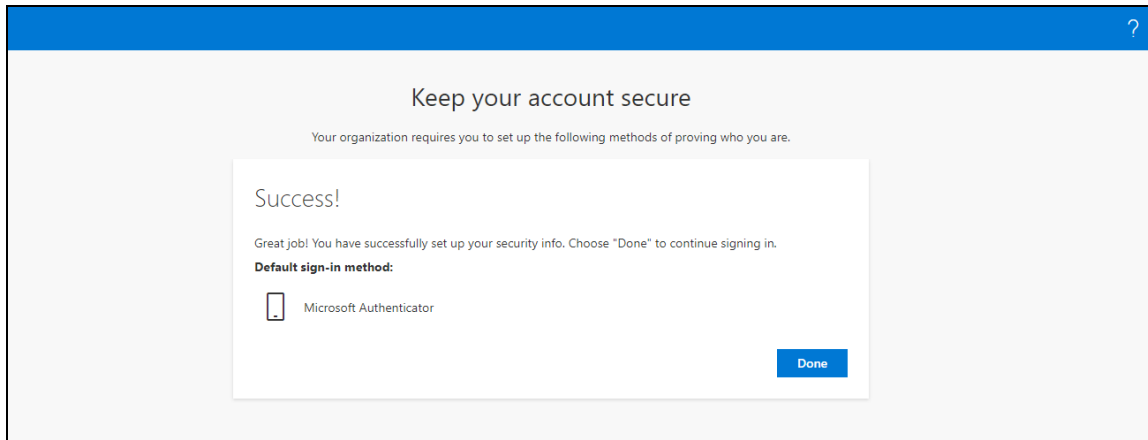


Figure 1.25: A message stating that the logon simulation endpoint registration is successful

8. Once the logon simulation endpoint registration is successful, you are required to set the Authenticator App as the default sign in method in your Microsoft Office 365 account. For this, you need to navigate to the Security Info page and click the **Change** link against the **Default sign-in method:** label (see Figure 1.26).
9. The **Change default method** pop up window will then be invoked. Here, select the **Authenticator app or hardware token - code** option from the **Which method would you like to use to sign in?** list.

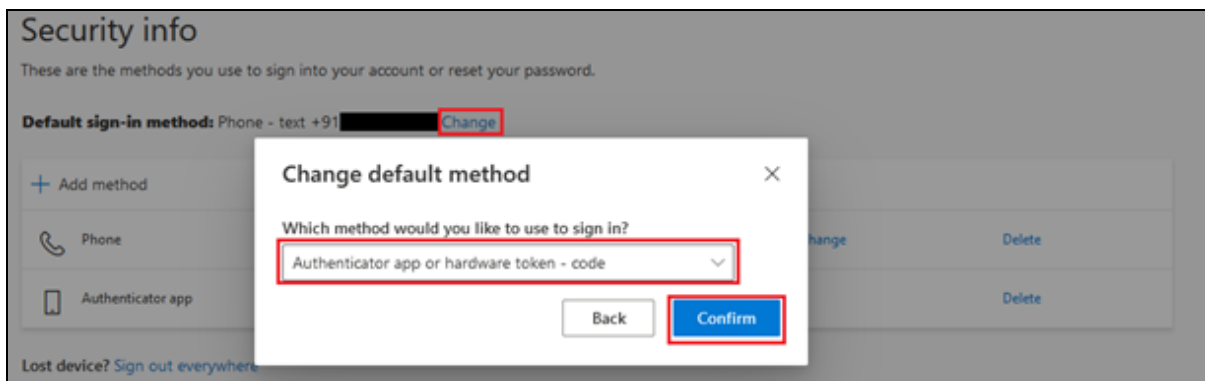


Figure 1.26: Changing the default sign in method

10. Clicking the **Confirm** button will ensure that your logon simulation endpoint is registered and is ready for monitoring.

1.8 Download and Install the Logon Simulator Agent

Click on **Download Agent** tab page in Figure 1.8 in the **Configure the Simulation** topic to download and install the Logon Simulator Agent. From the list of agent packages displayed in the tab

page (see Figure 1.27), click on the package that suits your environment.

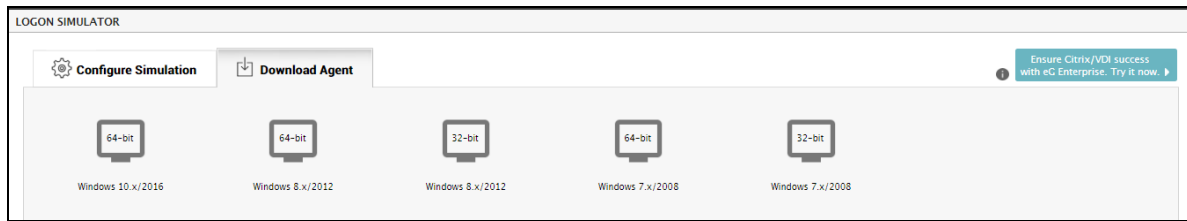


Figure 1.27: Downloading and installing the Logon Simulator Agent

A zip file will be downloaded to the location you specify. Extract the contents of the zip to any folder of your choice. Run the **setup.bat** file (in that folder) as administrator to install and configure the agent.

Note:

If the Logon Simulator Agent communicates with the Logon Simulator Portal via a Proxy server, then make sure you follow the procedure detailed in **Section 1.8.1** to install and configure the Logon Simulator Agent.

Setup will first check whether the target agent host fulfills all pre-requisites for simulation. If setup finds that a pre-requisite has not been fulfilled, it will highlight the failure in Red (as shown by Figure 1.28).

```
eG Express Logon Simulator for Citrix - Prerequisites Check for Chrome
-----
Login User: EGLAP0174-PC\Satheesh
Session ID: 2
Local Administrator Privileges for the Login User: Enabled
Registry Access Permission for the Current User: Allowed
Operating System Language: Supported
.NET Framework: Installed
Chrome Browser: Not Installed
Action: Please install the latest Chrome Browser.
Citrix Receiver/Workspace App: Installed
ICA Client Registry Settings: Enabled
eG Logon Simulator Agent communication with eG SaaS Portal: Successful
ACTION: Please ensure that all the prerequisites are met.
```

Figure 1.28: Setup script where a pre-requisite has failed

Use the pointers provided in Figure 1.28, just below the failed pre-requisite, to know how to fulfill that requirement. Then, rerun **setup.bat** to make sure that all pre-requisites are fulfilled, and then proceed with the installation.

Note:

- While installing the eG agent, the following registry entries will automatically be created in the simulation endpoint. If these entries are not available, then, for the simulator to interact with the

ICA object, manually add the following entries 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"

If all pre-requisites are fulfilled, then setup will prompt you to press any key on the keyboard, so that the agent installation can continue.

```
eG Express Logon Simulator for Citrix - Prerequisites Check for Chrome
-----
Login User: EGLAP0174-PC\Satheesh
Session ID: 2
Local Administrator Privileges for the Login User: Enabled
Registry Access Permission for the Current User: Allowed
Operating System Language: Supported
.NET Framework: Installed
Chrome Browser: Installed
Citrix Receiver/Workspace App: Installed
ICA Client Registry Settings: Enabled
eG Logon Simulator Agent communication with eG SaaS Portal: Successful
STATUS: All the prerequisites are met.
Note:
-----
* If the logon simulation endpoint is a VM, make sure that you run the RDPSessionInteractiveTask.exe on the system from
which you launched the RDP session to the VM.
```

Figure 1.29: All pre-requisites are fulfilled

If the agent installation is successful, then a message depicted by Figure 1.30 will appear.

```
C:\Windows\System32\cmd.exe
PLEASE DO NOT INTERRUPT THIS PROCESS.
*****
*****
The eG Application has been installed successfully!!!
*****
*****
Press any key to continue . . .

*****
Install the eGLogoffHelper on the Citrix ZDC (in case a Citrix
XenApp Server v6.5 is used), or on the Citrix Delivery
Controller (if Citrix XenDesktop v7.x is used). This helper
is required for the application/desktop logoff to occur. To
know how to install the helper, refer to The_eG_Enterprise_Express_
Logon_Simulator_for_Citrix_XenApp_and_XenDesktop document, which
will be available in the folder into which you extracted the
eG Agent zip.
*****
Press any key to continue . . .
```

Figure 1.30: Successful installation of the Logon Simulator Agent

Then, proceed to install the eG Logoff Helper. To know what is the eG Logoff Helper and how to install it, refer to [Installing the eG Logoff Helper](#) topic in **Section 1.9** of this document.

Once the agent is installed successfully, it automatically starts to perform the configured simulation.

1.8.1 Enabling the Logon Simulator Agent to communicate with the Logon Simulator Portal via a Proxy server

If the Logon Simulator Agent communicates with the Logon Simulator Portal via a proxy server, then you should ensure that the following steps are followed:

1. Download and extract the contents of the Logon Simulator agent zip file to any folder of your choice. Open the command prompt as an administrator and execute the following command:

setup.bat -proxyEnabled Yes

2. The Pre-requisites for installing the agent will then be checked as explained in **Section 1.8**. Once the agent is installed successfully, you will be required to configure the proxy server settings. For this do the following:

- Open the command prompt as an administrator.
- Navigate to the <eG_INSTALL_DIR>\eGurkha\lib directory and execute the changeAgentSettings.bat file.
- Once the file is executed, you will be asked to specify the IP/hostname and port of the Logon Simulator Portal. Here, specify the IP/Hostname as logonsimulator.eginnovations.com and the port as 80.

```
Please enter the IP/Hostname of the eG Manager to which this agent should report:
logonsimulator.eginnovations.com
Please enter the Port on the eG Manager to which this agent should report: 80
```

- Then, when prompted to indicate whether/not the eG manager is SSLEnabled, specify No. :

```
Please enter if the eG Manager is SSL enabled (Yes or No)? No
```

- Next, specify yes if the logon simulator agent should communicate with the logon simulator portal using a proxy server.

```
Should the Agent use a Proxy server to communicate with the eG Manager (Yes/No)? Yes
```

- Then, enter the credentials of the proxy server.

```
Please enter the proxy IP/Name:
```

```
Please enter the proxy port:
```

- Specify Yes if the proxy server requires user authentication.

```
Does the proxy require user authentication (Yes/No)? Yes
```

- Then, specify the user credentials through which the logon simulator agent will access the proxy server.

```
Please enter the proxy username:
```

```
Please enter the proxy password:
```

- Once you have specified the required credentials, you will see the following message in the command prompt:

```
The settings have been changed successfully!
```

```
*****
```

```
Please execute the debugon.bat to run agent in debug mode or
```

```
debugoff.bat to run agent in debug off mode
```

```
and then restart the agent to effect the changes.
```

```
*****
```

```
Press any key to continue...
```

- Execute the debugon.bat or debugoff.bat.
- Once the file is executed, restart the logon simulator agent.

1.9 Installing the eG Logoff Helper

The eG Enterprise Logon Simulator for Citrix can be used to simulate logons to both on-premises Citrix installations and those on the Citrix Cloud or Citrix Workspace. Typically, 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 Workspace App 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-premises, 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 used for the simulation, or the Citrix Delivery Controller, if Citrix XenDesktop v7.x is used.

In simulations performed on the Citrix Workspace or on the Citrix Cloud on the other hand, the eG Logoff Helper is not required. In this case, the eG agent itself automatically logs off the simulated application/desktop sessions.

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

1. Run the **eGLogoffHelper.exe** as an *Administrator* (see Figure 1.31).

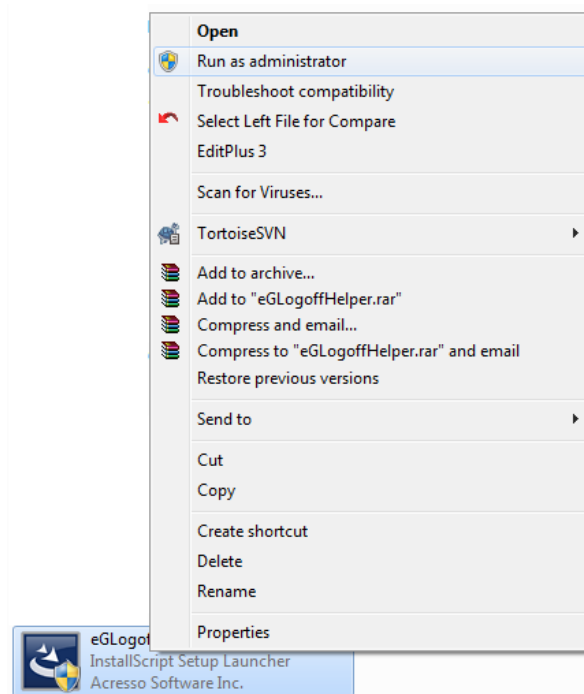


Figure 1.31: Running the eGLogoffHelper.exe as an Administrator

2. Figure 1.32 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 1.32. Then, click the **Next** button in Figure 1.32 to proceed.

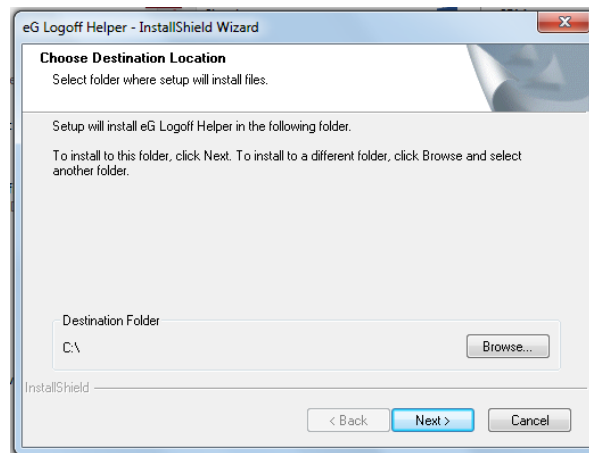


Figure 1.32: Specifying where the logoff helper is to be installed

- When Figure 1.33 appears, select **Citrix** as the infrastructure and click **Next** to move on.

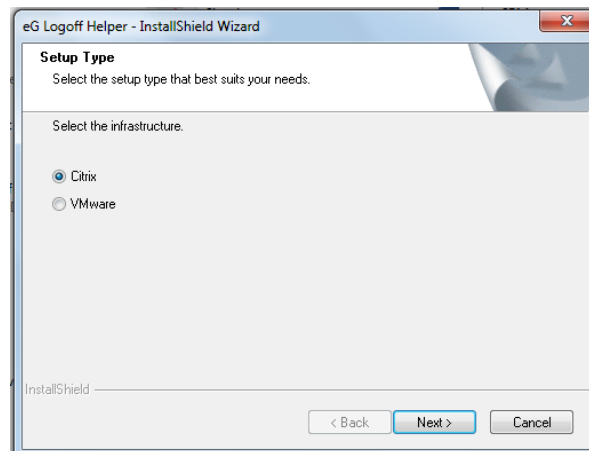


Figure 1.33: Selecting Citrix as the infrastructure

- In Figure 1.34 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>.**

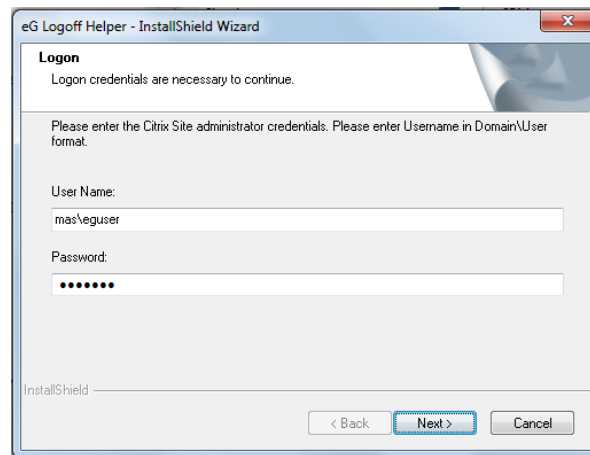


Figure 1.34: Providing the credentials of a Citrix Farm/Site administrator

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.

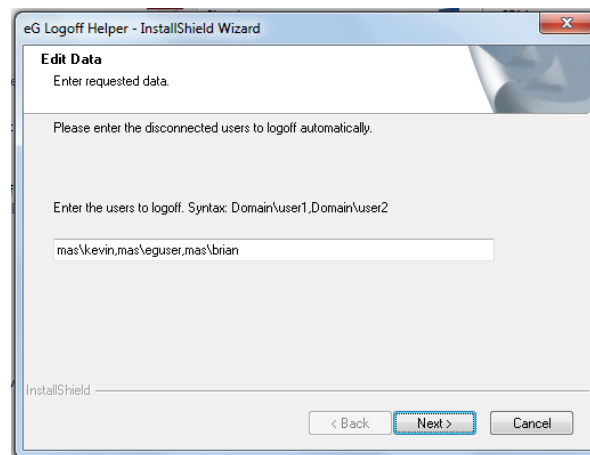


Figure 1.35: Providing a comma-separated list of application/desktop users to logoff

6. Upon successful installation of the helper, a message depicted by Figure 1.36 will appear.

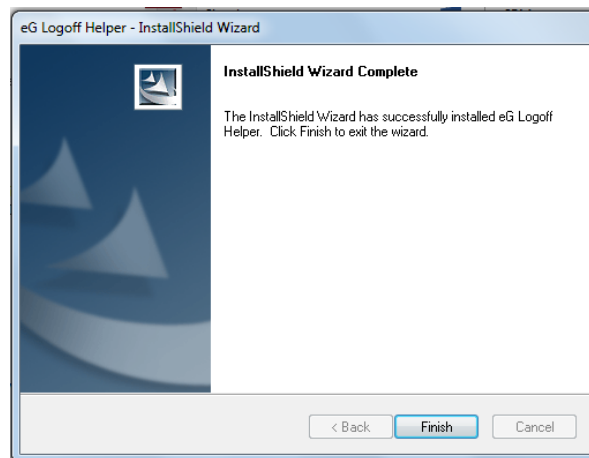


Figure 1.36: Successful installation of the logoff helper

7. Click the **Finish** button in Figure 1.36 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.

1.10 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*.

Note:

Editing the windows registry or executing the Autologon.exe will not work if the Logon Banner defined on the server either by a Group Policy object (GPO) or by a local policy appears before the login screen.

1.10.1 Fine-tuning the simulation using Autologon.exe

If you wish to automate the user login 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.

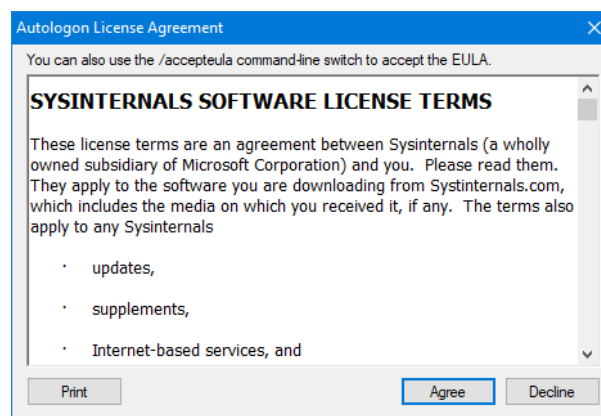


Figure 1.37: Agreeing to the Software License Terms

4. Figure 1.37 then appears. Click **Agree** to accept the Sysinternals Software License Terms.

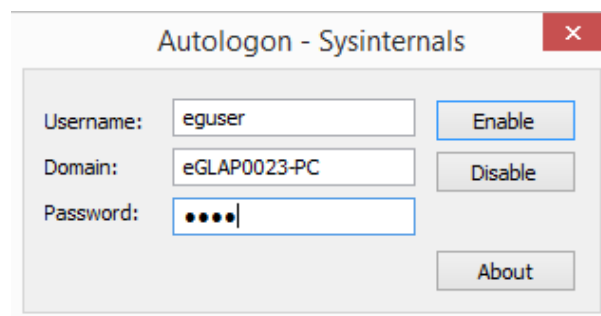


Figure 1.38: Provide the password in this form

5. In Figure 1.38 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.

1.10.2 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.

1.11 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 1.39 appears.

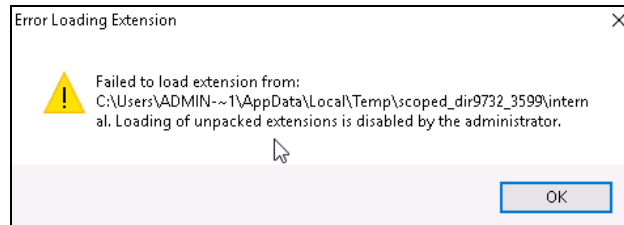


Figure 1.39: Error message that appears when chrome extensions failed to load

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.

1.12 Viewing and Interpreting the Simulation Results

Every time the Logon Simulator Agent performs a simulation, metrics on logon performance are captured and sent to the eG manager. Metrics reported per simulation are then displayed in the eG monitoring console. To view the metrics, simply click on the **Monitor** tab page in the eG user interface. A **Current Alarms** window will first appear. If any of the simulations you have configured has captured logon performance issues, then the **Current Alarms** window will report these issues.

Show	All Alarms	Filter by	Priority	Priority	All	Search	Q
	TYPE	COMPONENT NAME	DESCRIPTION	LAYER	START TIME		
<input type="checkbox"/>		Citrix Logon Si...	CtxLogonSim	Application/desktop enumeration failed ...	Citrix User Expe...	May 21, 2020 14:39	

Figure 1.40: The Current Alarms window reporting logon performance issues

Closing the **Current Alarms** window will reveal the Citrix Simulator Dashboard (see Figure 1.41).

CITRIX LOGON SIMULATIONS									
Simulator Agents:		All	Simulations						
APPLICATION/DESKTOP	SIMULATION	EXTERNAL AGENT	WEB URL	USER	SESSION HOST	WEB LOGON Availability	Duration (Secs)	ENUMERATION AVAILABILITY	APPLICATION/DESKTOP Launch
Remote Desktop	CtxLogonSim	logon_sim	https://remote.eginn...	satheesh	—	✓	8.69	✗	—
Outlook	ctx_logon_simulator	logon_sim	http://xendesk.org	citrix\cbuser	XENAPP7V6	✓	60.35	✓	9.21
Desktop_helpdesk	ctx_cloud_logon_sim	Xchag_sim_9.39	https://abccorp.x...	egin\vduser1	Desktop_helpdesk	✓	7.71	✓	20.66
Editplus	ctx_cloud_logon_sim	Xchag_sim_9.39	https://abccorp.x...	egin\vduser4	XENAPP7V6	✓	4.68	✓	6.66
Editplus	ctx_logon_simulator	logon_sim	http://xendesk.org	citrix\eguser	XENAPP7V6	✓	21.11	✓	18.19
Login_page	ctx_cloud_logon_sim	Xchag_sim_9.39	https://abccorp.x...	egin\vduser3	XENAPP7V6	✓	7.97	✓	21.37
Paint	ctx_cloud_logon_sim	Xchag_sim_9.39	https://abccorp.x...	egin\vduser2	XENAPP7V6	✓	4.67	✓	5.66
Paint	ctx_logon_simulator	logon_sim	http://xendesk.org	citrix\cbuser	XENAPP7V6	✓	4.71	✓	5.66
Windows Media Player	ctx_logon_simulator	logon_sim	http://xendesk.org	citrix\eguser	XENAPP7V6	✓	25.99	✓	18.56
Remote Desktop Connection	CtxLogonSim	logon_sim	https://remote.eginn...	satheesh	LTXAPP09	✓	9.12	✓	17.55

Figure 1.41: Metrics reported per simulation

The dashboard displays the applications/desktops accessed and metrics captured during each simulation. This way, the simulations that failed and the precise failure points - whether login, enumeration, application/desktop 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. Figure 1.42 will then appear.

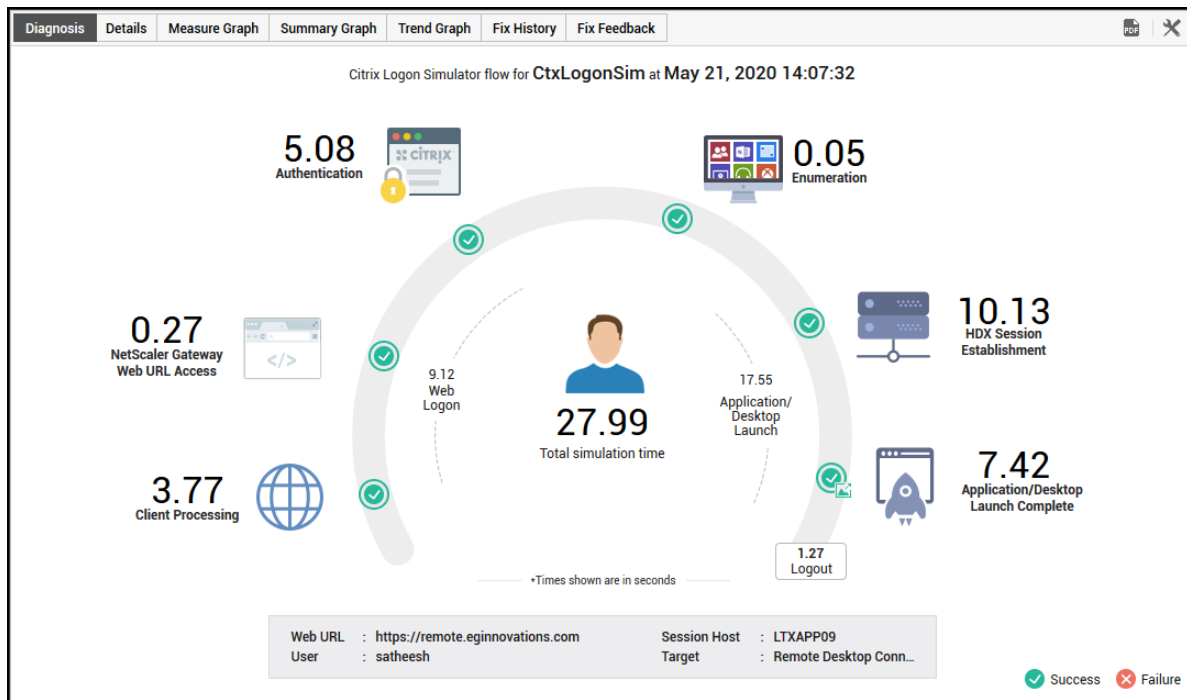



Figure 1.42: The Simulator Dashboard in the eG monitoring console revealing at first glance, the root-cause of logon slowness

A quick look at Figure 1.42 will reveal the total simulation time and the time taken at every step of the logon process. Without engaging in any detailed analysis, administrators can rapidly and accurately infer from Figure 1.42, which step of the logon process has caused the slowness.

Clicking on the  in Figure 1.42 will lead you to Figure 1.43 where you can figure out a screenshot showing that the simulation was successful.

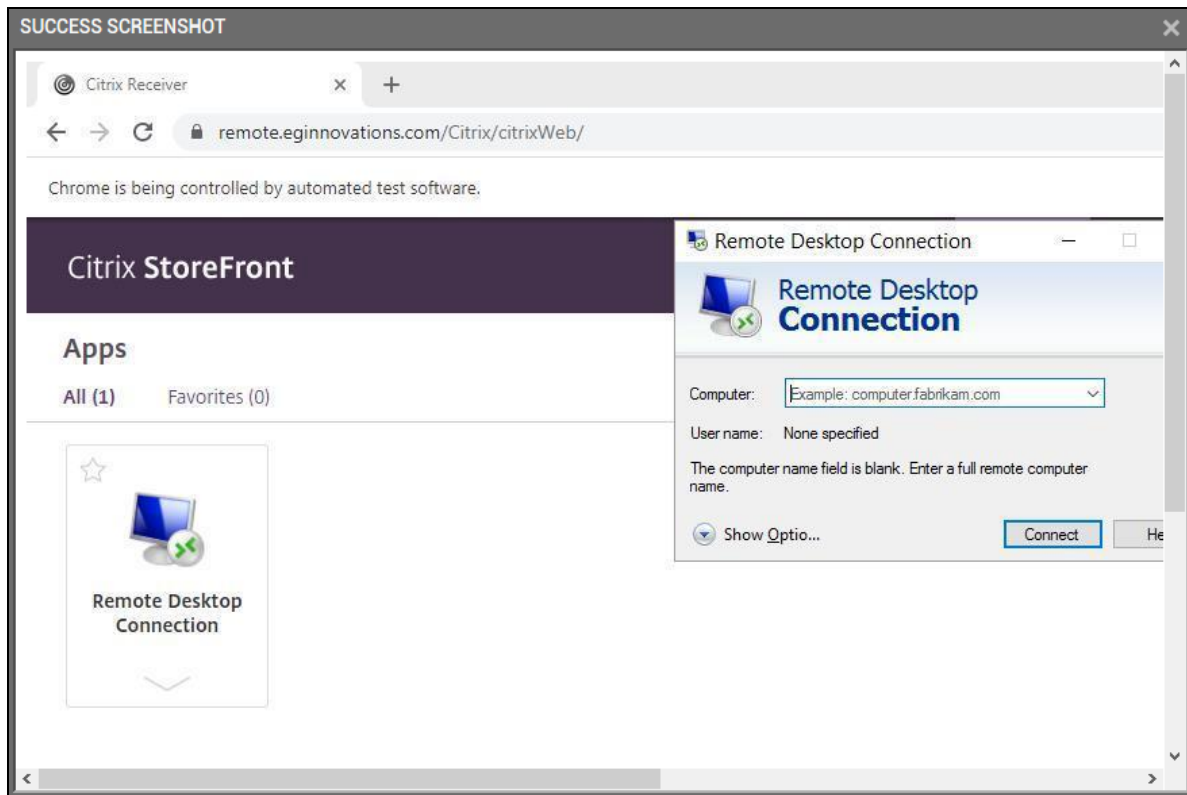


Figure 1.43: A Success screenshot captured by the logon simulator

Similarly, the dashboard can also reveal the exact step at which the simulation failed (see Figure 1.44).

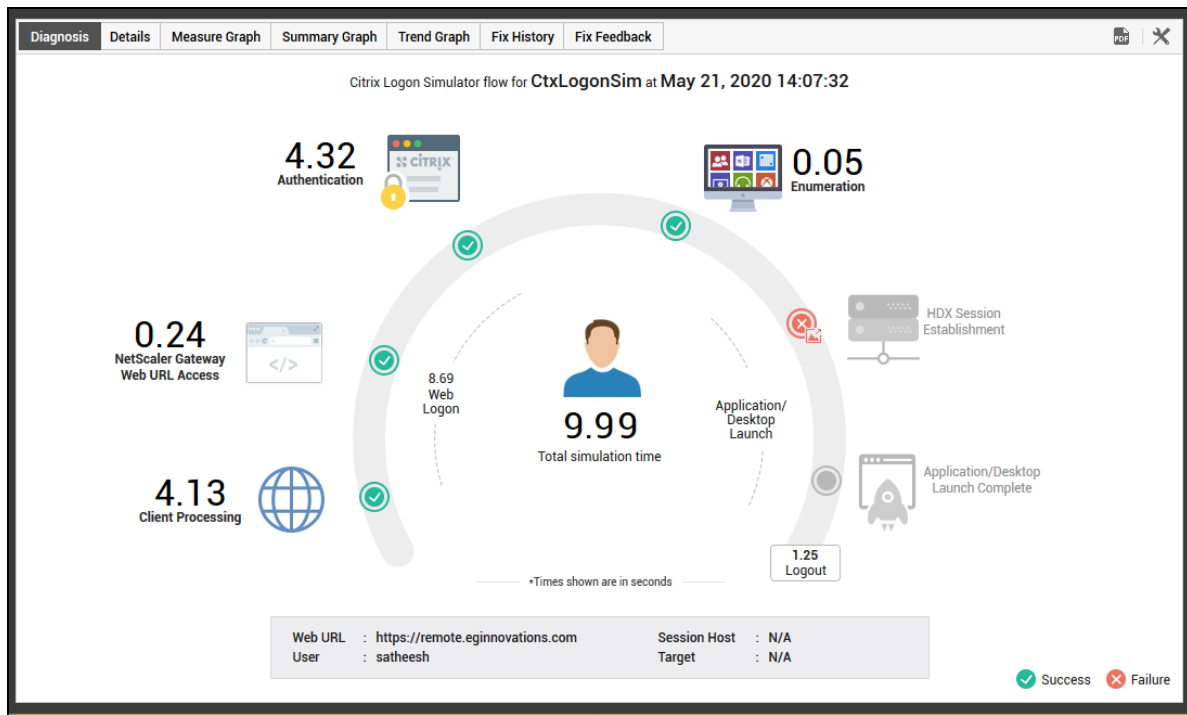



Figure 1.44: The Simulator Dashboard showing that the simulation has failed

Clicking on the  icon in Figure 1.44 will reveal the screenshot that was captured to support the failure.

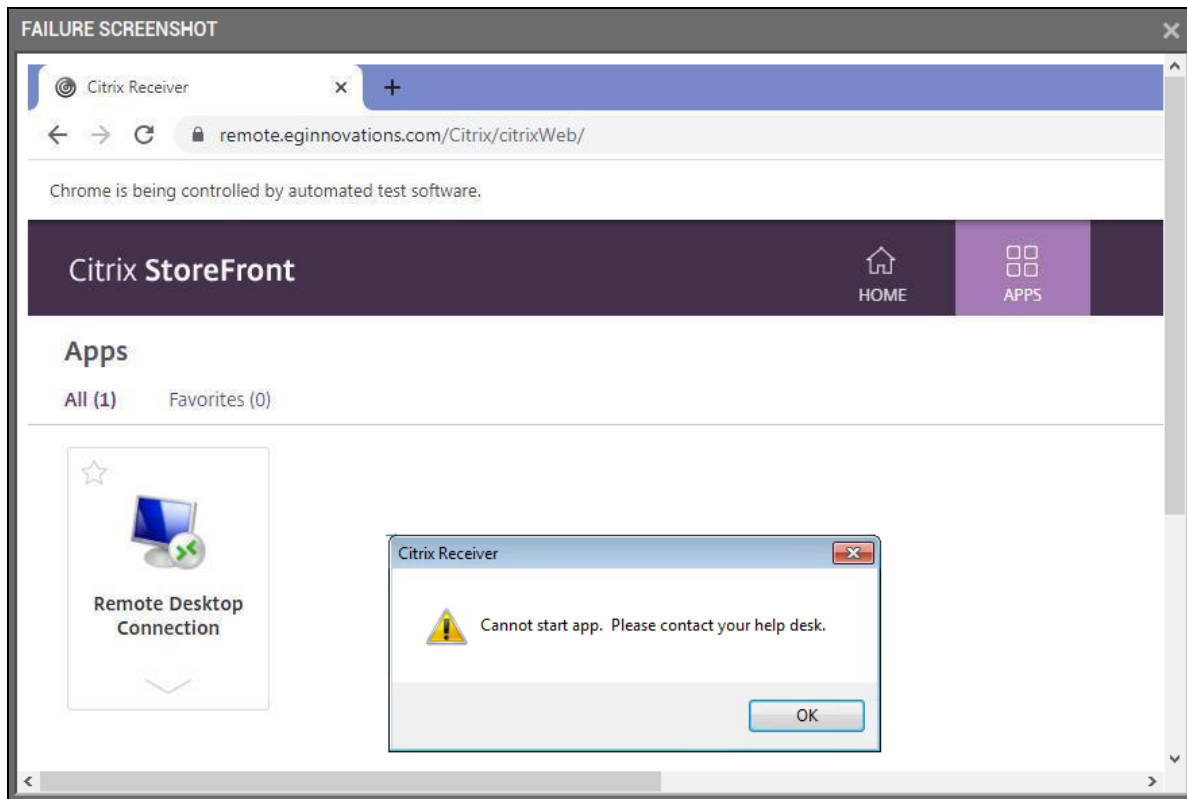


Figure 1.45: A failure screenshot captured by the logon simulator

For historical analysis of the simulated results, the eG Reporter provides a **Logon Simulator Report**. This report can be generated for one/all applications (or desktops), or for one/all Logon Simulation agents.

Use the **Logon Simulator - By Application** report to identify the problem-prone application/desktop in your Citrix farm, zoom into its logon performance, and diagnose its root-cause. For instance, if you generate this report for all applications/desktops that were launched by the simulator during a specified timeline, then Figure 1.46 will appear. A single glance at this report will reveal the following:

- Which application/desktops the simulator attempted to launch during the said timeline?
- In which simulation were logon performance issues detected time and again?
- At which step of the logon process were issues often detected?
- What was causing the issues - was it because a particular operation failed frequently? or was it because a particular operation was consistently taking longer than a configured (acceptable)

duration?

- Which operation (login, enumeration, or launch) is problem-prone?

The screenshot shows a web-based report titled "LOGON SIMULATOR - BY APPLICATION". It includes filters for Zone (Default), Component Type (Citrix Logon Simulator), Application (All), and a Time Range (Jun 20, 2017 18:35 hrs to Jun 27, 2017 18:35 hrs). The main table displays results for 12 applications, grouped under the simulation ID "LogonSimulator_XGIZTW". The table has four main columns: LOGON, APPLICATION ENUMERATION, and APPLICATION LAUNCH, each with sub-columns for AVAILABILITY (%) and DURATION (SECS). Availability is shown with green/red bars and checkmarks/crosses. Duration is shown with green/red bars and checkmarks/crosses.

SIMULATIONS	APPLICATIONS	LOGON		APPLICATION ENUMERATION		APPLICATION LAUNCH	
		AVAILABILITY (%)	DURATION (SECS)	AVAILABILITY (%)	DURATION (SECS)	AVAILABILITY (%)	DURATION (SECS)
LogonSimulator_XGIZTW	outlook	100	✓ 14.8875	0	-	-	-
	Calculator	100	✓ 28.23	100	✓ 3.09	100	✗ 104.18
	Excel	100	✓ 15.86	0	-	-	-
	Notepad	42	✓ 15.7438	98	✓ 1.1704	91	⚠ 31.3857
	eG-Pad	95	✓ 18.14	84	✓ 0.6306	93	✗ 107.3893
	eG-Paint	47	✓ 15.7509	93	✓ 2.8711	95	⚠ 30.6672
	Win8-Desktop	36	✓ 15.6533	99	✓ 3.0589	99	✓ 22.3873
	chrome	98	✓ 14.7808	0	-	-	-
	Win2k12-Server-Apps	35	✓ 16.4317	100	✓ 3.0845	90	✓ 24.9088
	firefox	100	✓ 15.6	0	-	-	-
	ieexplorer	93	✓ 15.442	0	-	-	-
	Cmd	100	✓ 15.1083	0	-	-	-

Figure 1.46: Logon Simulator - By Application Report

This way, you can rapidly identify the 'pain points' of your Citrix delivery infrastructure. Zooming into a particular application/desktop in Figure 1.46 will open Figure 1.47. Figure 1.47 provides a quick summary of the results of all simulations performed by the simulator for the chosen application/desktop.

Chapter 1: An Overview of the eG Enterprise Express Logon Simulator for Citrix

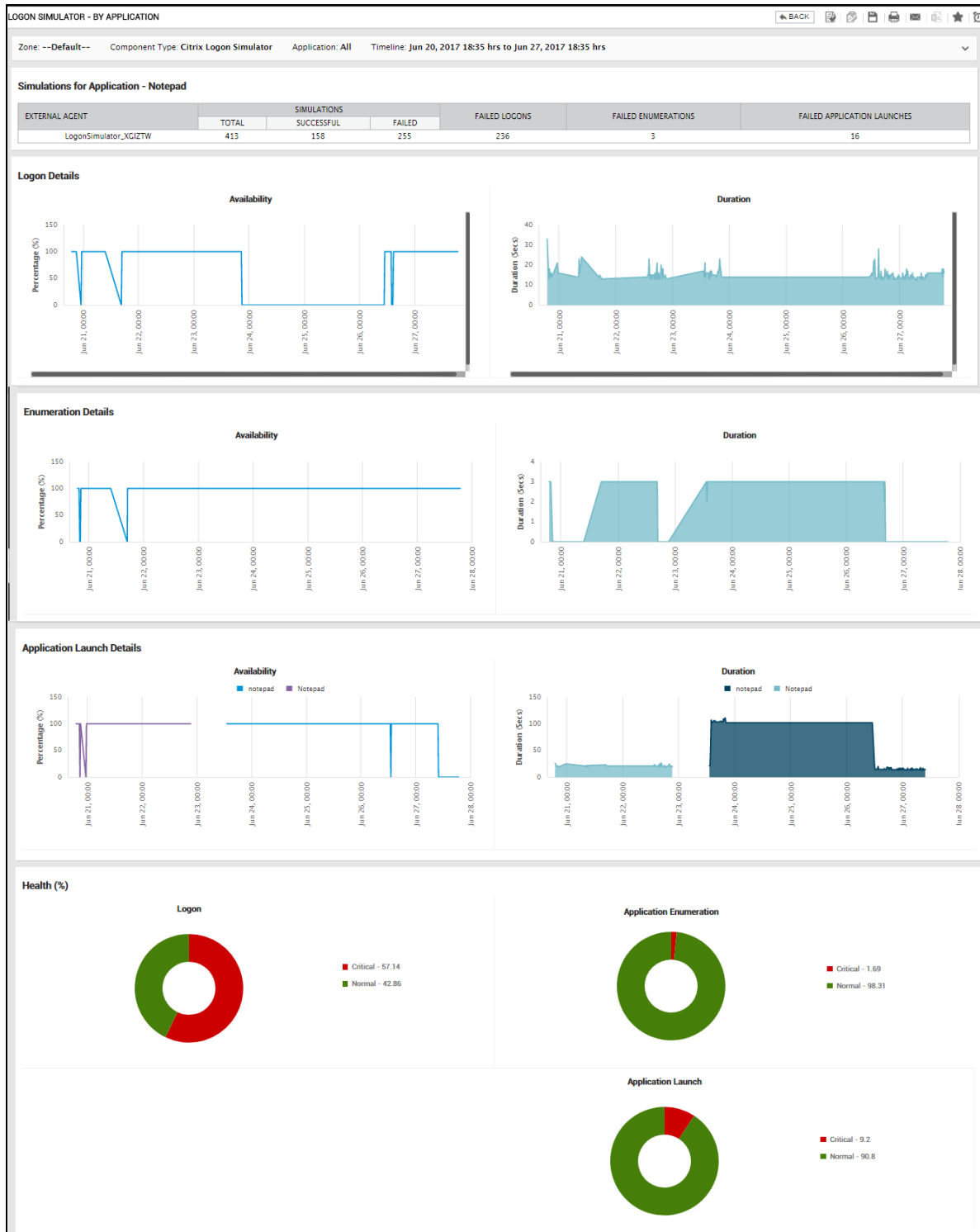


Figure 1.47: Deep dive diagnostics related to the simulations for a particular application/desktop

From Figure 1.47, you can instantly infer if simulations for the application/desktop have failed more often than they have succeeded. If so, Figure 1.47 also points you to the probable cause of these failures - login? enumeration? or application launch? You can then use the graphs in Figure 1.47 to isolate exactly when during the given timeline, simulations for that application/desktop failed or took longer than usual. Ascertain the overall application health during the specified timeline using the **Application Health** doughnut in Figure 1.47. This will reveal whether the application/desktop was healthy or in an abnormal state the majority of time.

The **Logon Simulator - By Simulator Agent** report (see Figure 1.48 and Figure 1.49) is ideal if you have configured multiple Logon Simulator Agents in different locations to perform the simulations. Using this report, you can:

- Easily compare the historical simulation results of the different agents;
- Accurately identify the agent that has reported issues much frequently than the rest;
- Zoom into the simulations performed by that agent and figure out if the agent location is the reason for the frequent issues;

SIMULATIONS	EXTERNAL AGENTS	LOGON		APPLICATION ENUMERATION		APPLICATION LAUNCH	
		AVAILABILITY (%)	DURATION (SECS)	AVAILABILITY (%)	DURATION (SECS)	AVAILABILITY (%)	DURATION (SECS)
LogonSimulator_XGIZTW	LogonSimulator_XGIZTW	100	14.8851	100	2.2974	86	16.6056

Figure 1.48: The Logon Simulator - By External Agent Report reporting logon performance metrics captured by all agents

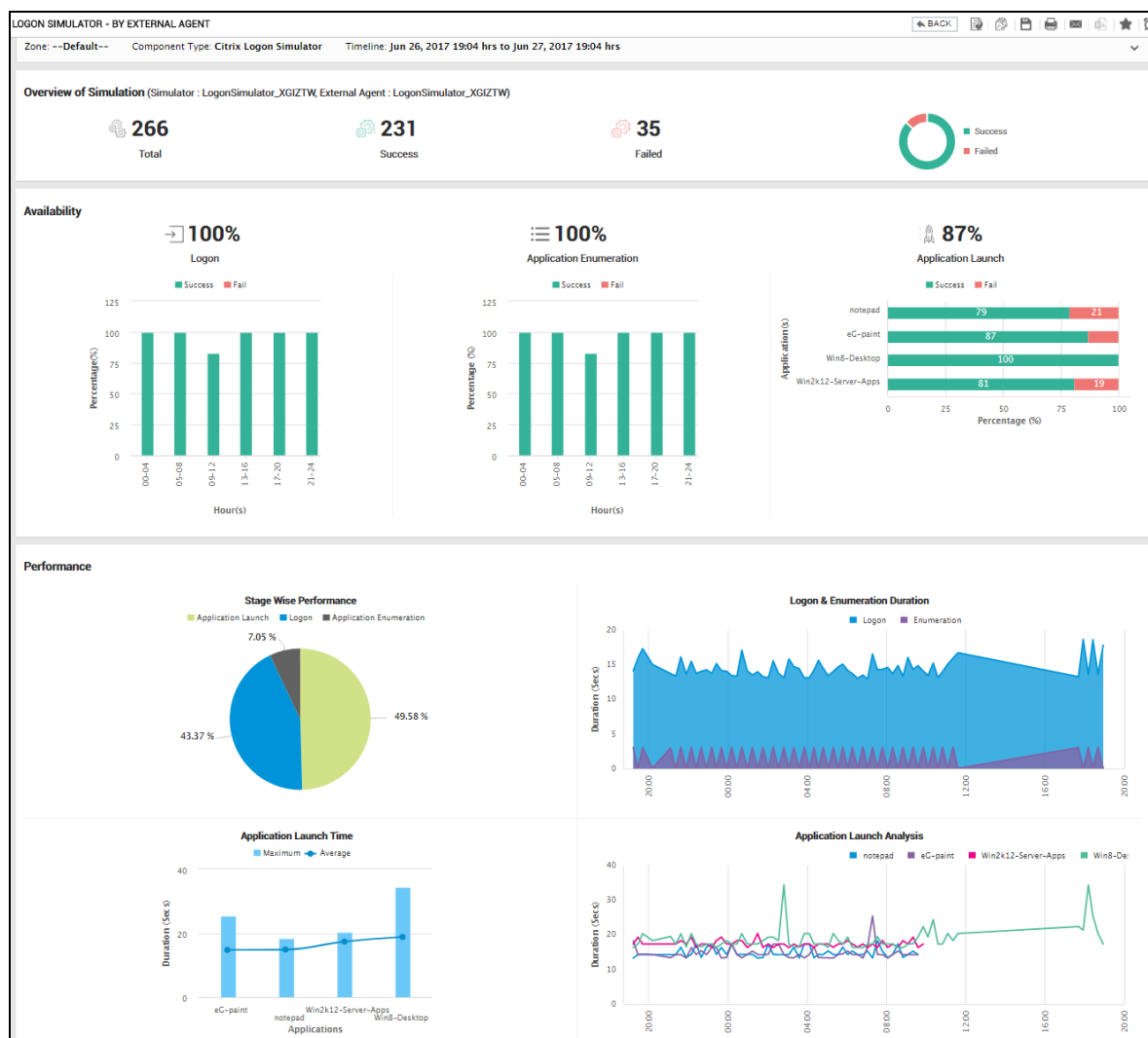


Figure 1.49: Zooming into the simulation results reported by a particular agent

Note:

The eG Enterprise Express Logon Simulator for Citrix maintains a rolling history of seven (7) days for storing logon simulation monitoring data. The reports discussed in this topic are generated using this data only. Data for any given day (stored by the free logon simulator) will be purged after a seven (7) day period, and will not be available to you for access via the logon simulator portal or any other means.

1.13 Enabling Email Notifications for Issues

If you want the alerts raised in the eG Enterprise Express Logon Simulator for Citrix XenApp and XenDesktop to be sent over email, then you can do so using the **USER PROFILE** window. This


window appears when you click on the  icon in the tool bar of the eG Enterprise Express Logon Simulator for Citrix XenApp and XenDesktop.



Figure 1.50: Clicking the User Profile icon

In Figure 1.51 that appears, simply click **Critical** or **Major** or **Minor** or a combination of criticality under the **Alarms by Mail** flag to receive email alerts on problematic conditions experienced during the simulation process. In our example below, since **Critical** is chosen, the email notifications are sent only when critical alarms are generated.

The image shows a 'USER PROFILE' dialog box with a close button (X) in the top right corner. It contains the following fields and options:

- User ID**: A text box containing 'partha.pm@eginnovations.com' with the note '(login does not expire)' below it.
- Alarms by Mail**: Three buttons labeled 'Critical' (with a red X icon), 'Major' (with an orange exclamation mark icon), and 'Minor' (with a green question mark icon). The 'Critical' button is highlighted.
- Mail ID**: A text box containing 'partha.pm@eginnovations.com'.
- CC**: An empty text box.
- BCC**: An empty text box.
- At the bottom, there is a 'Submit' button and a link labeled 'Edit Profile'.

Figure 1.51: Setting the Alarms by Mail flag to Critical

1.14 Benefits of the eG Enterprise Express Logon Simulator for Citrix

The key benefits of the express simulator are as follows:

- **Deliver great user experience for Citrix users:** Provide fast and uninterrupted Citrix services
- **Proactively detect Citrix logon issues** before end-users and business services are affected

- **Speed up mean time to resolution (MTTR):** Find and fix Citrix logon problems before users call the helpdesk
- **Benchmark and optimize your Citrix infrastructure:** Be the first to know if any changes are impacting the Citrix logon experience
- **Complete visibility into Citrix logon performance:** Monitor real user logon experience and simulation results from a single console

1.15 Going Beyond the eG Enterprise Express Logon Simulator for Citrix

The eG Enterprise Express Logon Simulator for Citrix is a useful tool for Citrix administrators to simulate and proactively monitor logon simulation in their XenApp and XenDesktop environments. You can go beyond the capabilities of the free logon simulator and get comprehensive Citrix monitoring, diagnosing and troubleshooting capabilities with eG Enterprise – a Citrix Ready performance monitoring solution for any size Citrix environment. eG Enterprise includes logon simulation capabilities, as well as real user experience monitoring capabilities.

Comparison of Features of the eG Enterprise Express Logon Simulator for Citrix and eG Enterprise Citrix Monitoring Suite

Key Features	eG Enterprise Express Logon Simulator for Citrix	eG Enterprise (Full-Featured Citrix Monitoring Solution)
Logon Simulation		
Number of Citrix farm URLs supported	Only one	Unlimited
Number of applications and desktops supported	Up to 3 applications or desktops (1 per user)	Unlimited
Number of users supported	Up to 3 users	Unlimited
Historical data retention for trending and reporting	Rolling history of up to 7 days	Unlimited
In-Depth Citrix Performance Monitoring		
Simulate the entire Citrix session (including user access to published applications)	No	Yes
Real user experience monitoring (ICA/HDX insights)	No	Yes
Performance monitoring of XenApp, XenDesktop, StoreFront, NetScaler, PVS, XenMobile, ShareFile, etc.	No	Yes

Automatic correlation and root cause diagnosis	No	Yes
Automatic dependency mapping and monitoring of the supporting infrastructure (network, storage, virtualization, cloud, etc.)	No	Yes
Out-of-the-box reports for capacity planning, forecasting and right-sizing	No	Yes
Deployment options	Only SaaS	On-premises or SaaS

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.

Copyright © 2022 eG Innovations Inc. All rights reserved.

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

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