



## The eG Enterprise Express Logon Simulator for Microsoft AVD

eG Innovations Product Documentation

[www.eginnovations.com](http://www.eginnovations.com)



# Table of Contents

---

CHAPTER 1: AN OVERVIEW OF THE EG ENTERPRISE EXPRESS LOGON SIMULATOR FOR MICROSOFT AVD .....	1
1.1 Challenges in Troubleshooting User Logon Performance Issues in Microsoft AVD Environments ..	1
1.2 The eG Enterprise Express Logon Simulator for Microsoft Azure Virtual Desktop .....	2
1.3 How Does the eG Enterprise Express Logon Simulator for Microsoft AVD Work? .....	2
1.4 Pre-requisites for eG Enterprise Express Logon Simulator for Microsoft AVD .....	4
1.5 Installing and Configuring the eG Enterprise Express Logon Simulator for Microsoft AVD .....	5
1.5.1 Subscribe to the Simulation Service .....	6
1.5.2 Configure the Simulation .....	9
1.5.3 Download and Install the Logon Simulator Agent .....	12
1.6 Microsoft AVD Logon Simulator Caveat .....	16
1.7 Fine-tuning the Simulation .....	21
1.7.1 Fine-tuning the simulation using Autologon.exe .....	22
1.7.2 Fine-tuning the simulation by editing the windows registry .....	23
1.8 Browser launch hindered due to disabled chrome extensions .....	24
1.9 Viewing and Interpreting the Simulation Results .....	25
1.10 Enabling Email Notifications for Issues .....	32
1.11 Benefits of the eG Enterprise Express Logon Simulator for Microsoft AVD .....	33
1.12 Going Beyond the eG Enterprise Express Logon Simulator for Microsoft AVD .....	33
ABOUT EG INNOVATIONS .....	35

# Table of Figures

Figure 1.1: Connecting to the URL: logonsimulator.eginnovations.com .....	6
Figure 1.2: Terms and conditions of service .....	7
Figure 1.3: Signing up to use the eG Enterprise Express Logon Simulator for Microsoft AVD .....	8
Figure 1.4: Specifying the verification code sent by email .....	8
Figure 1.5: Home page of the eG Enterprise Express Logon Simulator for Microsoft AVD portal .....	9
Figure 1.6: Configuring the simulation .....	9
Figure 1.7: Configuring the Published Resources .....	11
Figure 1.8: Downloading and installing the Logon Simulator Agent .....	12
Figure 1.9: Setup script where a pre-requisite has failed .....	13
Figure 1.10: All pre-requisites are fulfilled .....	13
Figure 1.11: Successful installation of the Logon Simulator Agent .....	14
Figure 1.12: The Group Policy Management Window .....	16
Figure 1.13: Creating a new GPO .....	17
Figure 1.14: Listing the newly created GPO .....	17
Figure 1.15: Editing the GPO .....	18
Figure 1.16: Editing the newly created GPO .....	18
Figure 1.17: Navigating to the Session Time Limits option .....	19
Figure 1.18: Editing the Set time limit for disconnected sessions option .....	19
Figure 1.19: Window to set time limit for disconnected sessions to logoff .....	20
Figure 1.20: Setting a time limit to end a disconnected session .....	21
Figure 1.21: Agreeing to the Software License Terms .....	22
Figure 1.22: Provide the password in this form .....	23
Figure 1.23: Error message that appears when chrome extensions failed to load .....	24
Figure 1.24: The Current Alarms window reporting logon performance issues .....	25
Figure 1.25: Metrics reported per simulation .....	25
Figure 1.26: The Simulator Dashboard in the eG monitoring console revealing at first glance, the root-cause of logon slowness .....	26
Figure 1.27: The Simulator Dashboard showing that the simulation has failed .....	26
Figure 1.28: A failure screenshot captured by the logon simulator .....	27
Figure 1.29: Logon Simulator - By Application Report .....	28
Figure 1.30: Deep dive diagnostics related to the simulations for a particular application/desktop .....	29
Figure 1.31: Zooming into the simulation results reported by a particular agent .....	31
Figure 1.32: Clicking the User Profile icon .....	32
Figure 1.33: Setting the Alarms by Mail flag to Critical .....	32

# Chapter 1: An Overview of the eG Enterprise Express Logon Simulator for Microsoft AVD

This document provides an overview of the eG Enterprise Express Logon Simulator for Microsoft AVD, 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 Microsoft AVD Environments

For years, slow logons have been the most common complaint in Azure infrastructures. For an Azure Virtual Desktop user, slow logons can lead to frustration, lower productivity and efficiency. For an Azure Virtual Desktop administrator, 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 logon process and they involve multiple components – Azure Active Directory, Azure Active Directory Connect Server, Azure Active Directory Domain Services Server, Microsoft Azure and so on. Identifying exactly what is causing the slowdown is often time consuming and laborious.
- **Collection of logon metrics challenging:** To ensure great Azure Virtual Desktop 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 Microsoft Azure Virtual Desktop 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 Microsoft Azure Virtual Desktop 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 Microsoft Azure Virtual Desktop, and at those times, it is important to know if Microsoft Azure Virtual Desktop logon is working and whether users can launch their applications and desktops successfully.

## 1.2 The eG Enterprise Express Logon Simulator for Microsoft Azure Virtual Desktop

The eG Enterprise Express Logon Simulator for Microsoft Azure Virtual Desktop (AVD), is a free cloud-based, on-demand service that delivers proactive visibility into the logon performance in Microsoft Azure infrastructures. This simulator emulates the exact same process that users go through when they logon to Microsoft Azure Virtual Desktop, and measures user experience during logon.

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

- Receive a consistent, true picture of Microsoft Azure Virtual Desktop logon performance, whether or not users are logged into the Microsoft Azure Virtual Desktop;
- 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 Microsoft Azure infrastructure are frequently complaining of slowness or failures when accessing their Azure Virtual 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 Microsoft Azure Virtual Desktop, 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 Microsoft AVD 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 Microsoft Azure Virtual Desktop and launching an application. 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 for connecting to the AVD Web Client;
- The credentials using which it needs to log into the Microsoft Azure Virtual Desktop;

- The applications and/or desktops that it needs to launch

Once the simulator is configured, it runs at a pre-configured frequency.

The simulation process is described below:

1. The simulator first opens the Chrome browser and connects to the configured URL that is required to connect to the AVD Web Client
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 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 Microsoft AVD 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 eG Enterprise Express Logon Simulator for Microsoft AVD

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

Category	Pre-requisites
<b>Logon Simulator Agent / Simulation Endpoint</b>	<ul style="list-style-type: none"> <li>• The Logon Simulator Agent should be installed on a dedicated endpoint. <b>The dedicated endpoint should only run an English version of Windows operating system.</b></li> <li>• No other eG agent should exist on the same host on which the Logon Simulator Agent has been installed.</li> <li>• .NET Framework 4.5 (or above) should pre-exist on the system hosting the Logon Simulator Agent.</li> <li>• The simulator requires a dedicated Microsoft Azure user account with rights to launch applications/desktops.</li> <li>• The simulator also requires a user account with local administrator rights on the simulation endpoint - i.e., on the system hosting the Logon Simulator Agent. This user should be logged in at all times for the simulator to run continuously.</li> </ul>
<b>Environment</b>	<ul style="list-style-type: none"> <li>• The simulator will only work with AVD Web Client.</li> <li>• The allocated desktop that is to be launched by simulation should be powered on and also should be a dedicated desktop.</li> </ul>

<b>Browser</b>	<p>The eG Enterprise Express Logon Simulator for Microsoft AVD mandates the presence of the Chrome browser v110 (and above). No other browser supports this simulation.</p> <p><b>Note:</b></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 Microsoft AVD, 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 simulation endpoint allows Chrome upgrades. To achieve this, before manually upgrading Chrome, follow the steps below:</p> <ul style="list-style-type: none"> <li>• Login to the eG agent host.</li> <li>• Open the Windows command prompt as Administrator.</li> <li>• Switch to the &lt;EG_AGENT_INSTALL_DIR&gt;\lib directory, and issue the following command:</li> </ul> <p><b>ChromeUpgradeHandler.exe enable</b></p>
----------------	--

## 1.5 Installing and Configuring the eG Enterprise Express Logon Simulator for Microsoft AVD

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

1. Subscribe to the Simulation Service
2. Configure the Simulation
3. Download and Install the Logon Simulator Agent

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



### 1.5.1 Subscribe to the Simulation Service

For this, first connect to <https://logonsimulator.eginnovations.com>. Figure 1.1 will appear.

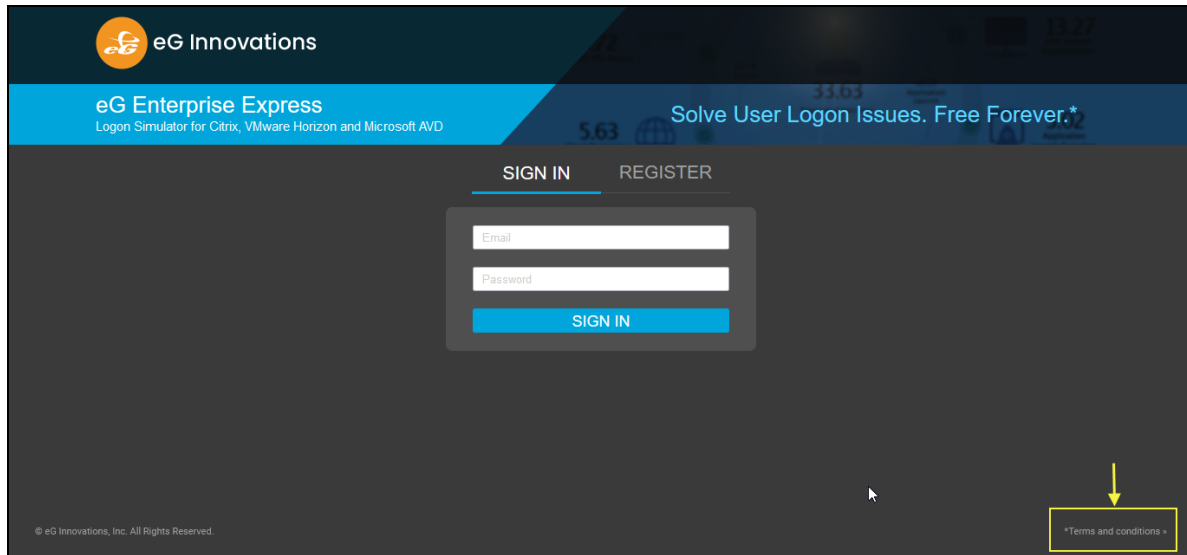


Figure 1.1: Connecting to the URL: [logonsimulator.eginnovations.com](https://logonsimulator.eginnovations.com)

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 1.1). Figure 1.2 will then appear.

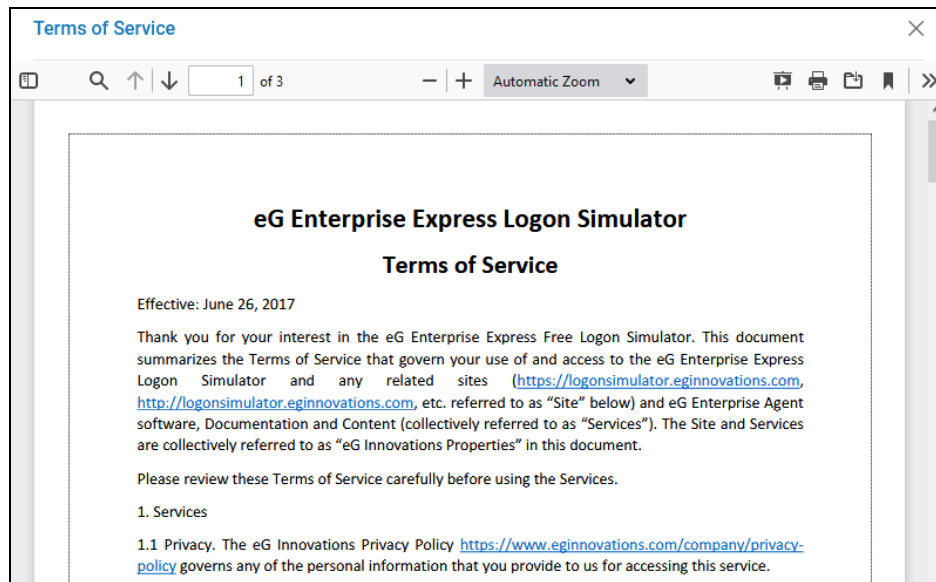


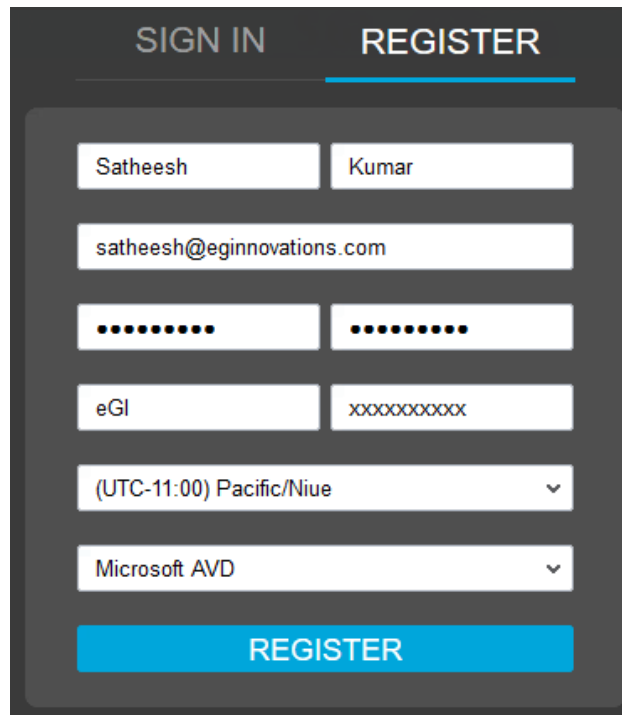
Figure 1.2: Terms and conditions of service

After reading the terms and conditions of service, close the window and return to the **SIGN IN** page of Figure 1.1. Then, to register, click on the **REGISTER** link in Figure 1.1. When Figure 1.3 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 Microsoft AVD, 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.

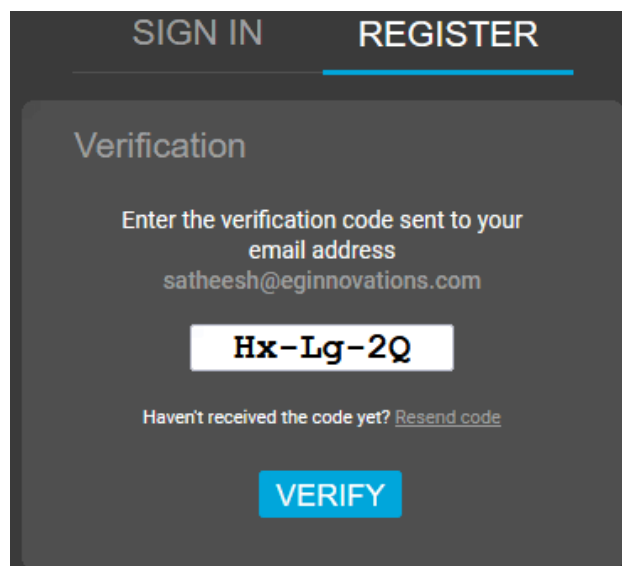
Also, specify your company name, pick a Time zone, and enter your phone number. eG Enterprise offers eG Enterprise Express Logon Simulator for Citrix VirtualApps / VirtualDesktops, VMware Horizon and Microsoft AVD. Select the environment for which you wish to configure the simulations from the **Environment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



The registration form is titled "REGISTER" and is part of a larger interface with a "SIGN IN" tab. It contains several input fields: a first name field with "Satheesh", a last name field with "Kumar", an email field with "satheesh@eginnovations.com", two password fields (one with dots, one with "xxxxxxxxxx"), a company field with "eGI", a time zone dropdown menu set to "(UTC-11:00) Pacific/Niue", and a device type dropdown menu set to "Microsoft AVD". A large blue "REGISTER" button is at the bottom.

Figure 1.3: Signing up to use the eG Enterprise Express Logon Simulator for Microsoft AVD

A Verification code will be sent to the email address you specified in Figure 1.3. Upon receipt of the code, copy and paste it in Figure 1.4 and click **Verify**.



The verification form is titled "REGISTER" and is part of a larger interface with a "SIGN IN" tab. It contains a "Verification" section with the text "Enter the verification code sent to your email address" and the email address "satheesh@eginnovations.com". Below this is a text input field containing the code "Hx-Lg-2Q". There is a link "Haven't received the code yet? [Resend code](#)". A large blue "VERIFY" button is at the bottom.

Figure 1.4: Specifying the verification code sent by email

Once the code is successfully verified, Figure 1.5 will appear, detailing the next steps for using this simulator.



Figure 1.5: Home page of the eG Enterprise Express Logon Simulator for Microsoft AVD portal

### 1.5.2 Configure the Simulation


To configure the simulation, click **Get Started Now** in Figure 1.5. Figure 1.6 will then appear.

Figure 1.6: Configuring the simulation

Provide the following inputs in Figure 1.6:

1. **Site URL:** The URL for connecting to the AVD Web Client.

**Note:**

- Only Microsoft AVD Host Pool is supported.
  - The eG Enterprise Express Logon Simulator for Microsoft AVD supports only up to one (1) URL that is connected to the AVD Web Client.
2. **Username, Password and Confirm Password:** Specify the credentials of the user is authorized to access the applications/desktops via the AVD Web Client in the **Username** and **Password** text boxes. Confirm the Password by retyping it in the **Confirm Password** text box.
  3. **Published resources:** Provide the name of a resource that is to be launched in the **Published resources** text box. The resource can be an application / desktop. When providing application/desktop names, make sure you provide the same name using which the applications/desktops are displayed in the AVD web console and the AVD Web Client. Also, make sure that the user you specify is authorized to launch all the applications/desktops configured in the Published resources text box. To provide a comma-separated list of Published resources, click on the  icon against **Published resources** (see Figure 1.6). To know how to configure the Published resources refer to **Section 1.5.2.1**.

**Note:**

You can configure a comma-separated list of **Published resources** only if the resources belong to the same domain. On the other hand, if you want to launch resources that belong to different domains, then, ensure that you configure each resource separately by clicking the **Add more published resources** button.

4. **Is disclaimer enabled?:** Some high-security AVD 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**.
5. **Resource domain, Resource username, Resource password, and Confirm Password:** Specify the domain in which the resource (that is to be launched) is stored in the **Resource domain** text box. Specify the credentials of the user who is authorized to access the **Resource domain** in the **Resource username**, **Resource password**, and **Confirm Password** text boxes. In case the target Microsoft AVD environment is SSO enabled (single


sign-on), then, specify *none* against the **Resource domain**, **Resource username**, **Resource password** and **Confirm password** text boxes.

**Note:**

- The eG Enterprise Express Logon Simulator for Microsoft AVD supports a maximum of only three (3) users for logon simulation.

Click **Add More Users** if you want to simulate accesses of another user launching an application / desktop. However, the eG Enterprise Express Logon Simulator for Microsoft AVD 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. Clicking the **Clear** button will clear your configuration.

### 1.5.2.1 Configuring Published Resources

Clicking on  icon in Figure 1.6 will lead you to Figure 1.7 using which you can configure a comma-separated list of Published resources.

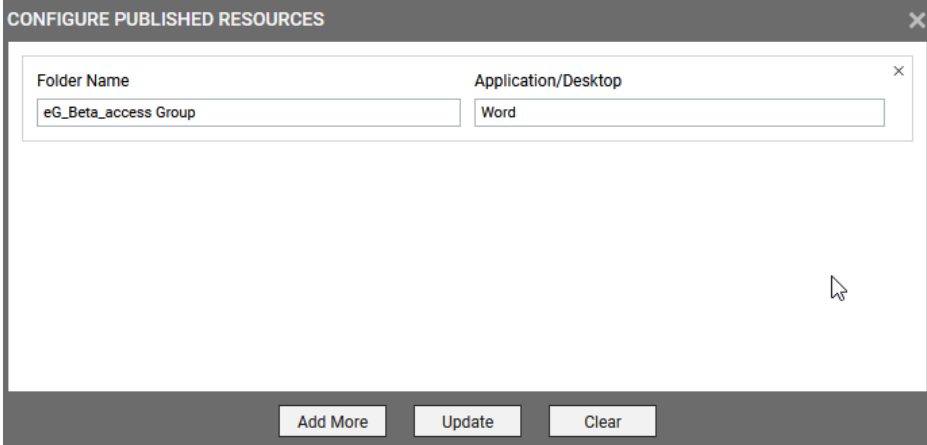


Figure 1.7: Configuring the Published Resources

In Figure 1.7, specify the following:

1. **Application/Desktop:** Specify the names of the applications/desktops to be launched.

**Note:**

The applications/desktops can be specified either in lower case or upper case or a combination of both.

2. **Folder Name:** If the simulator is simulating accesses to AVD environment via the AVD Web Client, then the **All Resources** page of the console will list the folders / groups that contain the resources (i.e., applications / desktops) that are available for access. The application / desktop that the simulator should launch may be in any of these folders / groups. By default, this is set to *none* if you are launching a unique application / desktop from the **All Resources** page. On the other hand, if the application / desktop to be launched is available in multiple folders of the **All Resources** page, then you must specify the exact **Folder Name** within which that application / desktop is present.

**Note:**

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

3. Finally, click the **Add More** button in Figure 1.7 to add more applications/desktops to be launched. If you do not want to add any more applications/desktops, click the **Update** button to save the changes.

### 1.5.3 Download and Install the Logon Simulator Agent

Click on **Download Agent** tab page in 1.5.2 to download and install the Logon Simulator Agent. From the list of agent packages displayed in Figure 1.8, click on the package that suits your environment.

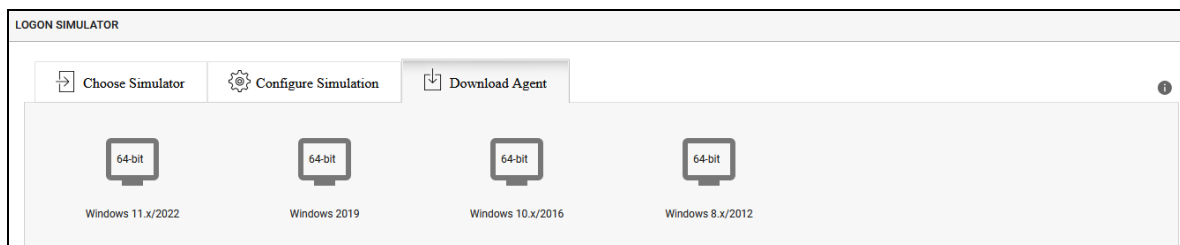


Figure 1.8: Downloading and installing the Logon Simulator Agent

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 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 1.5.3.1** 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 1.9).

```
eG Express Logon Simulator - 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.
eG Logon Simulator Agent communication with eG SaaS Portal: Successful
ACTION: Please ensure that all the prerequisites are met.
```

Figure 1.9: Setup script where a pre-requisite has failed

Use the pointers provided in Figure 1.9, 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.

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 - 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
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 1.10: All pre-requisites are fulfilled

If the agent installation is successful, then a message depicted by Figure 1.11 will appear.



```
eG Application is Installing ....

*****
This process will take few minutes to complete.
PLEASE DO NOT INTERRUPT THIS PROCESS.
*****

*****
The eG Application has been installed successfully!!!
*****

Press any key to continue . . .

*****
To know more about Microsoft AVD Logon Simulator, refer to
The_eG_Enterprise_Express_Logon_Simulator_for_Microsoft_AVD document,
which will be available in the folder into which you extracted the eG Agent zip.
*****

Press any key to continue . . .
```

Figure 1.11: Successful installation of the Logon Simulator Agent

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

### 1.5.3.1 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 1.5.3**. 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.

## 1.6 Microsoft AVD Logon Simulator Caveat

By default, the browser interface to Microsoft AVD allows a user to disconnect his/her initiated session rather than logout from the session completely. This is because, Microsoft AVD is designed to retain the session by default, and let the user connect back to the session if he/she connects again. Though this process is very simple to use from a user perspective, the logon simulator will not be able to capture the entire logon simulator process until the user is logged out of the session. This will therefore create a greater impact on how the user experience is measured on the Microsoft Azure Virtual Desktop. For this, administrators should ensure that the user is logged out after each simulation rather than the user session being in the disconnected state. To ensure that the user used for simulation is automatically logged out after each simulation, administrators should make the following changes on the Microsoft AVD host / Microsoft Azure Active Directory host on which the AVD logon simulation is configured for execution.

1. From the target Windows host, click the **Group Policy Management** that appears upon navigating through the menu sequence: *Start -> Windows Administrative Tools*. Figure 1.12 then appears.

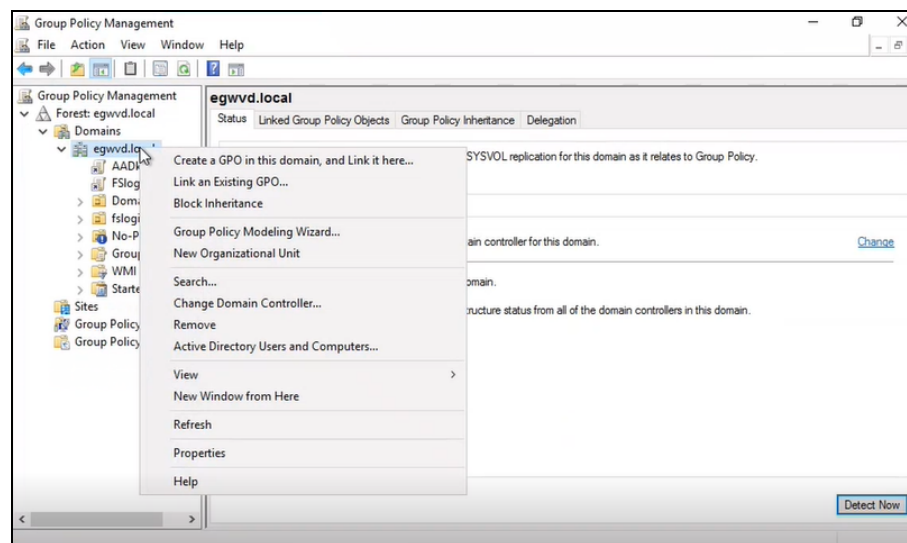


Figure 1.12: The Group Policy Management Window

2. From Figure 1.12, right click on the domain in your environment and select **Create a GPO in this domain, and Link it here...** option to create a new GPO. In Figure 1.13 that appears, specify the **Name** of the GPO that you are about to create and then, click **OK**.

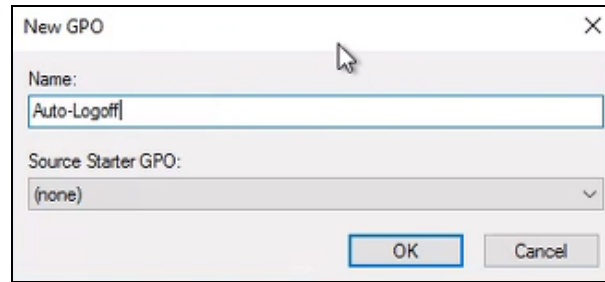


Figure 1.13: Creating a new GPO

3. The newly created GPO will then be listed as shown in Figure 1.14. The user associated with this GPO i.e., the user performing the logon simulation will be listed in the **Security Filtering** section.

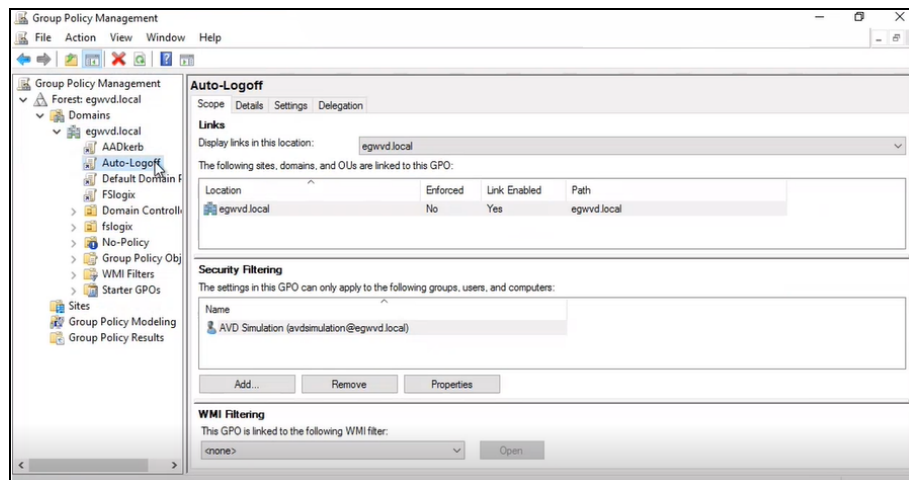


Figure 1.14: Listing the newly created GPO

4. Now, right click the GPO in Figure 1.14 and click the **Edit** option as shown in Figure 1.15.

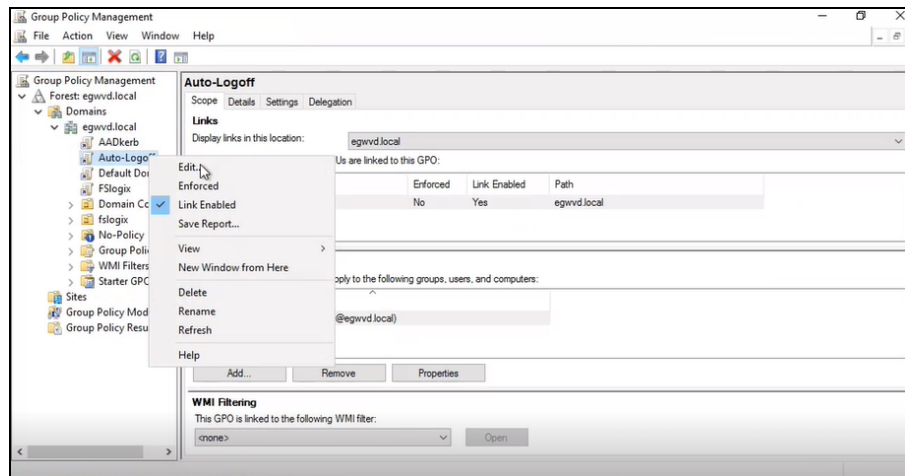


Figure 1.15: Editing the GPO

- Figure 1.16 will then appear listing the **Computer Configuration** and **User Configuration** nodes of the GPO.

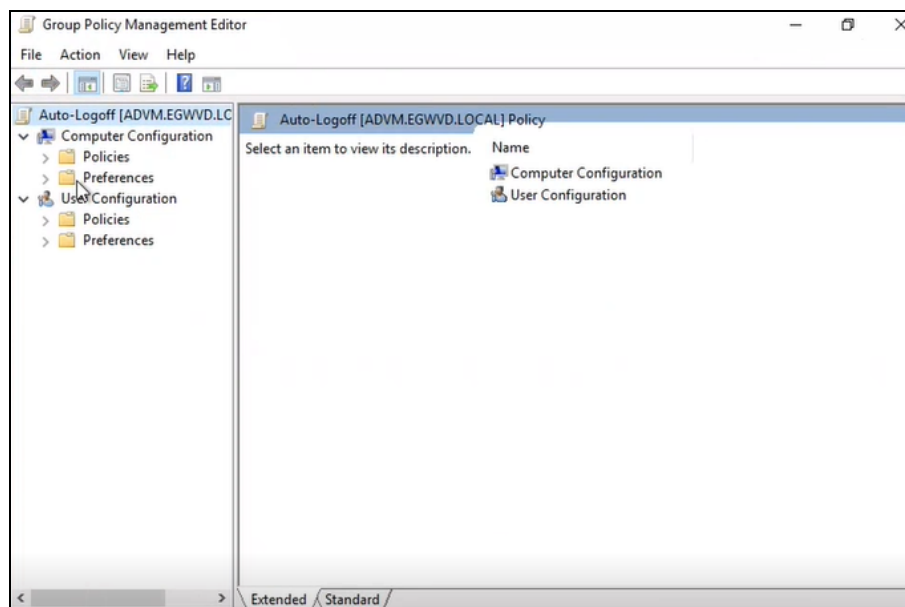


Figure 1.16: Editing the newly created GPO

- Expand the **User Configuration** node in Figure 1.16 and navigate through *Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host*. Clicking the **Session Time Limits** option will reveal Figure 1.17.

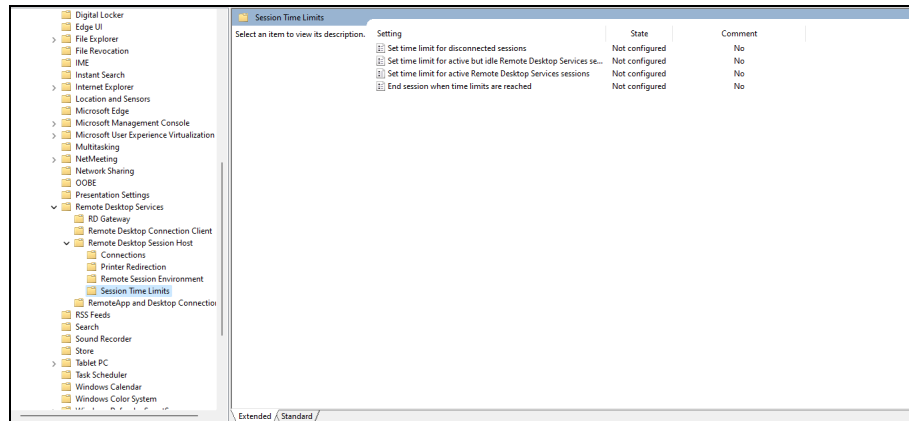


Figure 1.17: Navigating to the Session Time Limits option

7. In Figure 1.17, right click on the **Set time limit for disconnected sessions** option and click the **Edit** option as shown in Figure 1.18.

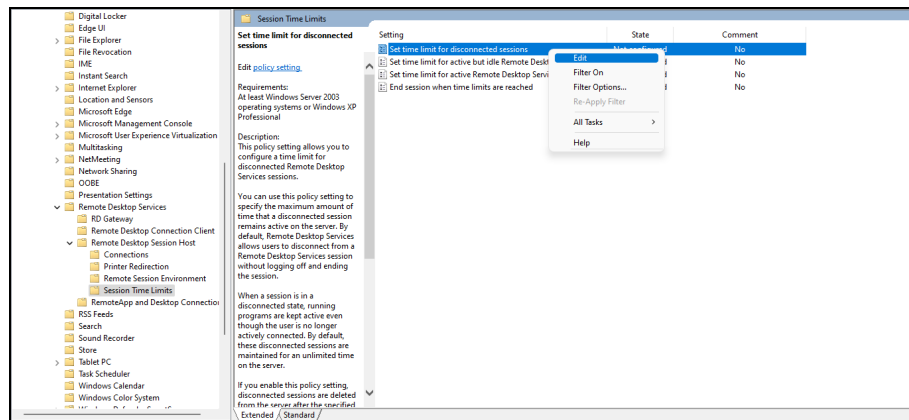


Figure 1.18: Editing the Set time limit for disconnected sessions option

8. Figure 8 will then appear.

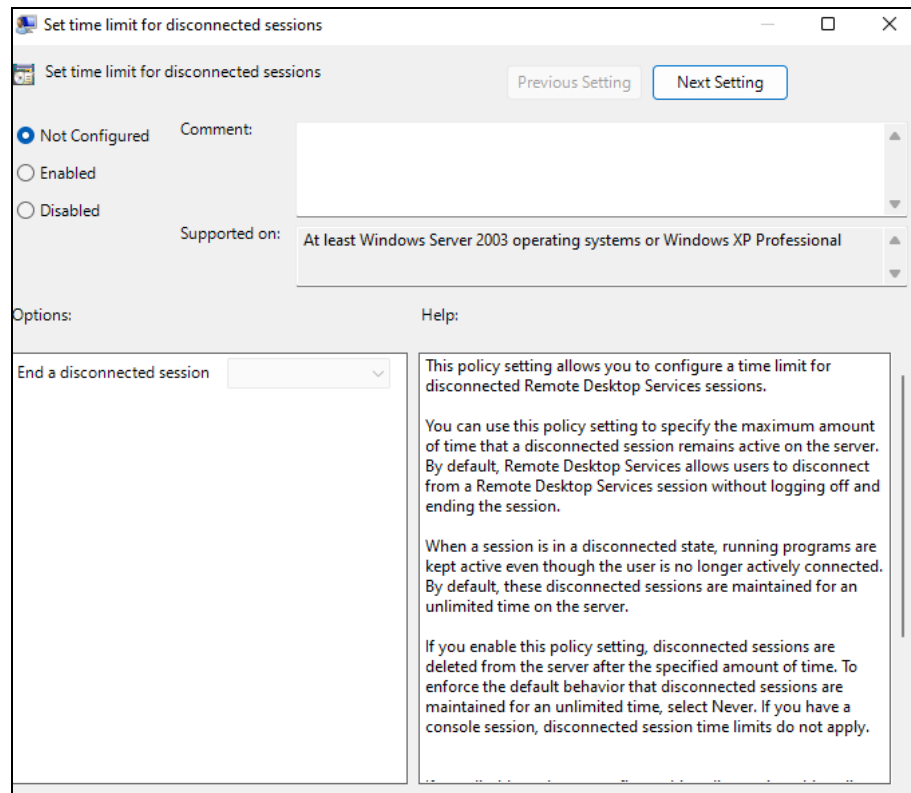


Figure 1.19: Window to set time limit for disconnected sessions to logoff

9. In Figure 1.19, choose the **Enabled** radio button and select an option from the **End a disconnected session** list box (see Figure 1.20). By default, *Never* will be displayed in this list.

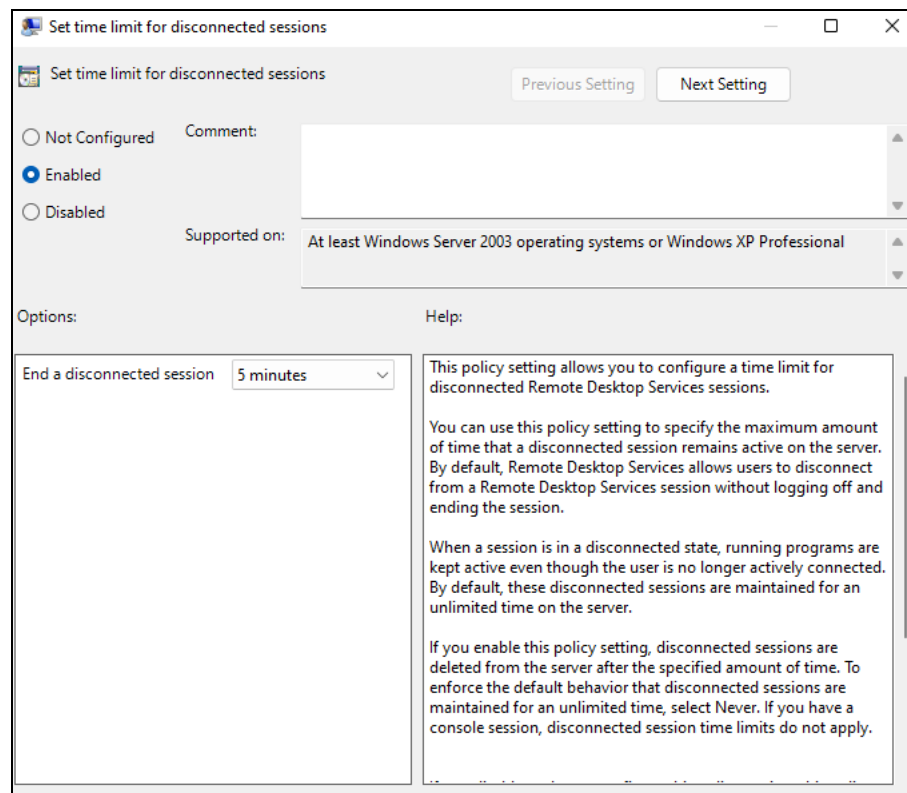


Figure 1.20: Setting a time limit to end a disconnected session

10. This time limit set to end a disconnected session is now automatically applied to the user performing logon simulation.

## 1.7 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.

### 1.7.1 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.

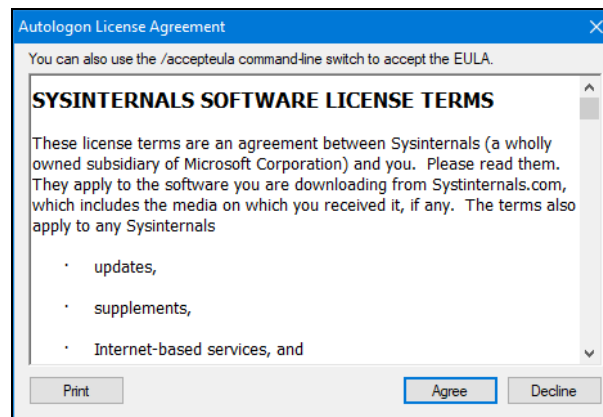


Figure 1.21: Agreeing to the Software License Terms

4. Figure 1.21 then appears. Click **Agree** to accept the Sysinternals Software License Terms.

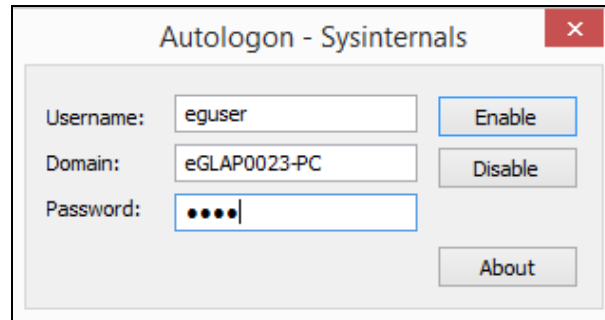


Figure 1.22: Provide the password in this form

5. In Figure 1.22 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.

### 1.7.2 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.

## 1.8 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 1.23 appears.

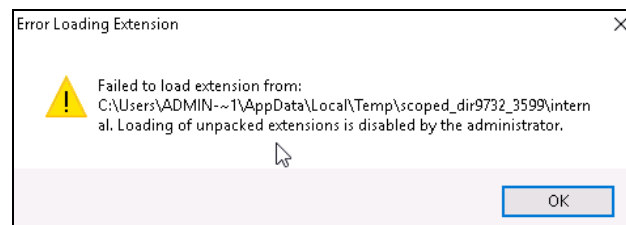


Figure 1.23: Error message that appears when chrome extensions failed to load

For the Microsoft AVD 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 Microsoft AVD Logon Simulator at periodic intervals.**

## 1.9 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.

TYPE	COMPONENT NAME	DESCRIPTION	LAYER	START TIME	
	Microsoft AVD Logon Si...	LogonSimulator_NLAUFJ	Launch of <u>Excel</u> failed for <u>Microsoft AVD Logon Simulator</u> ...	AVD User Experience	Mar 31, 2022 15:12

Figure 1.24: The Current Alarms window reporting logon performance issues

Closing the **Current Alarms** window will reveal the Microsoft AVD Simulator Dashboard (see Figure 1.25).

Synthetic Monitoring									
Simulations: <span>AVD Logon Simulation</span>		External Agents: <span>LogonSimulator_NLAUFJ</span>		Simulations <input type="text"/>					
	APPLICATION/DESKTOP		SIMULATION		WEB URL		USER	WEB LOGON	
								Availability	Duration (Secs)
	Wordpad		LogonSimulator_NLAUFJ		https://rdweb.wvd.microso...		wvduser2@egazureeg...		18.81
	Word		LogonSimulator_NLAUFJ		https://rdweb.wvd.microso...		wvduser2@egazureeg...		23.12
	Excel		LogonSimulator_NLAUFJ		https://rdweb.wvd.microso...		wvduser2@egazureeg...		16.52

Figure 1.25: 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 1.26 will then appear.

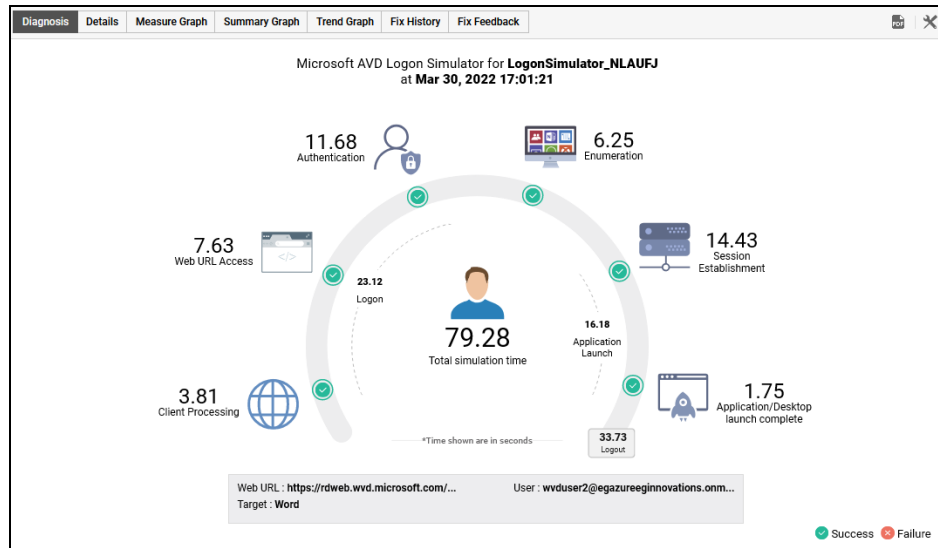


Figure 1.26: The Simulator Dashboard in the eG monitoring console revealing at first glance, the root-cause of logon slowness

A quick look at Figure 1.26 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 1.26, which step of the logon process has caused the slowness.

Similarly, the dashboard can also reveal the exact step at which the simulation failed (see Figure 1.27).

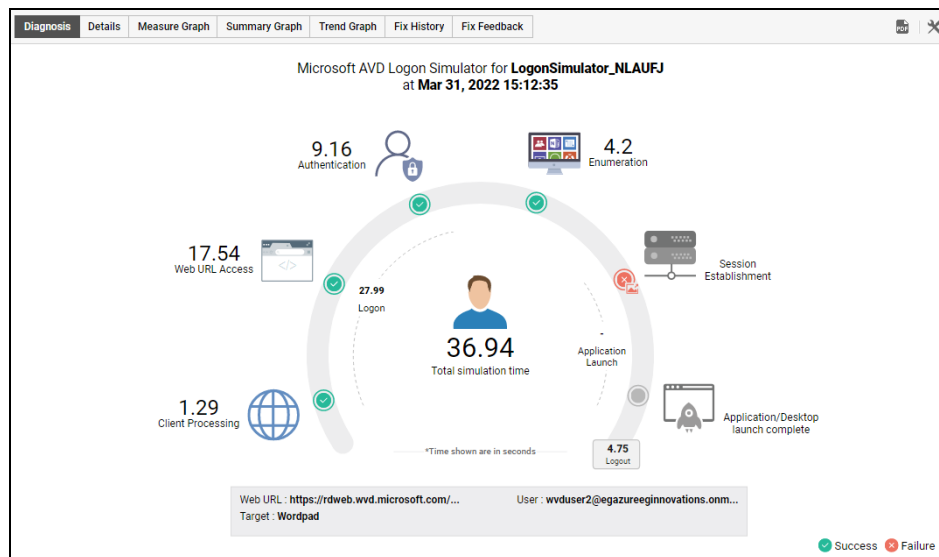



Figure 1.27: The Simulator Dashboard showing that the simulation has failed

Clicking on the  icon in Figure 1.27 will reveal the screenshot that was captured to support the failure.

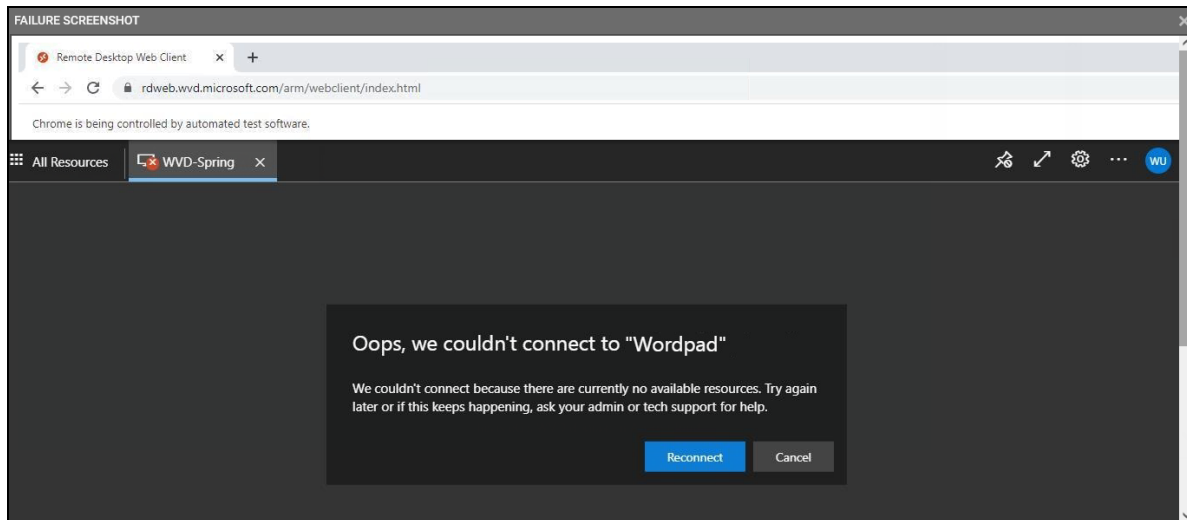


Figure 1.28: A failure screenshot captured by the logon simulator

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 Microsoft Azure infrastructure, 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 1.29 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?

By Application / Desktop								
Zone - --Default--    Component Type - Microsoft AVD Logon Simulator    Application - All    Timeline - Mar 30, 2022 16:23 hrs to Mar 31, 2022 16:23 hrs								
SIMULATION	APPLICATION/DESKTOP	WEB LOGON		APPLICATION/DESKTOP ENUMERATION		APPLICATION/DESKTOP LAUNCH		
		AVAILABILITY (%)	DURATION (SECS)	AVAILABILITY (%)	DURATION (SECS)	AVAILABILITY (%)	DURATION (SECS)	
LogonSimulator_NLAUFJ	Excel	100	✓ 19.88	100	✓ 4.3	78	✓ 16.36	
	Wordpad	95	✓ 20.39	100	✓ 4.47	77	✓ 15.66	
	Word	92	✓ 21.66	100	✓ 5.13	87	✓ 17.42	

Figure 1.29: Logon Simulator - By Application Report

This way, you can rapidly identify the 'pain points' of your Microsoft AVD infrastructure. Zooming into a particular application/desktop in Figure 1.29 will open Figure 1.30. Figure 1.30 provides a quick summary of the results of all simulations performed by the simulator for the chosen application/desktop.



Figure 1.30: Deep dive diagnostics related to the simulations for a particular application/desktop

From Figure 1.30, you can instantly infer if simulations for the application/desktop have failed more often than they have succeeded. If so, Figure 1.30 also points you to the probable cause of



these failures - login? enumeration? or application launch? You can then use the graphs in Figure 1.30 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 1.30. 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 1.31) 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;

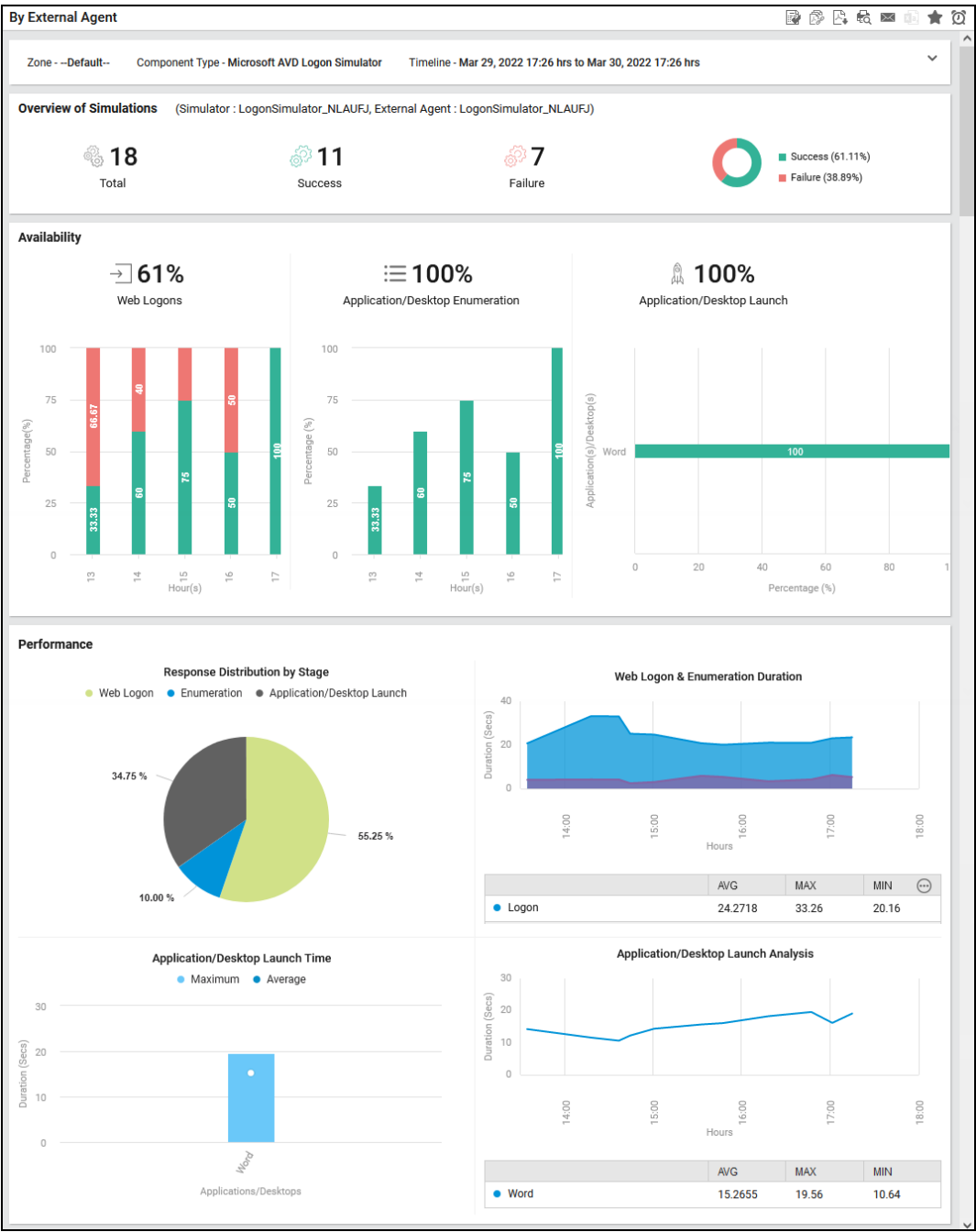


Figure 1.31: Zooming into the simulation results reported by a particular agent

**Note:**

The eG Enterprise Express Logon Simulator for Microsoft AVD 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.

## 1.10 Enabling Email Notifications for Issues


If you want the alerts raised in the eG Enterprise Express Logon Simulator for Microsoft AVD 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 Microsoft AVD.



Figure 1.32: Clicking the User Profile icon

In Figure 1.33 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.

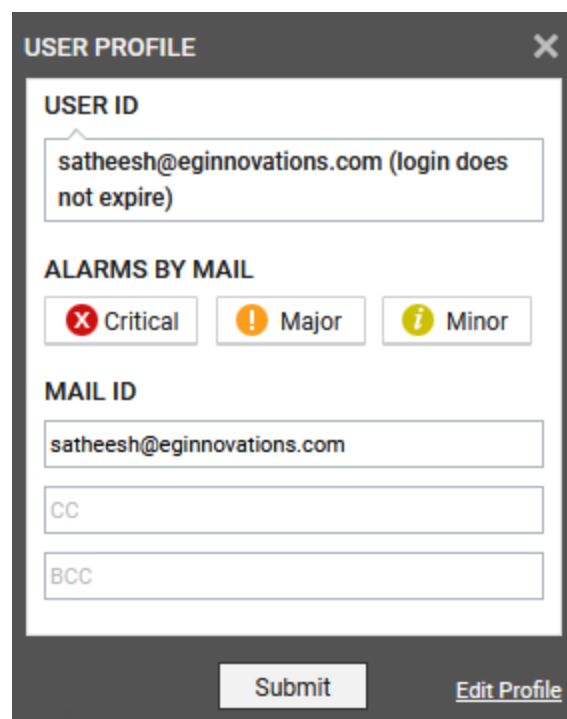

 A screenshot of a 'USER PROFILE' dialog box. The title bar says 'USER PROFILE' with a close button (X). Inside, there's a section for 'USER ID' with a text field containing 'satheesh@eginnovations.com (login does not expire)'. Below that is a section titled 'ALARMS BY MAIL' with three buttons: 'Critical' (with a red X icon), 'Major' (with a yellow exclamation mark icon), and 'Minor' (with a green 'i' icon). The 'Critical' button is selected. Below the alarms section is a 'MAIL ID' section with three text fields: 'satheesh@eginnovations.com' (for the main email), 'CC' (empty), and 'BCC' (empty). At the bottom, there are two buttons: 'Submit' and 'Edit Profile'.

Figure 1.33: Setting the Alarms by Mail flag to Critical

## 1.11 Benefits of the eG Enterprise Express Logon Simulator for Microsoft AVD

The key benefits of the express simulator are as follows:

- **Deliver great user experience for Microsoft Azure users:** Provide fast and uninterrupted services
- **Proactively detect logon issues** before end-users and business services are affected
- **Speed up mean time to resolution (MTTR):** Find and fix Microsoft Azure Virtual Desktop logon problems before users call the helpdesk
- **Benchmark and optimize your Microsoft Azure infrastructure:** Be the first to know if any changes are impacting the logon experience in Microsoft Azure environments
- **Complete visibility into Microsoft Azure Virtual Desktop logon performance:** Monitor real user logon experience and simulation results from a single console

## 1.12 Going Beyond the eG Enterprise Express Logon Simulator for Microsoft AVD

The eG Enterprise Express Logon Simulator for Microsoft AVD is a useful tool for Microsoft Azure administrators to simulate and proactively monitor logon simulation in their environments. You can go beyond the capabilities of the free logon simulator and get comprehensive Microsoft Azure monitoring, diagnosing and troubleshooting capabilities with eG Enterprise – a Microsoft Azure Ready performance monitoring solution for any size Azure 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 Microsoft AVD and eG Enterprise Microsoft AVD Monitoring Suite**

Key Features	eG Enterprise Express Logon Simulator for Microsoft AVD	eG Enterprise (Full-Featured Microsoft Azure Virtual Desktop Monitoring Solution)
<b>Logon Simulation</b>		
Number of Microsoft Azure 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

<b>In-Depth Microsoft Azure Virtual Desktop Performance Monitoring</b>		
Simulate the entire Microsoft Azure Virtual Desktop session (including user access to published applications)	No	Yes
Real user experience monitoring (Blast Extreme/PCoIP/RDP)	No	Yes
Performance monitoring of Microsoft Azure, Microsoft Azure AD Connect, Microsoft Azure Subscription Service 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](http://www.eginnovations.com).

### Contact Us

For support queries, email [support@eginnovations.com](mailto:support@eginnovations.com).

To contact eG Innovations sales team, email [sales@eginnovations.com](mailto:sales@eginnovations.com).

Copyright © 2023 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.