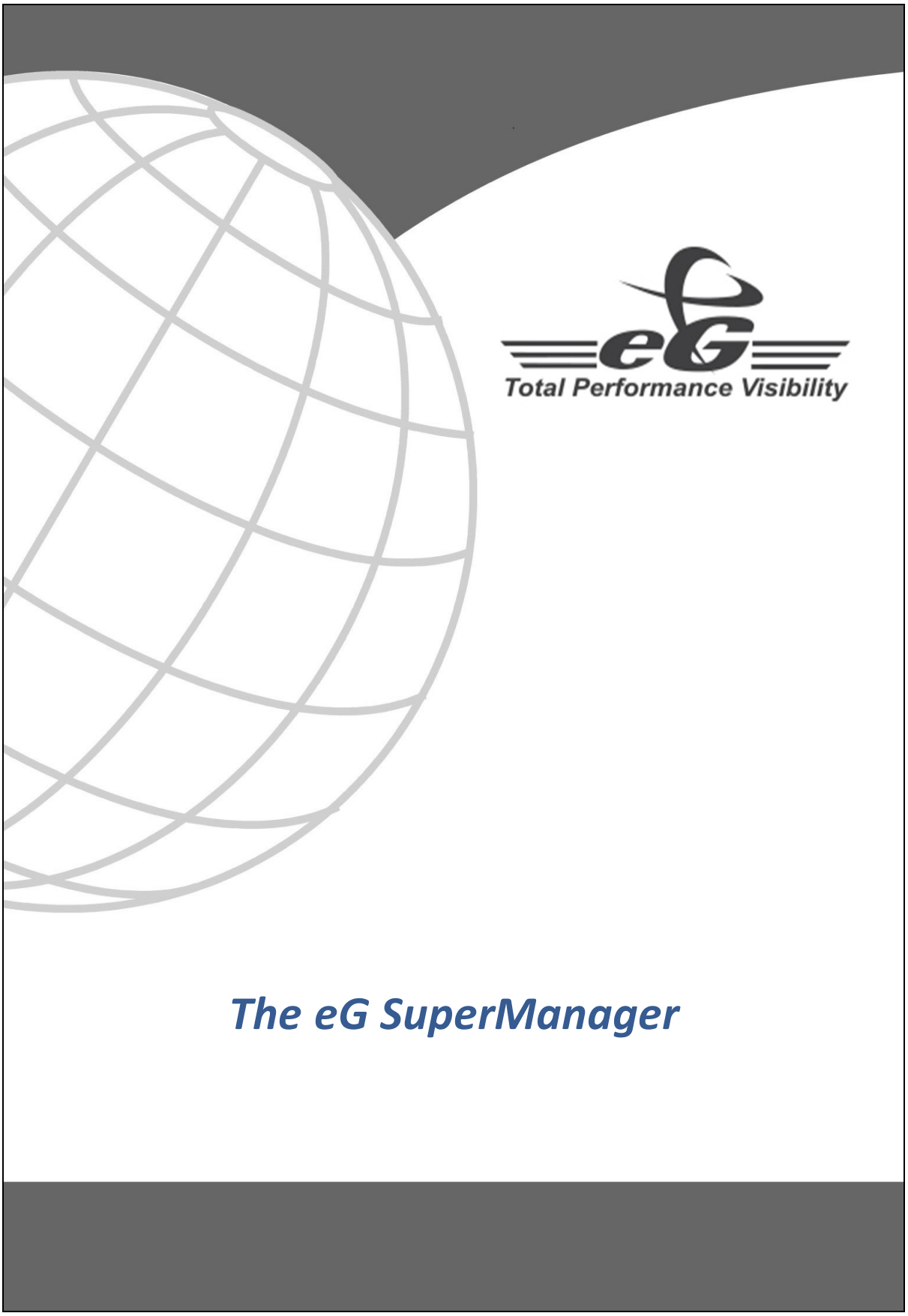


The eG SuperManager

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations Inc. eG Innovations Inc. 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.

Trademarks

Microsoft Windows, Windows 2008, Windows 7, Windows 8, Windows 10, Windows 2012, Windows 2016 and Windows 2019 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

©2020 eG Innovations Inc. All rights reserved.

Table of Contents

Table of Figures

Chapter 1: Introduction

Large enterprises often have thousands of devices, servers, and applications that have to be managed, and a single eG management console may not have the capacity to handle the entire enterprise. To support such enterprises, multiple eG managers may be needed. However, if each of these managers operate independently, they may not provide a common view of the entire enterprise. Hence, it could be very cumbersome to have the IT staff of the enterprise login to different eG management consoles to get a complete view of the status of the target infrastructure.

A SuperManager is a manager of managers that provides a consolidated view of the status of the IT infrastructure that is being handled by different eG managers. The eG suite offers two options for configuring a SuperManager. The **eG SuperManager** is a 100% web-based component of the eG suite that provides a consolidated view across disparate eG managers. On the other hand, an administrator can also use the Computer Associates Network and System Management (NSM) product as a super manager. The following sections however, discuss the **eG SuperManager** option alone.

To configure an eG SuperManager, you first need to ensure that the eG SuperManager license is enabled for your eG installation.

There are three main reasons why a SuperManager is necessary in an enterprise environment.

- **Scale of operation:** Large enterprises may comprise of thousands of devices, servers, and applications, and a single eG manager may not be sufficient to manage this environment. Hence, a multi-level architecture with individual eG managers reporting to a SuperManager is necessary.
- **Autonomous domains:** Large enterprises often comprise of multiple domains, which are managed autonomously. Each domain may require a separate eG manager, but there could be a common support team that is responsible for first level support for all the domains. The same situation could occur in a managed services environment as well - the manager service provider (MSP) is responsible for supporting different customer infrastructures (possibly from a central location) but each customer may prefer to have their separate management consoles for administration. In this case, the support organization/MSP will need a consolidated view of the status of the infrastructure across the different domains.
- **Geographically distributed environments:** Large enterprises will span multiple geographical locations and multiple eG managers – one per location – may be preferred so as to reduce the bandwidth involved in communicating all the measurements to a central

console. In this case, a common support organization may be involved, thereby necessitating a management console that consolidates the status across the individual eG managers.

The **eG SuperManager** is a central entity that integrates with multiple eG managers and provides a consolidated view of the infrastructure being monitored by each of the managers. Figure 1.1 depicts how the eG SuperManager works.

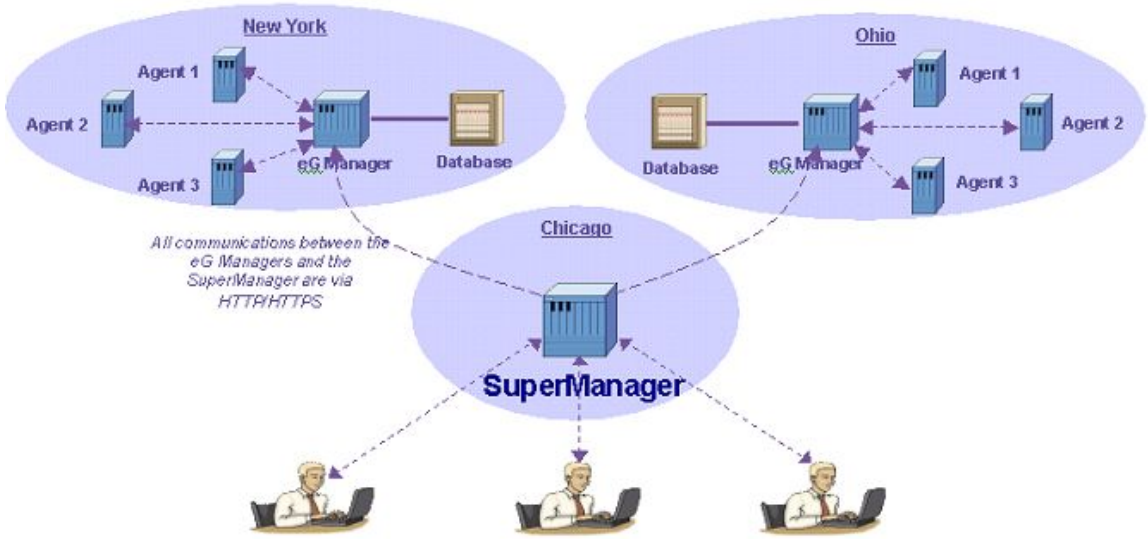


Figure 1.1: How the eG SuperManager works

The salient features of the eG SuperManager are discussed hereunder:

- **HTTP/HTTPS communication between the eG SuperManager and eG Manager:**

  When it is configured, the eG SuperManager is provided with the details of the individual managers that are reporting to it. Periodically, the eG SuperManager polls the individual eG managers at a pre-defined interval, collects status information from them, consolidates the information, and provides it to users. All communication between the eG SuperManager and the individual managers happen over HTTP/HTTPS.

  The SuperManager initiates all communication with each of eG managers in its control. Therefore, if a firewall exists between the managers and the SuperManager, this firewall should be configured to allow connections initiated by the SuperManager to the individual managers (see Figure 1.2).

  Also, when a user who logs into the eG SuperManager interface clicks on an alarm in the current alarms window, or the manager name in the home page, he/she would be redirected to the corresponding manager's console wherein further diagnosis can be performed. To

facilitate this, network connectivity should be provided such that all users have direct connectivity not only to the SuperManager but also to the individual managers (see Figure 1.2).

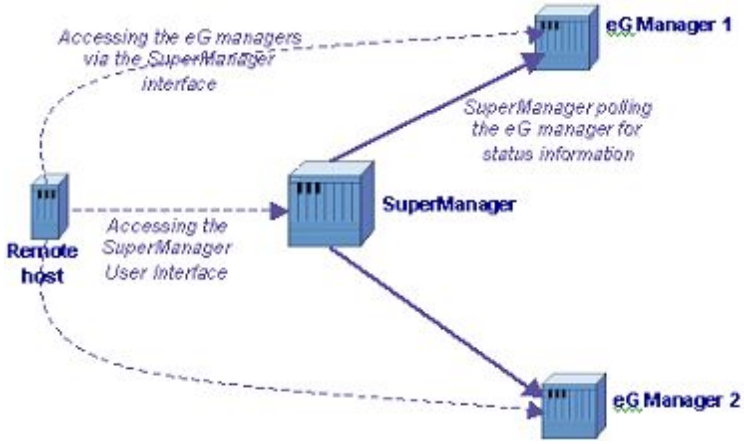


Figure 1.2: Remote host accessing the SuperManager and individual managers

- **Configured to work in NATed Environment:**

  In many large environments, there may be multiple demilitarized zones, with firewalls between the eG SuperManager and the eG managers. The geographic locations of the SuperManager and the eG managers may also be different. In such cases, the eG SuperManager cannot be accessed using a private IP address. For the eG SuperManager to be accessed externally by the eG managers, network address translation can be setup so that the eG SuperManager is accessed over the internet using a public IP address.

- **Manages redundant clusters:**

  If one of the managers that it operates with is part of a redundant cluster, the eG SuperManager will first try to communicate with the primary manager of the cluster. If the primary manager is not reachable, the eG SuperManager will automatically try to communicate with the secondary manager of the cluster.

- **Minimal dependence on Local data storage:**

  The eG SuperManager has an exclusive database to store specific data such as user logins, user preferences etc related to all the managers that are reporting to the SuperManager. Once these data are polled in the database of the SuperManager, whenever the user of an individual manager logs in, the SuperManager would check the database to find out which of the managers reporting to the SuperManager allows access to the user. Moreover, the database of the SuperManager does not store metrics reported by each of the individual

managers reporting to the SuperManager. Instead, the SuperManager contacts the managers based on the user logged in, collects the required information from the managers and displays the information upfront. Nowhere does the SuperManager stores metrics collected from the managers reporting to the SuperManager. This architecture of the SuperManager considerably saves time since the SuperManager need not contact all the managers to figure out the user logged in and moreover database overhead of storing scores of metrics is avoided thereby increasing the efficiency of the SuperManager.

Note:

A user can login to the SuperManager as long as he/she is a registered user of one or more of the managers reporting to the SuperManager.

If a user is registered with one of the managers alone, the view that the user sees is consistent with what he/she would see if they were to login to the manager to which they were registered directly. On the other hand, if the user is registered with more than one manager, the SuperManager produces a consolidated view based on the responses from the individual managers.

Note:

In its current implementation, the eG SuperManager mainly serves as a central console where users can get a consolidated view of alerts from different managers. Any configuration changes necessary have to be performed directly on the individual managers.

- **Supports eG managers with heterogeneous configurations:**

  The individual managers reporting to a SuperManager can have heterogeneous configurations. For example, one of the managers can be running on Microsoft Windows, whereas another could be running on Sun Solaris. Likewise, the databases of the individual managers can also be different – for example, one of the managers may use Microsoft SQL server as the database, while another may use Oracle as the database.

- **Supports multiple languages:**

  The alarm and dashboard displays in the eG SuperManager console are language-customizable! The language preferences set by the users registered with each of the managers reporting to the SuperManager, will affect the alarm and dashboard displays in the eG SuperManager console as well. For example, say that a user to an eG manager at *Spain* chooses *Spanish* as the language in which he/she would prefer to view performance information reported to the manager. When such a user logs into the SuperManager that manages the *Spain* manager, the alarms and performance details pertaining to that user will be displayed in the eG SuperManager console in the *Spanish* language only. Moreover, if the

managers reporting to a SuperManager are double-byte enabled and support double-byte languages such as Chinese or Japanese, then the SuperManager interface too will display data in double-byte.

- **No change in agent architecture:**

  In this architecture, since the agents continue to report to their respective eG managers, there is no change needed in the eG agent architecture.

The eG SuperManager can be applied in the following environments:

- In a large enterprise with thousands of devices, servers, and applications, the eG SuperManager ensures that the eG suite can scale to handle such an environment;
- In a distributed network, eG managers can be installed in each domain of the network and managed autonomously; At the same time, using the eG SuperManager, a single integrated console can be provided for the support team that is responsible for monitoring each of the domains;
- In a managed service environment, each customer network could have an independent eG manager, but with an eG SuperManager installed, the managed service provider could get an integrated view of the status of all the customer networks that they are responsible for managing.

The chapters to come will elaborately discuss how to install and configure the eG SuperManager.

1.1 Sizing the Hardware and Database Required by an eG SuperManager

Before deploying an eG SuperManager to monitor your infrastructure, it is essential to determine the hardware required to host the eG SuperManager. The eG database also has to be configured appropriately to ensure that sufficient client connections can be simultaneously established from the eG SuperManager to the eG database server.

Clearly, as the number of infrastructure components that each eG manager reporting to an eG SuperManager is handling increases, the resource requirements for the eG SuperManager will increase. The resources to be considered when determining the configuration of the eG SuperManager and eG database include:

- CPU availability
- RAM availability
- Disk space availability

- Simultaneous client connections that can be established by the eG manager to the eG database
- Database IOPS

To determine the sizing of the eG SuperManager and eG database, you first need a count on the eG managers reporting to the eG SuperManager and also the number of components managed by each eG manager.

The table below provides thumb-rules that can be used to configure the eG manager and database for your infrastructure.

Resources	eG SuperManager	eG Database
CPU	Minimum 4 GHz and 2 vCPUs.Add 1 GHz processing for every 100 monitoring units	Minimum 4 GHz and 2 vCPUs.
Memory	8 GB. Add 1 GB RAM for every 100 monitoring units of each eG manager.	Minimum 2GB
Disk Storage	1 GB	

Chapter 2: Installing and Configuring the eG SuperManager

The procedure for installing the eG SuperManager differs according to the operating system used on the server on which the SuperManager is to be installed. The eG SuperManager is available for Windows 2008/2012/2016/2019, Windows 7, Windows 8 and Windows 10 operating system environments. This section describes the steps involved in installing and configuring the eG SuperManager on Windows operating system environments.

Prior to installing the eG SuperManager, ensure that the pre-requisites provided in Section **2.1** are in place.

2.1 Prerequisites for Windows Installation of the eG SuperManager

Following are the pre-requisites that should be fulfilled before installing the eG SuperManager:

1. Minimum requirement: OpenJDK 12 and above Recommended: OpenJDK 12 and above - By default, the OpenJDK is pre-bundled with the eG SuerManager setup.
2. Windows 2008, Windows 2012, Windows 2016, Windows 2019, Windows 7, Windows 8, Windows 10 servers
3. Only systems with a static IP address (i.e., no DHCP address) should be used for installing the eG SuperManager
4. A minimum of 8 GB RAM would be required for installing the eG SuperManager on a 64-bit host
5. A minimum of 1 GB disk space
6. Internet Explorer Version 10, 11 or Edge (OR) Google Chrome version 28 or above (OR) Mozilla Firefox Version 18 or above
7. A valid eG SuperManager license

   Note:

   The eG SuperManager and the eG Manager cannot exist on the same host.

2.1.1 Installing and Configuring the eG SuperManager on Windows

The broad steps involved in the eG SuperManager's installation and configuration process are as follows:

1. Installing the eG SuperManager
2. Configuring the eG Database
3. Configuring the Basic Manager Settings

A user-friendly wizard enables you to perform each of these steps seamlessly. A single self-extracting program drives this wizard. Based on what flavor/version of Windows is in use, you have to choose from the following self-extracting programs:

- The **eGManager_win2008_x64.exe**, if you are installing the eG SuperManager on a 64-bit Windows 2008/Windows 7 host;
- The **eGManager_win2012_x64.exe**, if you are installing the eG SuperManager on a 64-bit Windows 8/Windows 2012 host;
- The **eGManager_win2016_x64.exe**, if you are installing the eG SuperManager on a 64-bit Windows 2016/Windows 10 host;
- The **eGManager_win2019_x64.exe**, if you are installing the eG SuperManager on a 64-bit Windows 2019 host;

Once you pick the executable that is ideal for your environment, proceed to install the eG SuperManager.

2.1.1.1 Installing the eG SuperManager

To begin the installation, double-click on the corresponding executable. The installation wizard that then appears guides you through the installation process.

1. The **Welcome** screen appears first. Click the **Next** button here to continue with the setup.

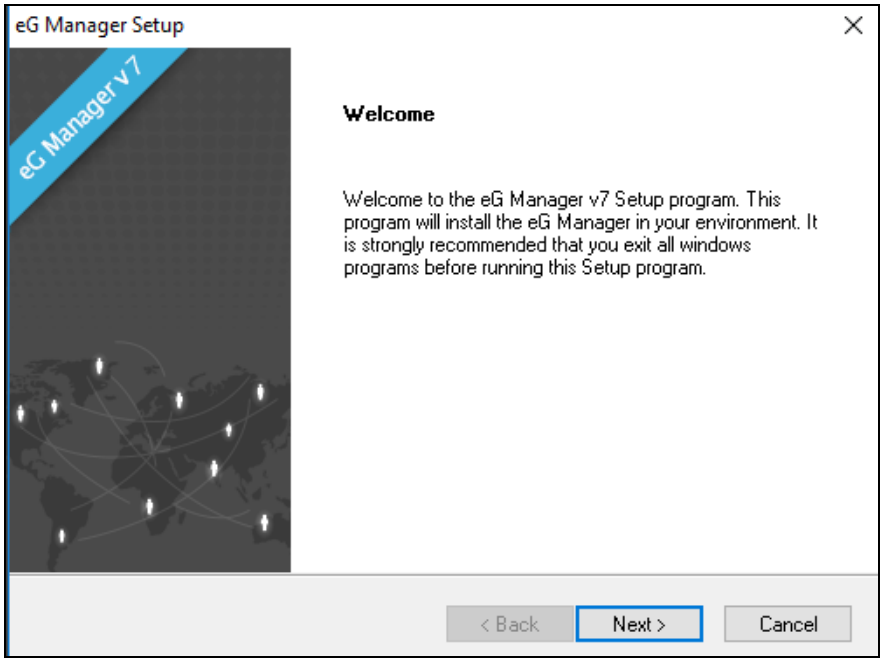


Figure 2.1: The Welcome screen of the installation wizard

2. Accept the license agreement that follows by clicking the **Yes** button therein (see Figure 2.2).

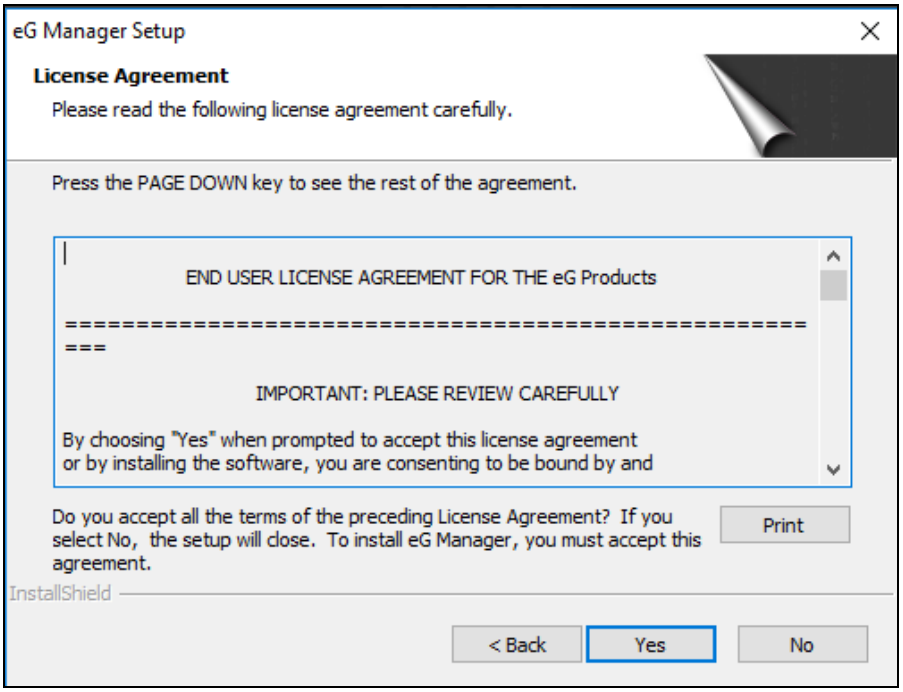


Figure 2.2: Accepting the license agreement for installing the eG SuperManager

3. The setup process now requires the hostname and port number of the host on which the eG SuperManager is being configured (see Figure 2.3). By default, setup auto-discovers the host name and the IP address(es) of the eG SuperManager host, and makes it available for selection inFigure 2.3. You can pick the host name or any of the IP addresses listed therein to take the eG SuperManager installation forward. If the IP address/host name that you want to use for your eG SuperManager is not discovered for some reason, then, you can choose the **Other** option in Figure 2.3. This will invoke Figure 2.4 where you can manually specifiy the IP address/host name of the eG SuperManager. If the domain name service is used in the target environment, use the full hostname. Otherwise, specify the IP address. However, 7077 is the default port. You can change this port if you so need.

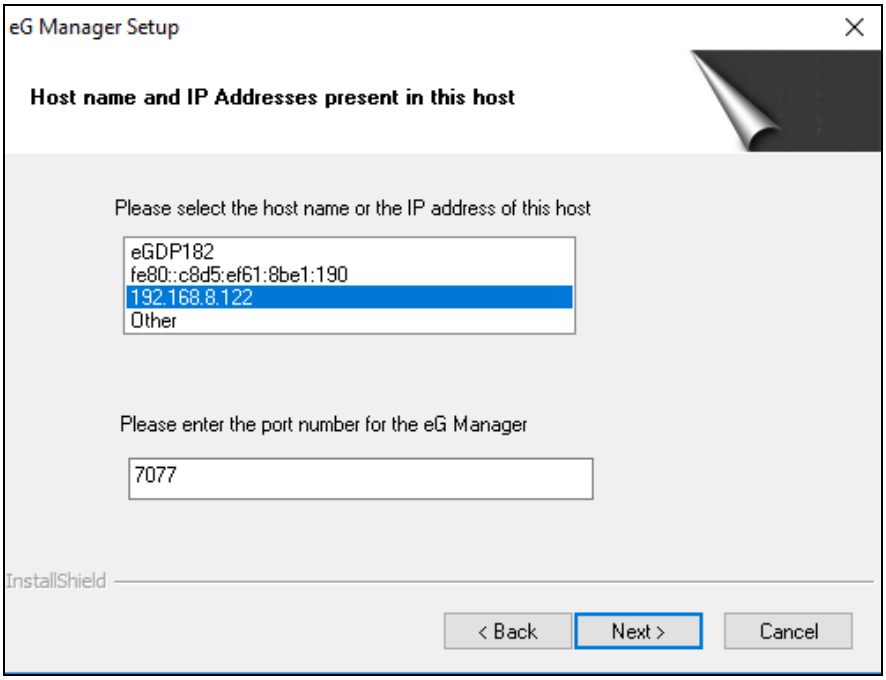


Figure 2.3: Selecting the IP address/host name to use for the eG SuperManager

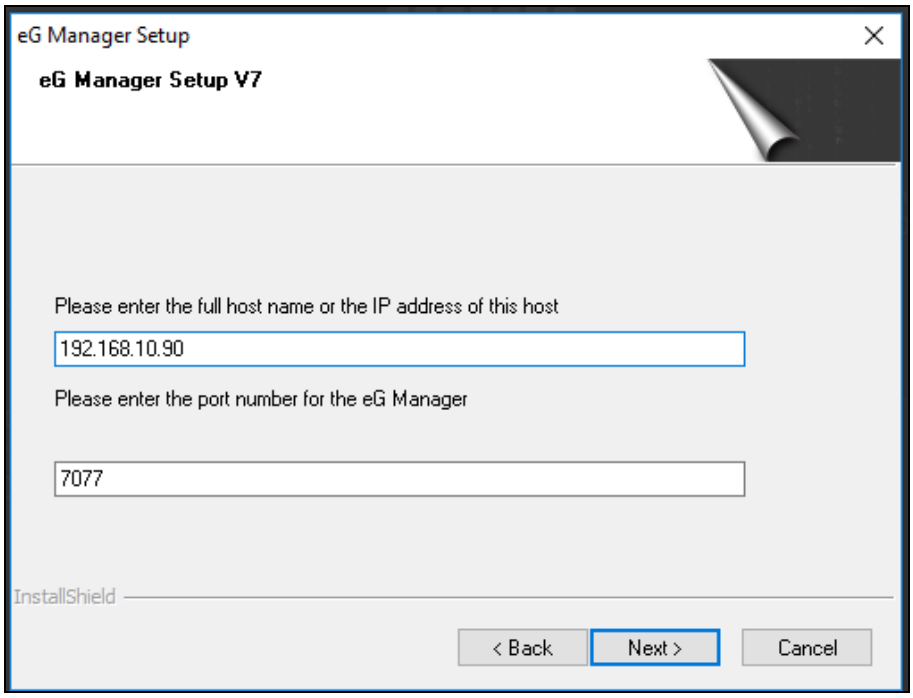


Figure 2.4: Hostname and port number of the system on which the eG SuperManager will execute

Note:

- While specifying the host name/IP address of the manager, please take care of the following aspects:

  a. If the host name is provided when installing the manager, use this name (and not the IP address) for accessing the user interface via the web browser.

  b. If the host name is provided, make sure that forward and reverse lookups for this name are enabled via the DNS service in the target environment.

- When providing an IP address for the eG SuperManager, note that only an IPv4 address can be provided. To configure the eG SuperManager on a host that has been configured with an IPv6 address, you will have to provide the fully-qualified host name of that host or an alias name, in Figure 2.4.

4. The eG Enterprise system provides users with the option to view and key in data in a language of their choice. Different users connecting to the same manager can view data in different languages. However, some languages such as Chinese, Japanese, and Korean, support a double-byte character set. To view data in the eG user interface in Chinese, Korean, or Japanese, the eG SuperManager should be explicitly configured to display and process double-byte characters. In such a case, enable double-byte support for the eG SuperManager by clicking the **Yes** button in the figure below. On the other hand, for handling the character sets of other

languages (example: French, German, Spanish, Portugese, etc.), the eG SuperManager need not be double-byte enabled. At such times, click the **No** button to disable double-byte support for the eG SuperManager.

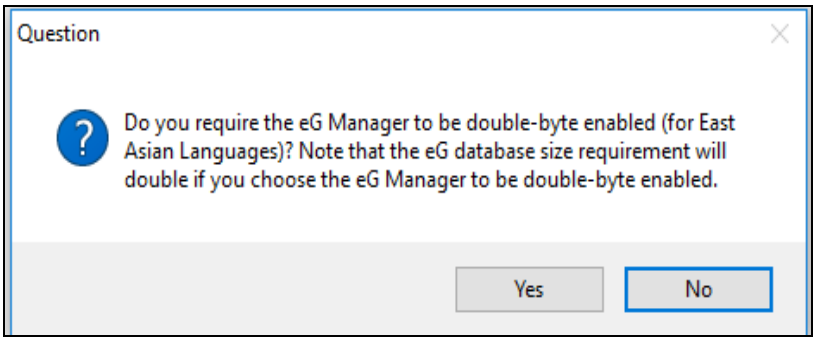


Figure 2.5: Enabling double-byte support for the eG SuperManager

Note:

For a detailed discussion on how to enable double-byte support for eG Enterprise, refer to Configuring Double-byte Support for eG Enterprise .

5. Setup then prompts you to indicate if the eG SuperManager is to be SSL-enabled. If so, click **Yes**. If not, click **No**.

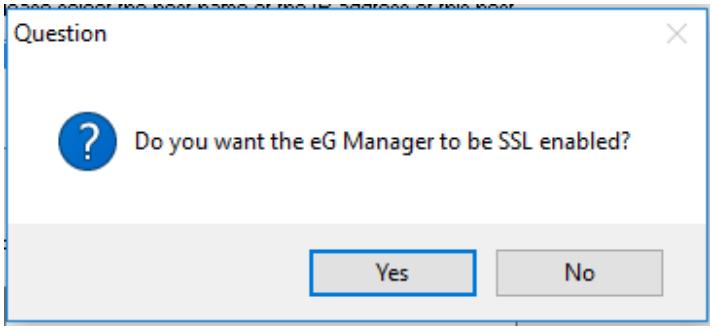


Figure 2.6: Indicating whether/not to SSL-enable the eG SuperManager

6. Next, indicate where the eG SuperManager is to be installed. By default, setup installs the eG SuperManager in the C drive. If you want the eG SuperManager installed in a different directory, use the **Browse** button in Figure 2.7. Then, click the **Next** button in Figure 2.7 to move to the next step.

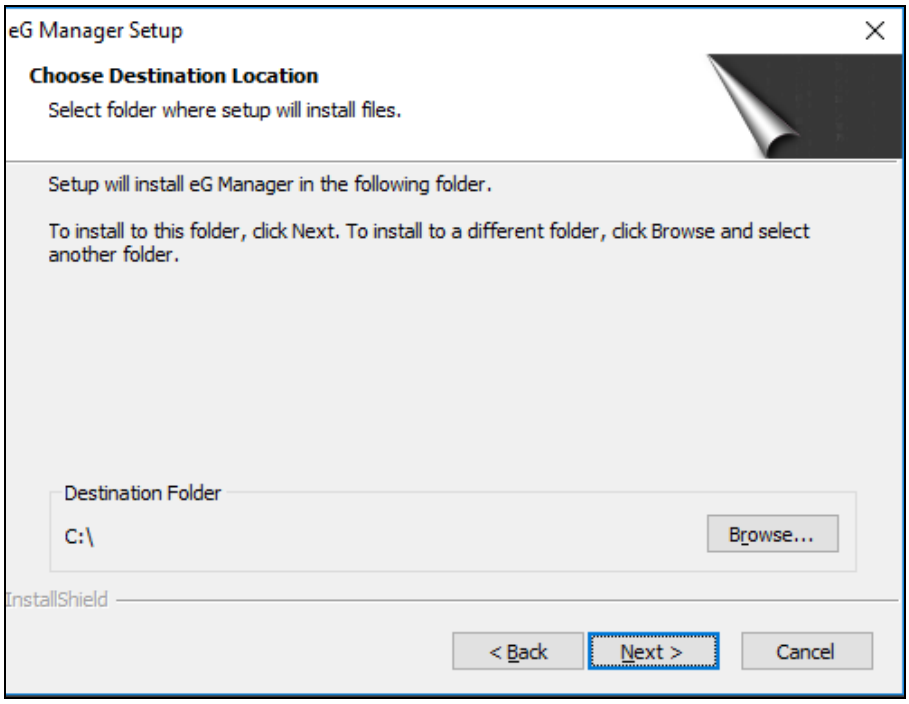


Figure 2.7: Specifying the location of the eG SuperManager

7. Figure 2.8 then appears, using which you can quickly review your install specifications. To proceed, click the Next button in Figure 2.8.

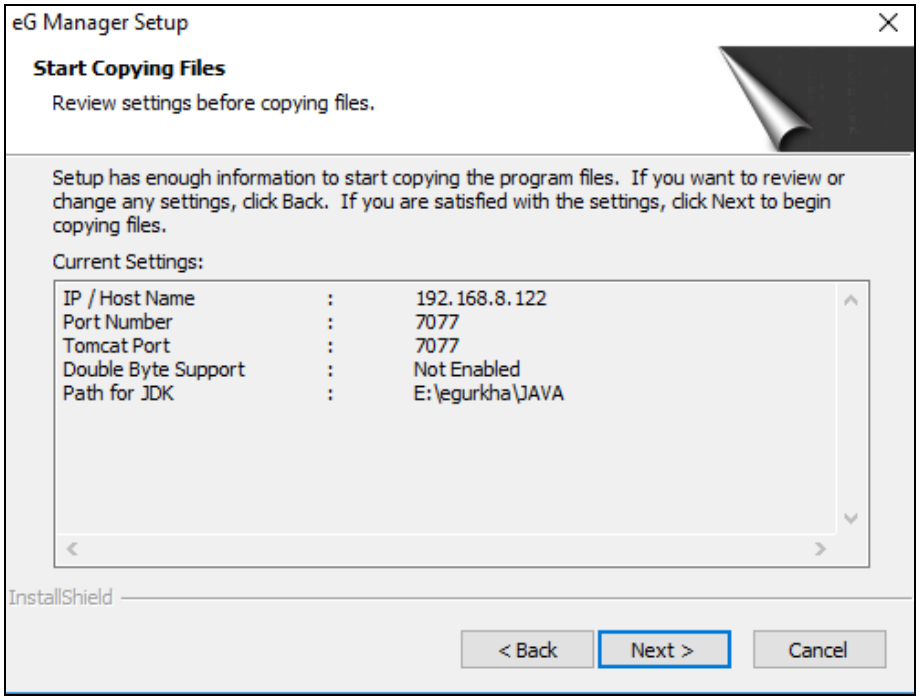


Figure 2.8: Reviewing the install settings

8. This will begin the eG SuperManager installation. During this process, setup automatically extracts and deploys the built-in JDK - OpenJDK 12 - for the eG SuperManager's use. Additionally, setup also automatically configures and readies the built-in Apache Tomcat server, so that the eG SuperManager can service web requests to it efficiently. Once the installation completes successfully, the message depicted by Figure 2.9 will appear.

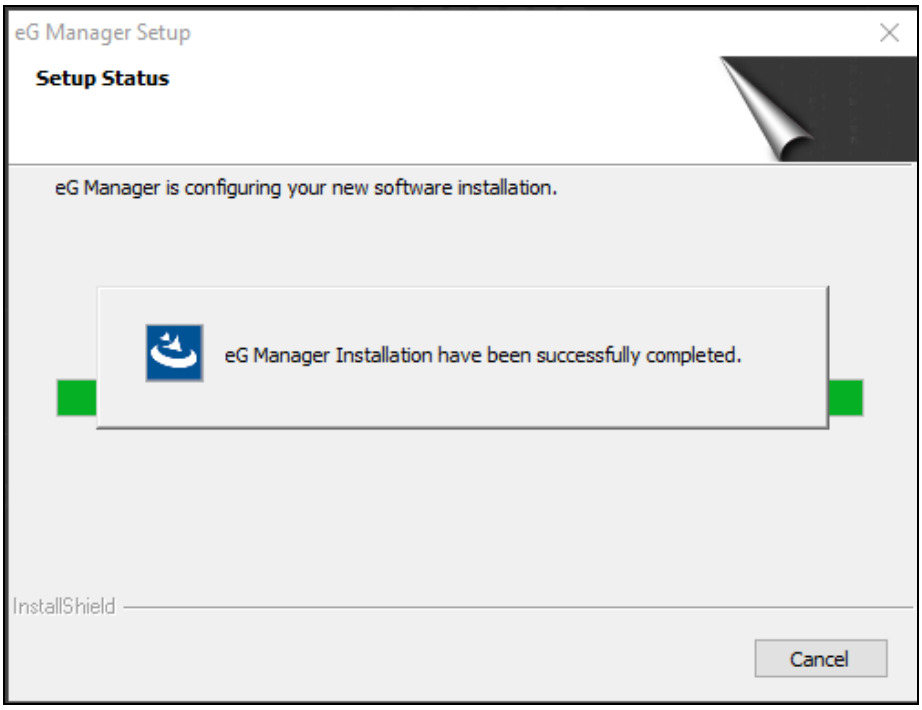


Figure 2.9: The message confirming the successful eG SuperManager installation

2.1.1.2 Configuring the eG Database

After installing the eG SuperManager, proceed to configure the eG database. The eG SuperManager stores real-time performance metrics, history of alarms, detailed diagnostics, thresholds, and even performance trends in this database.

If a SQL database pre-exists on Microsoft Azure, you can configure such a database as the eG database. On the other hand, if a Microsoft Azure SQL database is not in use in your environment, then it is essential to ensure that an Oracle / Microsoft SQL server is available to host the eG database. Such a database server can either reside on the eG SuperManager itself or it could be hosted on an external server.

To enable you to easily configure an eG database, setup automatically leads you to a special web page, soon after the successful installation of the eG SuperManager. Using this web page, you can

pick a backend for the eG SuperManager, and configure an eG database on it. The sections below elaborately discuss how this web page can be used to perform the following:

- Configure a Microsoft SQL database (on a Microsoft SQL server or on Microsoft Azure) as the eG database;
- Configure a database on an Oracle database server as the eG database;

2.1.1.2.1 Using Microsoft SQL Database

As soon as the web page opens, the **Microsoft SQL Server** tab page opens in it by default (see Figure 2.10).

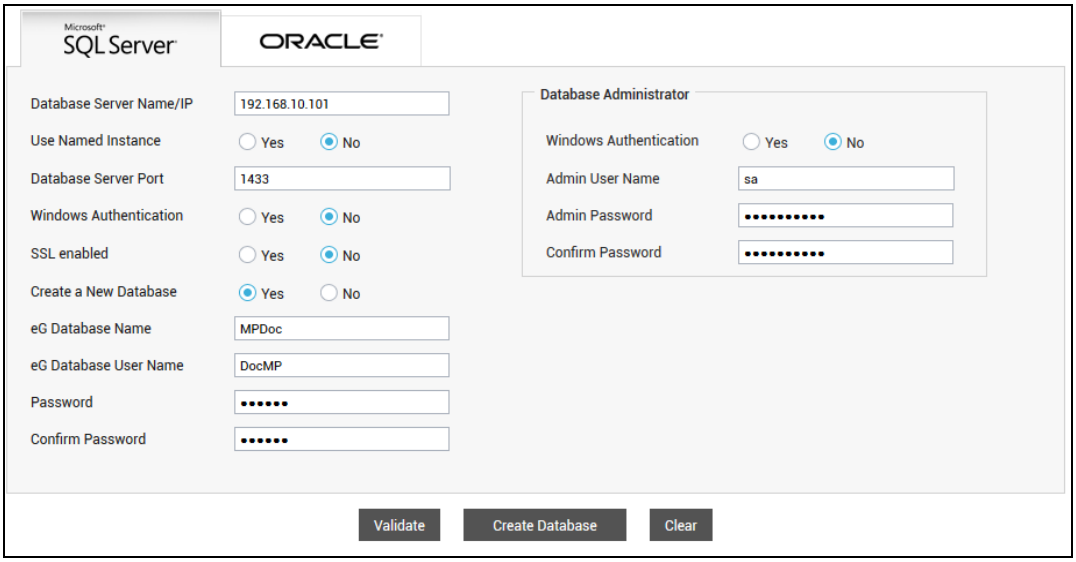


Figure 2.10: Configuring the eG database on a Microsoft SQL Server

If you choose to configure an Microsoft SQL database (on Azure or on a Microsoft SQL server) as the eG backend, then do the following using Figure 2.10:

1. First, enter the location of the Microsoft SQL server by specifying the hostname and port on which the server is hosted against **Database Server Name/IP**. If you have already configured a SQL database on Microsoft Azure and want to use this database as the eG database, then, against **Database Server Name/IP**, provide the fully-qualified SQL server name that Azure auto-generates when creating a SQL database.

   Note:

- If the Microsoft SQL server being configured is part of a Microsoft SQL Cluster, then make sure you specify the virtual cluster IP address / cluster name as the hostname / IP address of the Microsoft SQL server in Figure 10
- If the Microsoft SQL server being configured is part of an SQL AlwaysOn Availability Group, then make sure you specify the name of the *availability group listener* as the hostname / IP address of the Microsoft SQL server. An availability group listener is the name of the SQL server to which clients can connect in order to access a database in a primary or secondary replica of an AlwaysOn availability group. If such a SQL server is not configured with a listener name, then enter the virtual cluster IP address or cluster name against hostname / IP address.

2. If the Microsoft SQL server being configured uses named instances, then set the **Use Named Instance** flag to **Yes**. Then, specify the name of the instance against the **Instance Name** field, as depicted by Figure 2.11.

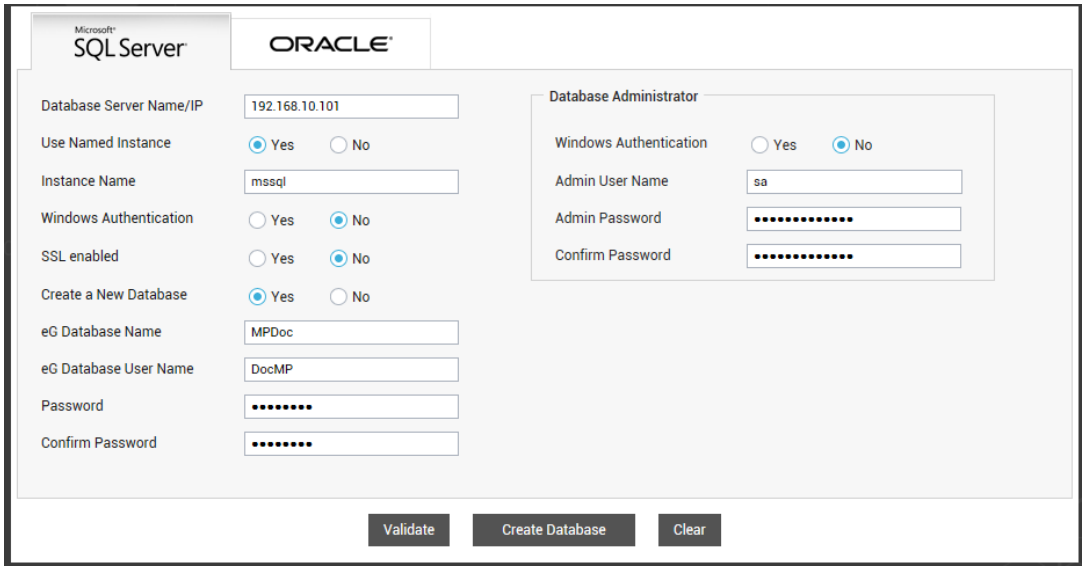


Figure 2.11: Specifying the name of the SQL server instance to use

3. On the other hand, if the Microsoft SQL server does not use named instances, then set the **Use Named Instance** flag to **No**, and enter the port at which the SQL server listens in the **Database Server Port** text box (see Figure 2.10).

4. Next, indicate what type of authentication is enabled for the target Microsoft SQL server. If Windows authentication is enabled, then set the **Windows Authentication** flag to **Yes**. If SQL Server authentication is enabled, then set the **Windows Authentication** flag to **No**. Note that if you are configuring a SQL database on Azure as the eG database, you have to set the **Windows Authentication** flag to **No** only, as Microsoft Azure SQL Database supports only **SQL Server Authentication** by default.

5. If the **Windows Authentication** flag is set to **Yes**, then an additional **NTLMv2 enabled** flag will appear (see Figure 2.12). In some Windows networks, *NTLM* (*NT LAN Manager*) may be enabled. NTLM is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. NTLM version 2 ("NTLMv2") was concocted to address the security issues present in NTLM.If NTLMv2 is enabled for the target Microsoft SQL server, then set the **NTLMv2 enabled** flag to **Yes**; else, set it to **No**.

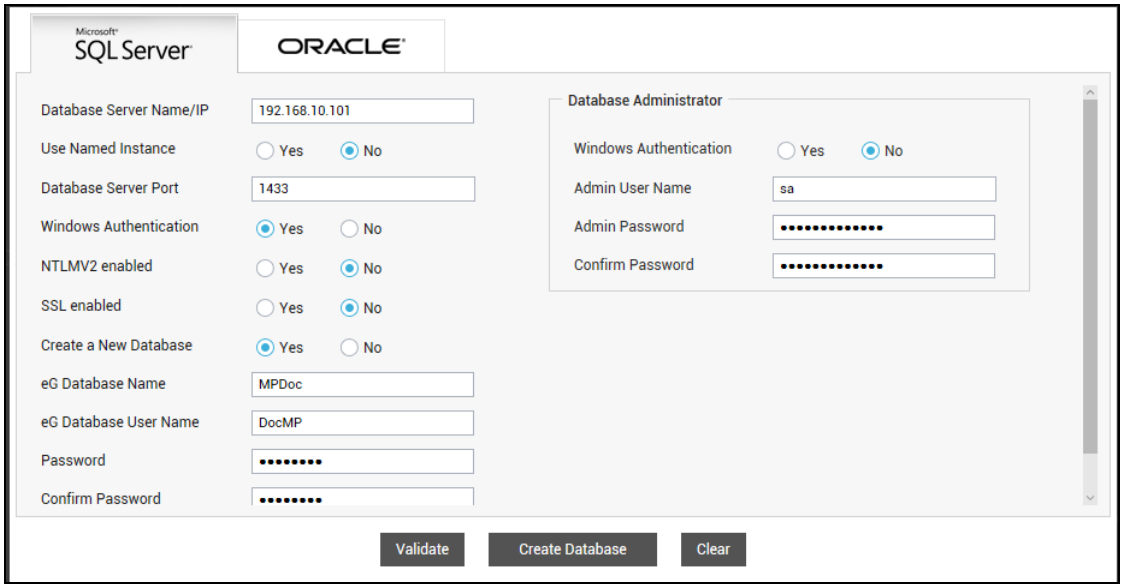


Figure 2.12: Indicating whether/not the Microsoft SQL server is NTLMv2 -enabled

6. Then, you need to indicate whether the Microsoft SQL server instance that will be hosting the eG database is SSL-enabled or not. If not, set the **SSL enabled** flag to **No**; if it is SSL-enabled, set the flag to **Yes**. However, when configuring an existing SQL database on Azure as the eG database, you must set the **SSL enabled** flag to **Yes**, as the SQL server instance that Azure creates is SSL-enabled by default.

7. Next, specify whether/not a new database has to be created to host the eG database. To create a new database, set the **Create a New Database** flag to **Yes**. To use an existing database instead, set the **Create a New Database** flag to **No**. This means that to use a SQL database that pre-exists on Azure, you need to set the **Create a New Database** flag to **No**.

8. If the **Create a New Database** flag is set to **Yes**, then specify the name of the new database that you want to create in the **eG Database Name** text box (see Figure 2.12). On the other hand, if the **Create a New Database** flag is set to **No**, then, in the **Existing databasename** text box, mention the name of the existing database in which the eG SuperManager will be storing metrics (see Figure 2.13). When using an existing SQL database on Azure therefore, enter the name you

assigned to that database when you created it on Azure, against **Existing database name**.

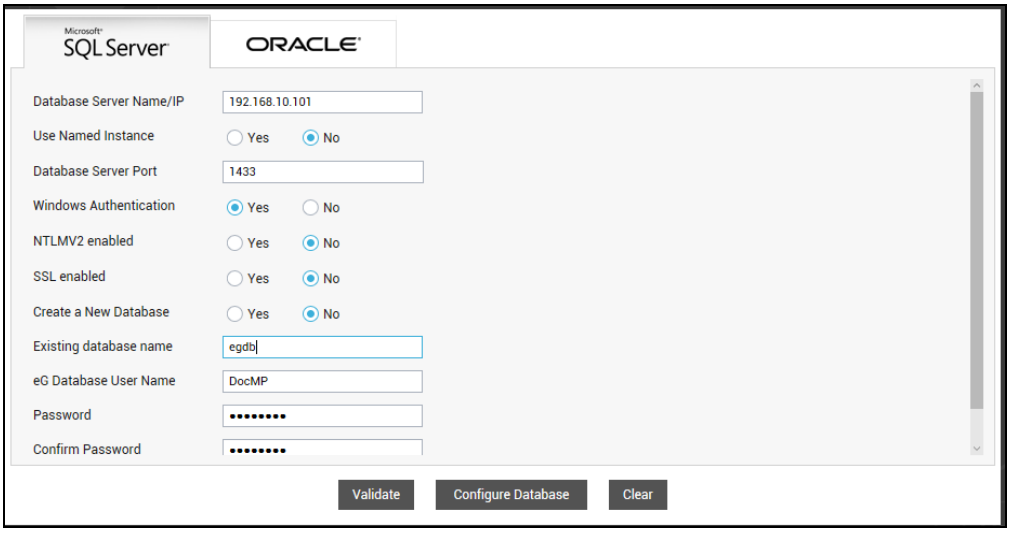


Figure 2.13: Using an existing database on the Microsoft SQL server as the eG database

9. The eG database is created in the Microsoft SQL server's database using a special user account. Next, specify the user name and password to be used for this account. If you want to create a new database for the eG SuperManager - i.e., if you have set the **Create a New Database** flag to **Yes** and have specified a new **eG Database Name** (see Figure 2.12) - then you can use either a new user account for creating that database, or an existing user account. However, if you want to use an existing database as the eG database - i.e., if you have set the **Create a New Database** flag to **No** and have specified an **Existing database** name (see Figure 2.13) - then you should use an existing user account alone for configuring that database. When using the SQL database on Azure therefore, use the user account you associated with that database when creating it on Azure.

   Note:

   When using an existing user account on a Microsoft SQL server, make sure that you use an account vested with *DBOwner* rights on the specified database.

10. If **Windows Authentication** is enabled on the Microsoft SQL server - i.e., if the **Windows Authentication** flag is set to **Yes** - then the user should be a valid Windows domain user. Accordingly, provide a valid domain user's name against **eG Database User Name**, type the password of that user against **Password**, confirm the password by retyping it against **Confirm Password**, and specify the **Domain Name** to which that user belongs (see Figure 2.14).

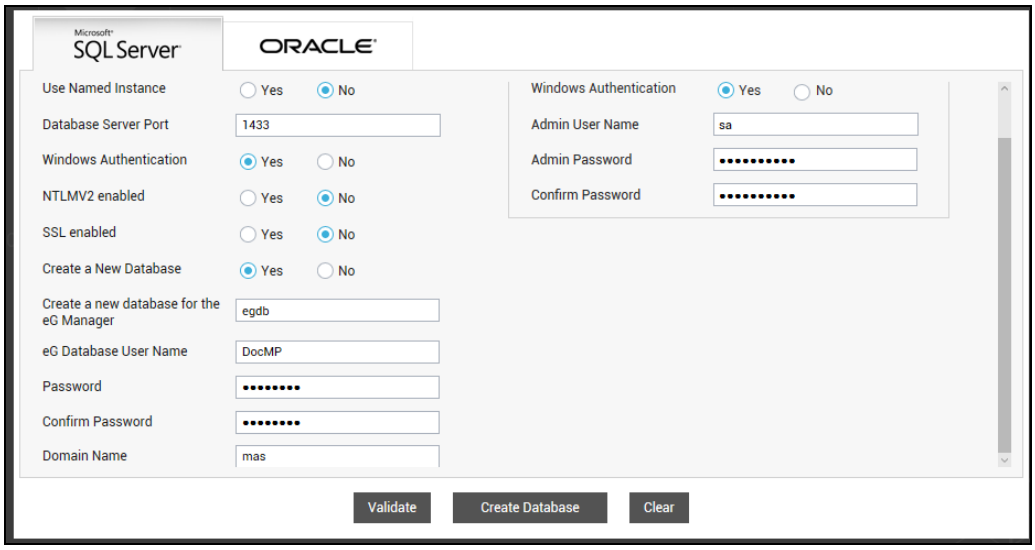


Figure 2.14: Specifying the credentials of the special database user, when Windows Authentication is enabled

11. On the other hand, if **SQL Server Authentication** is enabled on the Microsoft SQL Server - i.e., if the **Windows Authentication** flag is set to **No** - then you will not be required to indicate the domain to which the special database user belongs. In this case therefore, provide a valid user name against **eG Database User Name**, type the password of that user against **Password**, and confirm the password by retyping it against **Confirm Password** (see Figure 2.15).

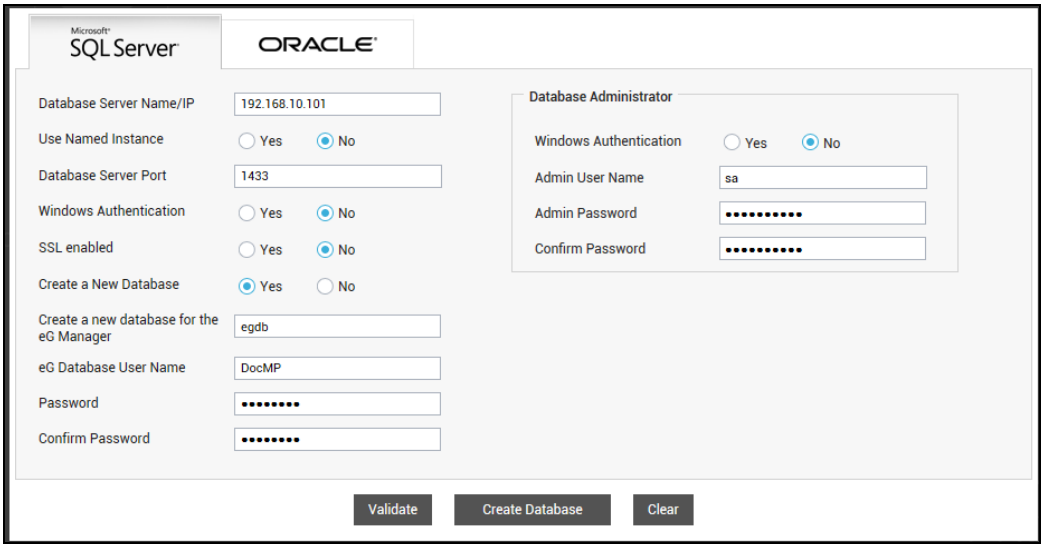


Figure 2.15: Specifying the credentials of the special database user, when SQL Server Authentication is enabled

12. When configuring a Microsoft Azure SQL database, since only **SQL Server Authentication** is

supported by default, you do not have to provide the **Domain name**. You only need to specify the following:

- Against **eG Database User Name**, specify the login name that you provided when creating the SQL database on Azure.
- In the **Password** text box, enter the password that you provided for the login name at the time of creating the Azure SQL database
- Confirm the password by retyping it in the **Confirm Password** text box.

Note:

- Make sure that the eG database user name you provide - whether it is that of a new user or an existing user - does not contain any special characters.
- Ensure that the password provided for the special database user is a **strong password.** Strong passwords are defined by the following parameters:
  - Has at least 6 characters
  - Does not contain “Administrator” or “Admin”
  - Contains characters from three of the following categories:
    - Uppercase letters (A, B, C, and so on)
    - Lowercase letters (a, b, c, and so on)
    - Numbers (0, 1, 2, and so on)
    - Non-alphanumeric characters (#, &, ~, and so on)
    - Does not contain the corresponding username

  For instance, if the name of the special database user is **egdb**, then the password that you set for this user should be a **strong password** such as, **db123$%#@**.

  Note that without a ‘strong password’, the eG SuperManager installation will fail.

13. Only a database administrator is authorized to create a new database on a Microsoft SQL server. Therefore, if you have chosen to configure a new database for the eG SuperManager in step 7 above , then make sure you configure the **Database Administrator** section in Figure 2.15 with the credentials of the database administrator. This way, you can make sure that setup has the necessary rights to create the database on the target Microsoft SQL server. For that, first indicate whether/not **Windows Authentication** is enabled for the database administrator. If it is, then set

the **Windows Authentication** flag to **Yes**. On the other hand, if only **SQL Server Authentication** is enabled, then set the **Windows Authentication** flag to **No**.

14. Next, ensure that the credentials of the database administrator are provided. If **Windows Authentication** is enabled - i.e., if the **Windows Authentication** flag in the **Database Administrator** section is set to **Yes** - then you will have to provide the name of a valid Windows domain user with database administrator privileges against **Admin User Name**, specify his/her password against **Password**, confirm the password by retyping it against **Confirm Password**, and also provide the **Domain Name** to which the database administrator belongs (see Figure 2.16).

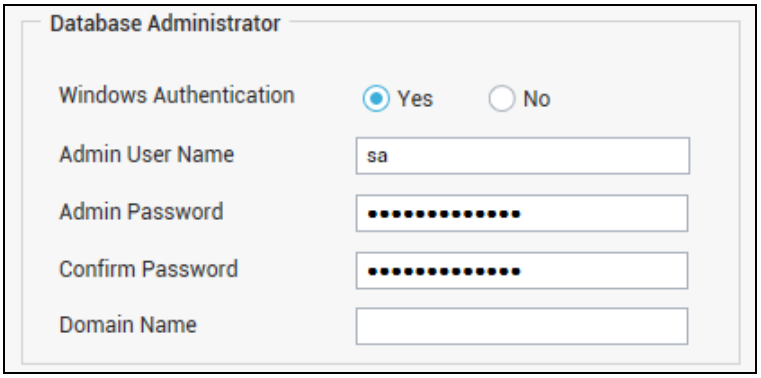


Figure 2.16: Providing the credentials of a DBA with Windows Authentication enabled

15. On the other hand, if **SQL Server Authentication** is enabled - i.e., if the **Windows Authentication** flag in the **Database Administrator** section is set to **No** - you will not be required to indicate the domain to which the database administrator belongs; in this case therefore, you only have to provide the **Admin User Name** and **Admin Password**, and confirm the password by retyping it against **Confirm Password** (see Figure 2.17).

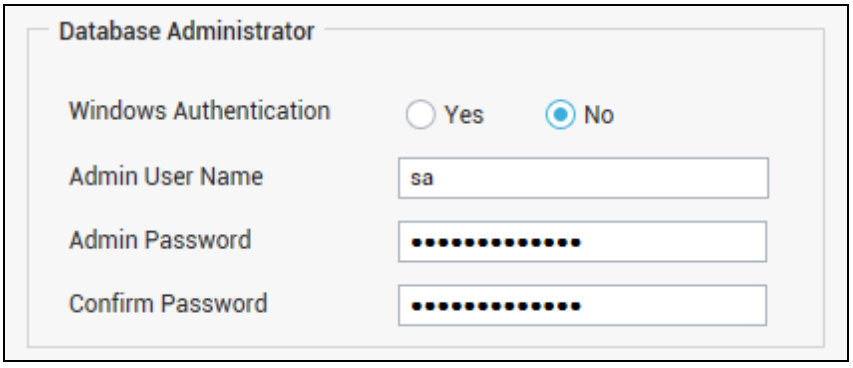


Figure 2.17: Providing the credentials of a DBA without Windows Authentication enabled

Note:

Typically, when providing database administrator credentials, **sa** user name and password are used. If, due to security concerns, you decide not to use the **sa** user's credentials, then you can create a user with the following server roles: **securityadmin, serveradmin,** and **public**, and then provide that user's credentials in the **Database Administrator** section depicted by Figure 2.17. Figure 2.18, Figure 2.19, and Figure 2.20 depict how to create a new user with the aforesaid privileges using the **Microsoft SQL Server Management Studio**.

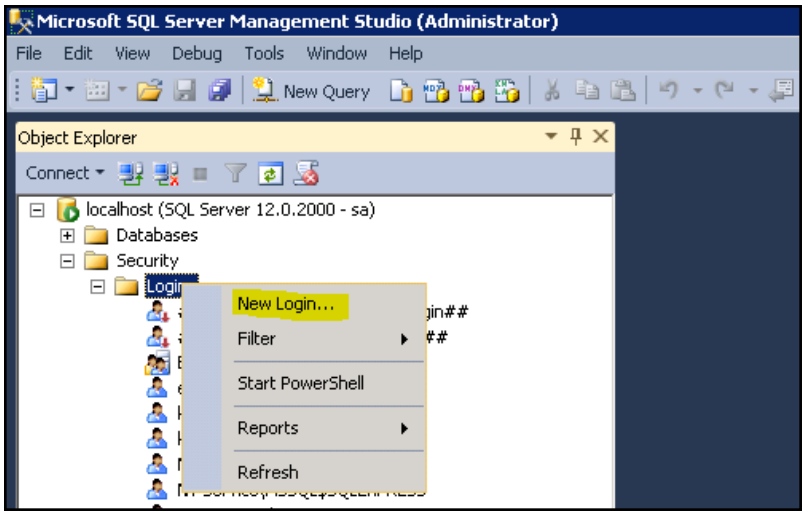


Figure 2.18: Choosing to create a new login

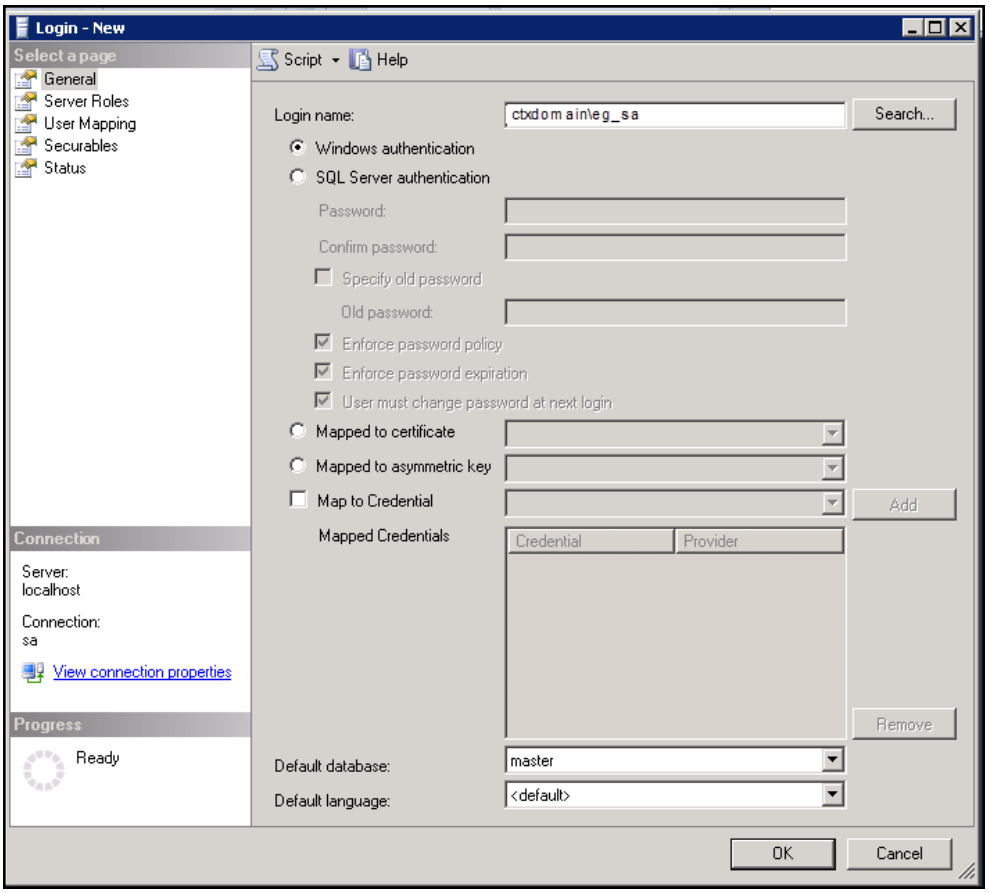


Figure 2.19: Creating a new user

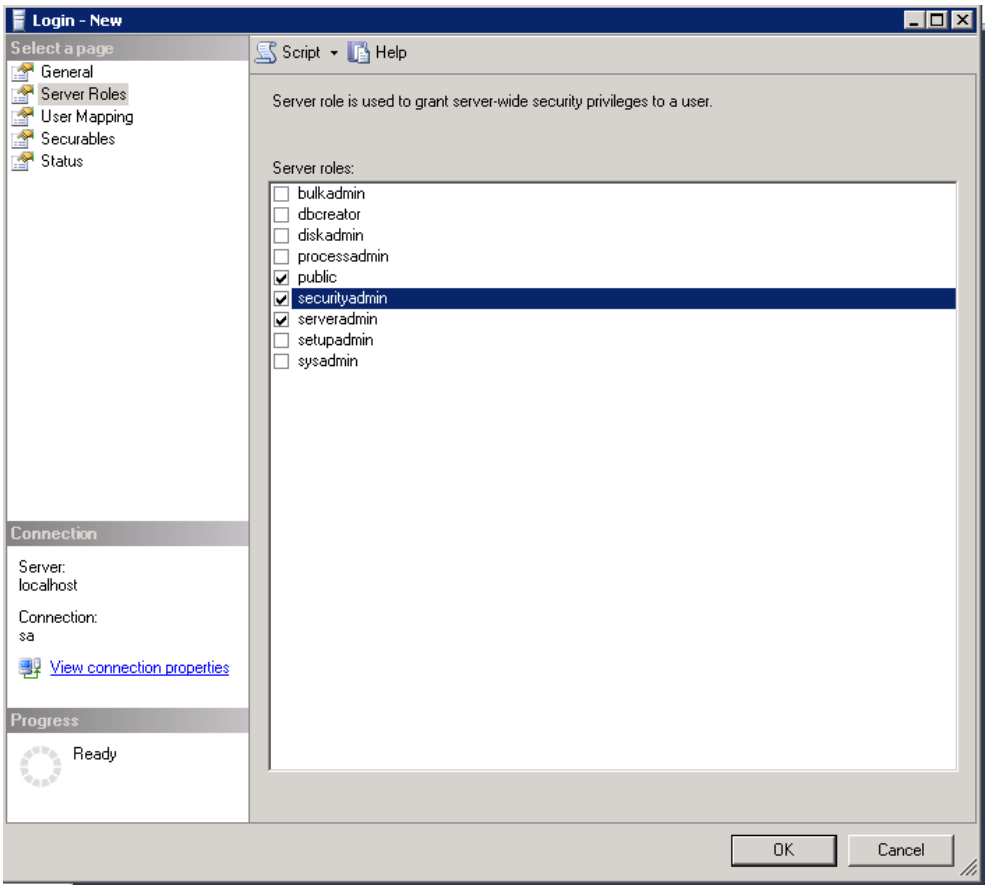


Figure 2.20: Granting the requisite privileges to the new user

When creating a new DBA, make sure that the user name you provide for the new DBA user does not contain special characters. Also, ensure that either provide a **strong password** for the user. Strong passwords are defined by the following parameters:

- Has at least 6 characters
- Does not contain “Administrator” or “Admin”
- Contains characters from three of the following categories:

a. Uppercase letters (A, B, C, and so on)

b. Lowercase letters (a, b, c, and so on)

c. Numbers (0, 1, 2, and so on)

d. Non-alphanumeric characters (#, &, ~, and so on)

e. Does not contain the corresponding username

For instance, if the name of the database administrator is **egdb**, then the password that you set for this user should be a **strong password** such as, **db123$%#@**. **Note that without a 'strong password', the eG SuperManager installation will fail.**

If you do not want to provide a strong password, then, make sure that the **Enforce password policy** option is disabled while creating the user profile in the **Microsoft SQL Server Management Studio**.

16. You can check the veracity of your database server, database, database user, and DBA configurations by clicking the **Validate** button in Figure 2.15. If your specifications are valid, then a message to that effect will appear. If not, an error message will appear, prompting you to check the *eGManager_Install* log file in the drive that hosts the eG SuperManager, for more details. You can then make changes to your specifications based on the error message logged in the log file.
17. Once validation is successful, proceed to create the database by clicking the **Create Database** button in Figure 2.15. This button will appear only if the **Create a New Database** flag is set to **Yes** and a new **eG Database Name** is provided. On the other hand, if you had chosen to use an existing database by setting the **Create a New Database** flag to **No**, then click the **Configure Database** button to configure that database as the eG database.
18. Setup will then proceed to create/configure the database and database user account. In the process, if setup finds that the database name and/or database user name provided in Figure 2.15 already exist on the target Microsoft SQL server, then it will prompt you to confirm whether you want to use the same names or change them. Click the **OK** button in the message box to proceed with the same names. Click **Cancel** to return to Figure 2.15, so you can change the database and/or database user names.
19. Once database configuration completes successfully, setup will allow you to configure certain basic manager settings, so that the eG SuperManager begins monitoring and alerting in no time! To know what these settings are and how to configure them, refer to Section **2.1.1.3**.

Note:

By default, the eG SuperManager is configured for agent-based monitoring - i.e., when a server is auto-discovered and then managed, it is monitored in an agent-based manner. Administrators have an option to set agentless monitoring as the default for the eG SuperManager.

On Windows systems, the script <EG_INSTALL_DIR>\lib\set_manager_default can be used to set agentless monitoring as the default option for the eG SuperManager. The output of this script is shown below:

```
Do you want to set the eG Manager for agentless monitoring by default? y/n[n]: y
************************************************************
Changes to the eG Manager default setting have been successfully made!
************************************************************
```

2.1.1.2.2 Using Oracle Database

If you want to configure the eG database on an Oracle database server, then, click the **Oracle** tab page in the web page that appears soon after successful manager installation. Figure 2.21 will then appear.

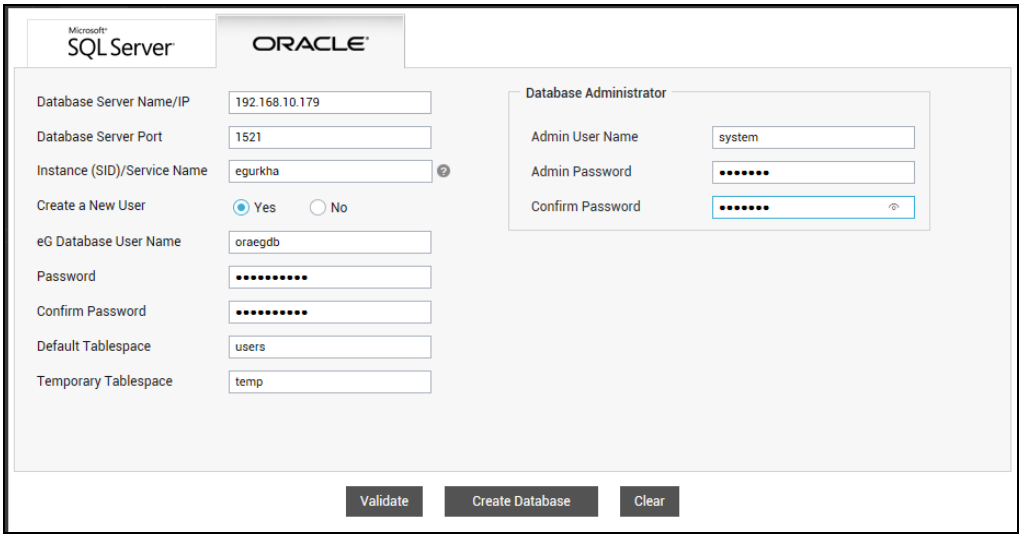


Figure 2.21: Configuring the eG database on an Oracle database server

To configure the eG database on Oracle, do the following using Figure 2.21:

1. Enter the name/IP address of the Oracle database server you want to use in the **Database Server Name/IP** text box.
2. Against **Database Server Port**, specify the port at which the Oracle database server listens. By default, this is 1521.
3. Next, in the **Instance (SID)/Server Name** text box, specify the name of the Oracle instance the eG SuperManager should use. A Service Name is mandatory if a pluggable database is being used.
4. The eG SuperManager requires a special Oracle database user account to store its measures. You can either create a new account for this purpose, or use an existing user account. If you want

setup to automatically create a new user account on Oracle for the eG SuperManager to use, first set the **Create a New User** flag in Figure 2.21 to **Yes**. Then, specify the name of the new user account in the **eG Database User Name** text box, provide a **Password** for the new user, and confirm the password by retyping it in the **Confirm Password** text box.

Note:

If the user chooses not to have the user account created by the configuration process, the user account has to be created manually on the Oracle database server with *connect, resource, and select_catalog* privileges. To know how to create such a user, refer to the table below, which describes the complete syntax for user creation on different versions of Oracle:

Version	Syntax for User Creation
Oracle 11G	create user $username identified by $password default tablespace $tspace1 temporary tablespace $tspace2; Grant connect, resource to $username; Grant select_catalog_role to $username; For example: create user john identified by john123 default tablespace dtspace temporary tablespace ttspace; Grant connect, resource to john; Grant select_catalog_role to john;
Oracle 12C (and above) - Normal Setup	create user $username identified by $password default tablespace $tspace1 temporary tablespace $tspace2; Grant connect, resource to $username; Grant select_catalog_role to $username; alter user $username quota unlimited on $tspace1; For example: create user james identified by j@m3s default tablespace jdspace temporary tablespace jtspace; Grant connect, resource to james; Grant select_catalog_role to james; alter user james quota unlimited on jdspace;

Version	Syntax for User Creation
Oracle 12C (and above) - Multi-tenant Setup (PDB and CDB)	alter session set container=$PDB_Name; create user $username identified by $password container=current default tablespace $tspace1 temporary tablespace $tspace2; Grant connect, resource to $username; Grant select_catalog_role to $username; alter user $username quota unlimited on $tspace1; For example: alter session set container=pdb1; create user mary identified by m1r2y container=current default tablespace mardspace temporary tablespace martspace; Grant connect, resource to mary; Grant select_catalog_role to mary; alter user mary quota unlimited on mardspace; **Note:** In a 12C Multi-tenant setup, the CDB cannot be used as the eG backend. This is why, in this case, you have to configure a PDB as the eG database. To know which PDB to use, you need to first take a look at the available PDBs. For that, log into a CDB and run the query below at the SQL prompt to get the list of PDBs: *select pdb_name from dba_pdbs where pdb_name not like '%$%';*

Once the user account is created, you can then use step 5 below to configure an existing database for the eG SuperManager's use.

5. If you want to use an existing database user account for the eG SuperManager, first set the **Create a New User** flag to **No** (see Figure 2.22). Then, specify the name of the existing user in the **eG Database User Name** text box, provide the valid **Password** of that user, and confirm the password by retyping it in the **Confirm Password** text box.

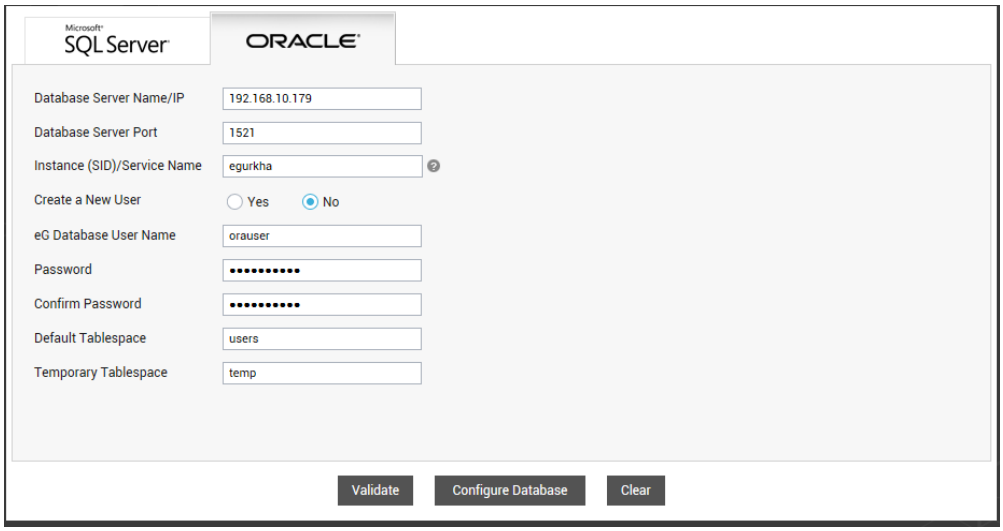


Figure 2.22: Configuring an existing database user account for the eG SuperManager

Note:

If you set an existing database user as the eG database user at step 5, then before configuring the eG SuperManager to use Oracle as its backend, make sure that *connect, select_catalog,* and *resource* privileges are granted to the existing user.

6. To create a new user account for an Oracle database server, a data tablespace and a temporary tablespace have to be associated with the new user account (as shown in Figure 2.21). For this purpose, specify the same in the **Default Tablespace** and **Temporary Tablespace** text boxes, respectively. On the other hand, if you will be using an existing user account, then make sure that the **Default Tablespace** and **Temporary Tablespac**e text boxes are configured with the default and temporary tablespace that is already mapped to the specified database user account. The default values for the data and temporary tablespaces values are *users* and *temp,* respectively.

   Note:

   - We recommend that when you install the eG SuperManager with an Oracle database backend, the following tablespaces (with the parameters indicated) are specifically created for eG:

```
create tablespace egurkhadata01
datafile 'C:\Oracle\ORADATA\egurkha\eGurkhaData01.dbf' size 10240M
autoextend off extent management local autoallocate;
create temporary tablespace egurkhatemp01
```

```
tempfile 'C:\Oracle\ORADATA\egurkha\eGurkhaTemp01.dbf' size 512M
autoextend off extent management local uniform;
```

- Create rollback tablespaces and rollback segments as needed.
- The usage of an Oracle backend for the eG SuperManager also necessitates the resetting of the following Oracle initialization parameters.
- The **processes** parameter should be set to a minimum of 100
- The **open_cursors** parameter should be set to a minimum of 200.

These parameters might have to be tuned further based on an increase in server load.

7. Database administrator privileges are required for creating a new database user. Therefore, if you have chosen to create a new database user - i.e., if the **Create a New User** flag is set to **Yes** - then, you will have to use the **Database Administrator** section of Figure 2.21 to configure the credentials of the database administrator. For that, type the name of database administrator against **Admin Name**, specify the password of the database administrator against **Password**, and confirm the password by retyping it against **Confirm Password**. On the other hand, if you want to use an existing user account for the eG SuperManager, then you will not have to provide database administrator credentials. In this case therefore, the **Database Administrator** section will not appear (see Figure 2.22).
8. To check the veracity of your configuration, click the Validate button in Figure 2.22. If your specifications are valid, then a message to that effect will appear. If not, an error message will appear, prompting you to check the *eGManager_Install* log file in the drive that hosts the eG SuperManager, for more details. You can then make changes to your specifications based on the error message logged in the log file.
9. Once validation is successful, proceed to create the new database user by clicking the **Create Database** button in Figure 2.21. This button will appear only if the **Create a New User** flag is set to **Yes** and a new **eG Database User Name** is provided. On the other hand, if you had chosen to use an existing database user account by setting the **Create a New User** flag to **No**, then click the **Configure Database** button (see Figure 2.22) to configure the specified database user account for use by the eG SuperManager.
10. Setup will then proceed to create/configure the database user account. In the process, if setup finds that the database user name provided in Figure 2.21 or Figure 2.22 already exists, then it will prompt you to confirm whether you want to use the same user name or change it. Click the **OK** button in the message box to proceed with the same user name. Click Cancel to return to Figure 2.21, so you can change the user name.

11. Once database configuration completes successfully, setup will allow you to configure certain basic manager settings, so that the eG SuperManager begins monitoring and alerting in no time! To know what these settings are and how to configure them, refer to Configuring Basic Manager Settings.

2.1.1.3 Configuring the Basic Manager Settings

Once the eG database is successfully configured, setup automatically opens the **Manager Configuration** page (seeFigure 2.23). This page enables you to indicate what type of environment your eG SuperManager deployment needs to monitor. Depending upon the type of environment, you can even turn on/off certain key capabilities of the eG SuperManager using this page. This way, you can custom-define how your manager performs monitoring and alerting, enforce organizational security policies, and enable the auditing of supermanager operations, without even logging into the eG management console!

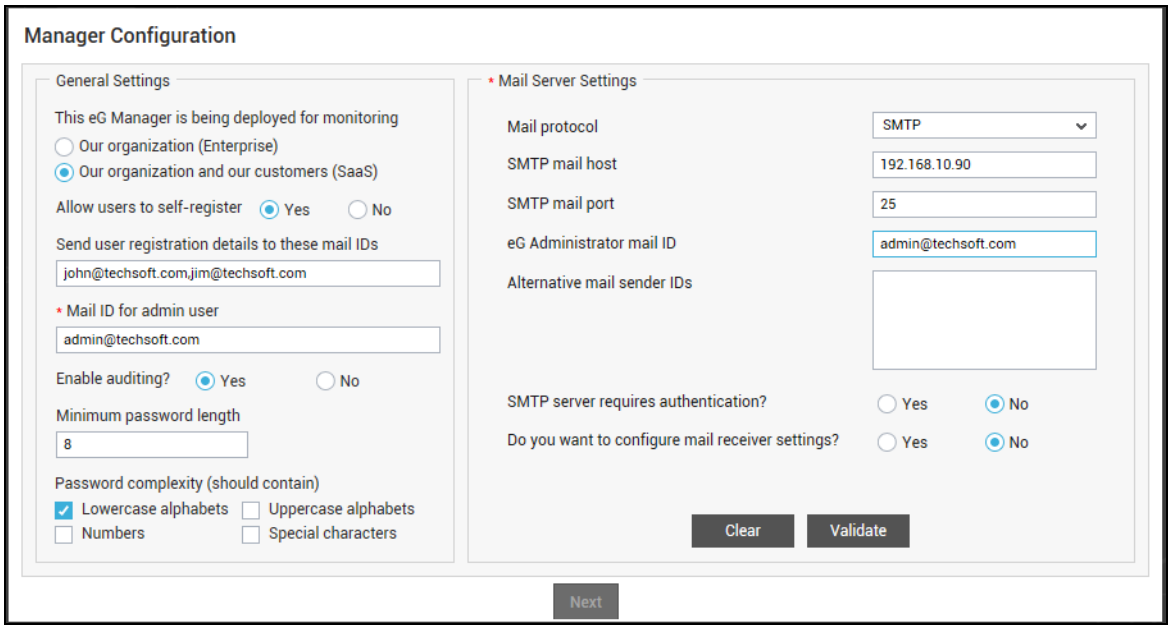


Figure 2.23: Configuring the basic manager settings

Using Figure 2.23, do the following:

1. First, choose Our organization (Enterprise) as the deployment model for the eG SuperManager.

    - Enterprise: This model is ideal if your eG SuperManager will be monitoring only your organization's IT infrastructure. In this case, eG's agent-based/agentless monitors will be deployed on and will pull metrics from the components in your infrastructure only. The

employees of your organization will be the primary stakeholders and consumers of the performance data so collected.

Such a model is typically, administrator-driven. In other words, an administrator will be responsible for performing all administrative activities related to the eG SuperManager - this includes, installing agents, managing the components, configuring thresholds, tests and alerting, managing users, building segments and services, defining zones, and more. The other stakeholders - i.e., the employees - will usually be vested with only monitoring rights, or in some special cases, very limited administrative rights, as the administrator deems fit.

2. Next, specify the **Mail ID for admin user**. The admin user is one of the default users of the eG Enterprise system. This user is automatically created by the eG Enterprise system, soon after an eG SuperManager is deployed. This user has unrestricted administrative and monitoring powers. If you login to the eG management console as user admin (with default password admin), you can configure your environment for monitoring, and also view performance and problem statistics pertaining to your environment. Typically, an administrator's mail ID is assigned to the default admin user. This way, the admin user can receive email notifications whenever the eG SuperManager detects issues in any core component of the eG architecture - say, the eG database - or in any component of the monitored IT infrastructure. This enables the admin user to keep tabs on the health of the eG Enterprise system and that of the monitored environment.

3. Using Figure 2.23, you can also enable/disable audit logging for your eG SuperManager. An audit log can be best described as a simple log of changes, typically used for tracking temporal information. The eG SuperManager can be configured to create and maintain audit logs in the eG database, so that all key configuration changes to the eG Enterprise system, which have been effected via the eG user interface, are tracked.

   The eG audit logs reveal critical change details such as what has changed, who did the change, and when the change occurred, so that administrators are able to quickly and accurately identify unauthorized accesses/modifications to the eG Enterprise system.

   By default, audit logging is disabled. To enable it, set the **Enable auditing?** flag to **Yes** (see Figure 2.23).

4. Users with administrative rights to the eG Enterprise system can allow other users access to the eG management console, by configuring a dedicated profile in eG for each user. Using the profile, the administrator assigns login credentials - i.e., login user name and password - to a

user. At any given point in time, the administrator or the corresponding user can change his/her login password.

In some high-security environments, password policies are often defined, which dictate how long and how strong a login password should be. If, for security reasons, you want to define and enforce a password policy for the login passwords of eG users, you can do so using the options provided by Figure 23.

For instance, in the **Minimum password length text box** of Figure 2.23, specify the minimum number of characters a login password should contain. When creating/modifying the password of an eG user, you need to make sure that at least this many characters are present in the password; if not, eG will automatically reject the password and insist that you specify another one.

You can also define the password strength, by selecting the checkboxes you need under **Password complexity**. For example, if you want the login password of an eG user to compulsorily contain some lowercase characters and numbers, then select the **Lowercase alphabets** and **Numbers** checkboxes in Figure 2.23.

Note:

Password policies set here apply only to local users of eG Enterprise, and not domain and SAML users.

5. By default, the **Mail Server Settings** are not supported for the eG SuperManager. You can skip this configuration and click the **Next** button to proceed further.

   - If you have configured an Oracle database backend for the eG SuperManager, then Figure 2.24 will appear.

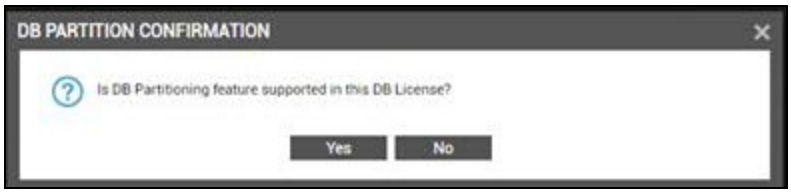


Figure 2.24: Confirming whether/not the Oracle DB license enables support for Partitioning feature

'Partitioning' is a licensed capability, which is available only for Oracle 12c (and above). If your Oracle database server license enables partitioning support, then you can have the eG SuperManager store performance and configuration metrics in partitions on the eG database. If you have configured Oracle database server 12c (or above) as the eG backend, and if your

Oracle DB license enables the 'Partitioning' feature, then click **Yes** in Figure 2.24 to confirm support. If you confirm support, then setup will automatically create a partition and store metrics in it. On the other hand, if the SuperManager is not configured to use an Oracle database server 12c (or above) as its backend, or if your DB license does not support the 'Partitioning' feature, then click the **No** button in Figure 2.24. In this case, data insertions on the Oracle backend will be done based on available space – i.e., data will be inserted into any space available anywhere in a table.

- Figure 2.25 will then appear, displaying the URL using which the eG SuperManager should be accessed. The default URL will be of the format http://<eGSuperManagerIPorHostName>:<eGSuperManagerPort> or https://<eGSuperManagerIPorHostName>:<eGSuperManagerPort>, depending upon whether/not the SuperManager is SSL-enabled. If your eG SuperManager is behind the NAT, then you may want to replace the default URL with the externally accessible URL. Then, click the **Update** button.

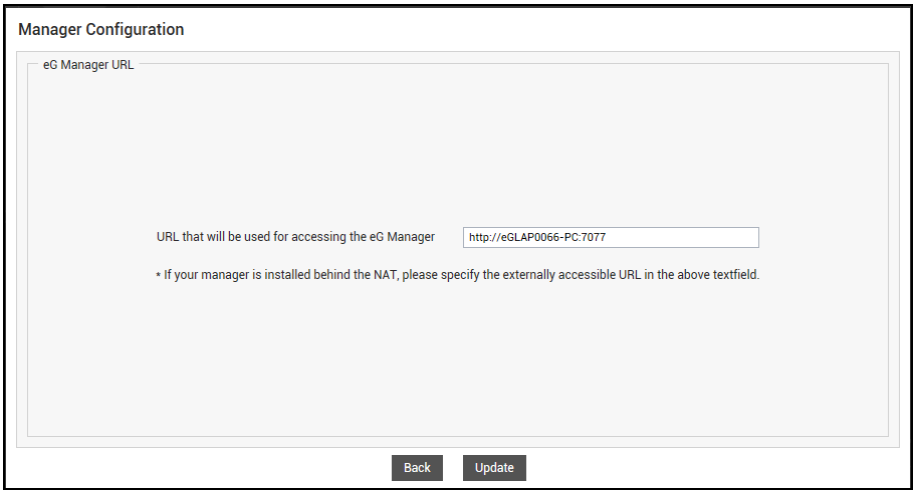


Figure 2.25: The URL that will be used for accessing the eG SuperManager

- Figure 2.26 will then appear informing you of the successful installation of the eG SuperManager. If you have a valid eG license, then set the **Do you have a valid license?** flag to **Yes**. Then, specify the full path to the license file against **Choose a license file** text box. You can even use the **Browse** button to locate the license file. Finally, click the **Upload License** button.

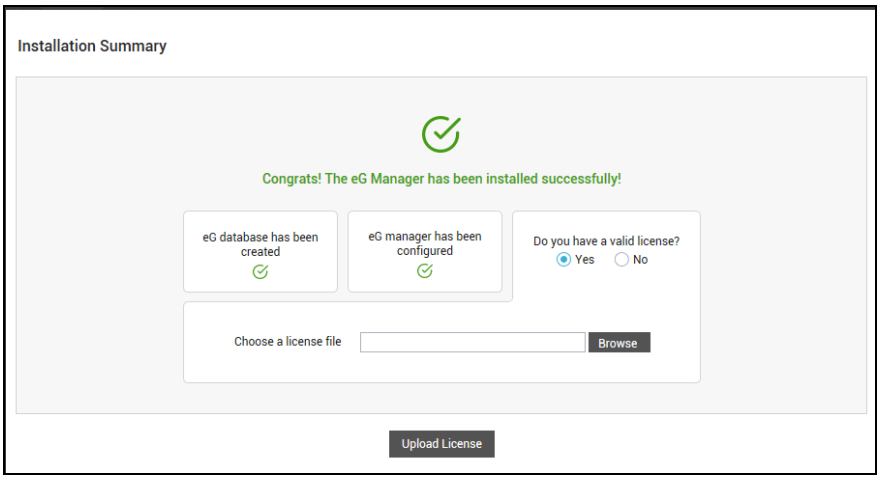


Figure 2.26: Uploading the license file

On the other hand, if you do not have a valid license file, then set the **Do you have a valid license?** flag to **No** (see Figure 2.27). In which case, you can write to support@eginnovations.com requesting for a valid eG license. Once you receive the license file, make sure you copy it to the <EG_INSTALL_DIR>\bin folder. Then, start the manager.

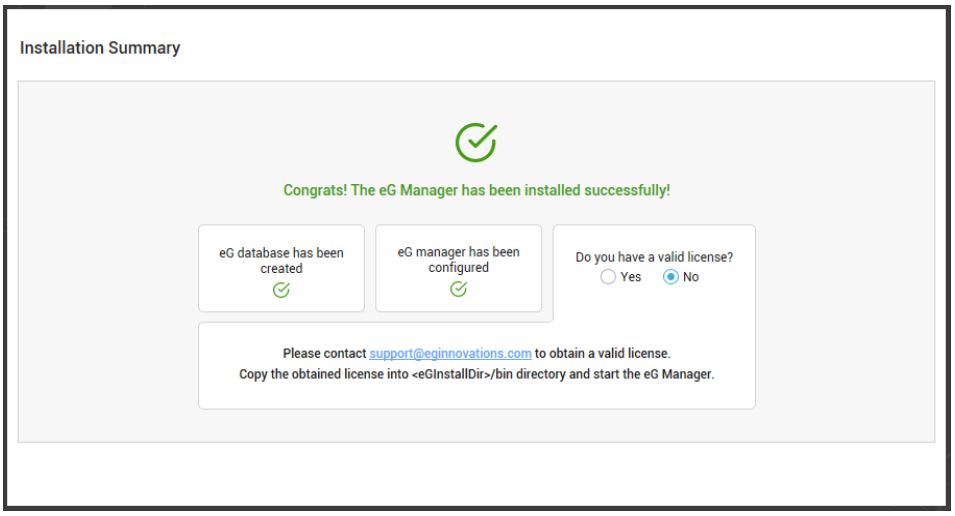


Figure 2.27: Requesting a valid license

2.2 SSL- Enabling the eG SuperManager on Windows Environments

The eG SuperManager on Windows includes a default SSL certificate. If you SSL-enable the eG SuperManager using this default certificate, then all you need to do is click the **Yes** button when the eG SuperManager setup process requests you to indicate whether the manager is to be SSL-

enabled or not. Doing so will instantly enable the eG manager to communicate with the eG SuperManager via HTTPS and vice versa.

However, if you choose not to use the default certificate, then, you have the following options:

1. You can obtain a signed certificate from an internal certifying authority (e.g., Microsoft Active Directory Certificate Services) and use this certificate to SSL-enable the eG SuperManager, (OR)
2. You can obtain a signed certificate from a valid, external certifying authority (e.g., Verisign) and use this certificate to SSL-enable the eG SuperManager

If you go with option (a), use the procedure detailed in *SSL-Enabling the eG Manager Using a Certificate Signed by Internal CA* section of the *eG Installation Guide*.

If you pick option (b), use the procedure detailed in *SSL-Enabling the eG Manager Using a Signed Certificate Obtained from a Valid Certifying Authority* section of the *eG Installation Guide*.

2.3 Configuring an eG SuperManager to Manage the eG Managers in a Redundant Cluster

You can ensure that the managers in a redundant setup report to an eG SuperManager, by following the steps given below:

a. Install and configure the eG SuperManager using the procedure discussed in Installing and Configuring the eG SuperManager on Windows Environments .

b. Next, you would have to ensure that the eG SuperManager is made aware of the individual eG managers that it needs to receive metrics from. In a non-redundant setup, you would typically follow the procedure detailed in Section **4.1** to achieve this. In a redundant setup however, since the primary manager is configured to receive metrics from all the other managers in a cluster, it would suffice to configure a line of communication between the eG SuperManager and the primary manager alone i.e., it is suffice for you to provide the IP address and port of the primary manager in the cluster and assign a nick name to the primary manager.

The next step is to configure each of the eG managers to talk to the eG SuperManager. To achieve this for an individual manager, you need to simply follow the steps discussed in Section **2.4**, on the manager. However, in the case of a redundant setup, since the primary manager shares its configuration information with the secondary managers in the clusters, it would suffice to follow the procedure detailed in Section **2.4** on the primary manager alone.

2.4 Configuring the Individual eG Managers to Work with the eG SuperManager

To configure the eG Managers to work with the eG SuperManager, login to the admin interface of each of the managers configured for the SuperManager and then explicitly add the SuperManager. To achieve this, do the following:

1. Login to the eG administrative interface as *admin* with password *admin*.
2. Follow the menu sequence: *Admin -> Miscellaneous -> SuperManager Settings*. Figure 2.28 will then appear.

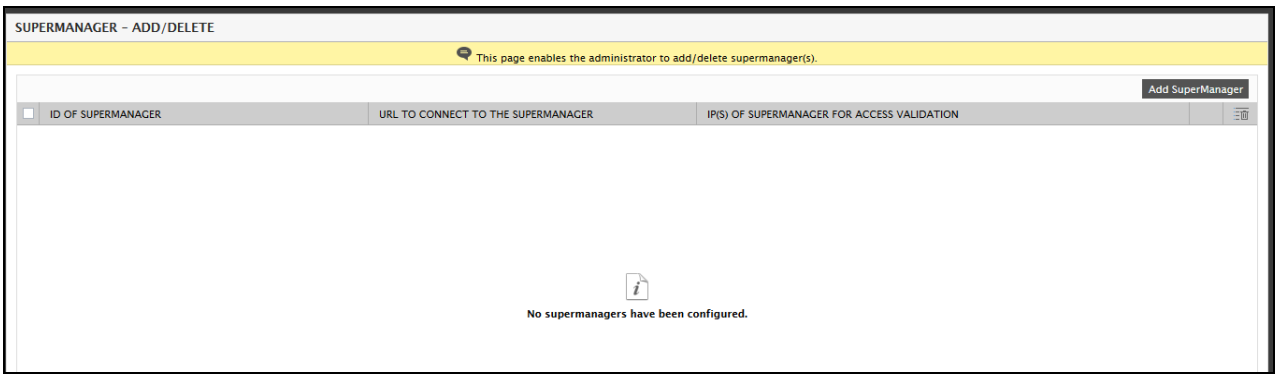


Figure 2.28: Add/delete SuperManager

3. To add the SuperManager, click the **Add SuperManager** button in Figure 2.28. Figure 2.29 then appears.

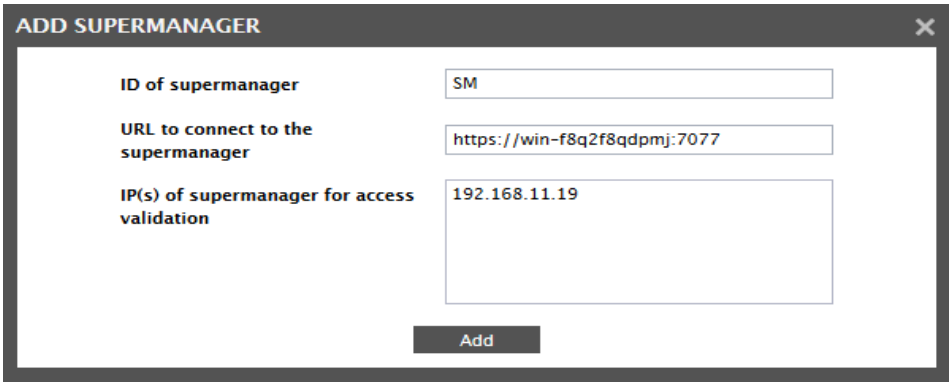


Figure 2.29: Adding a SuperManager to which this manager should report

4. In Figure 2.29, specify the following:

- **ID of supermanager** - Specify the name of the SuperManager or the IP address of the SuperManager to which the eG manager should report to.
- **URL to connect to the SuperManager** - Specify the URL of the SuperManager which would be used by the eG manager to communicate with the SuperManager.
- **IP(s) of supermanager ofr access validation** - If the eG SuperManager and the eG manager reside in the same local environment but on different host, then the eG manager would be able to communicate with the SuperManager using an intranet IP. In such cases, provide the alternate IP of the SuperManager in the SuperManager Alternate IP(s) text box.
- Clicking the **Add** button would add the SuperManager to the manager as shown in Figure 2.30.

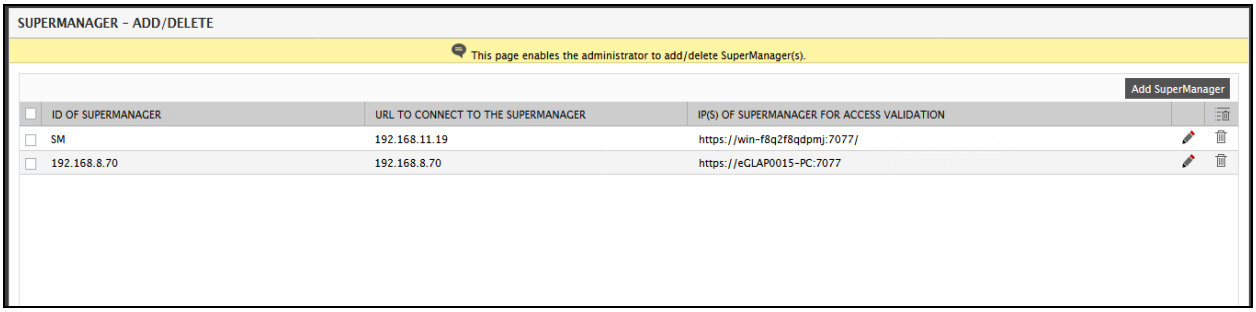


Figure 2.30: The list of SuperManagers to which an eG manager is to report to

Note:

The eG manager is capable of communicating with multiple SuperManagers simultaneously. Therefore, you can add multiple SuperManagers from an eG manager using Figure 2.29.

5. You can even modify the SuperManager settings by clicking the button.
6. You can even delete a SuperManager specification, by clicking the button against the eG SuperManager in Figure 2.30 , that you wish to delete. If you wish to delete all the SuperManagers, then, select the check box against the **ID OF SUPERMANAGER** label and click the button.

2.5 Starting and Stopping the eG SuperManager

Before starting a SuperManager, ensure the following:

1. Ensure that a proper license file is available in the **<EGSUPERMANAGER_INSTALL_DIR>\bin** directory)

2. View the license by executing the command: **<EGSUPERMANAGER_ INSTALL_ DIR>\bin\viewCert <License File Name>**. A sample output of the **viewCert** command has been provided below.

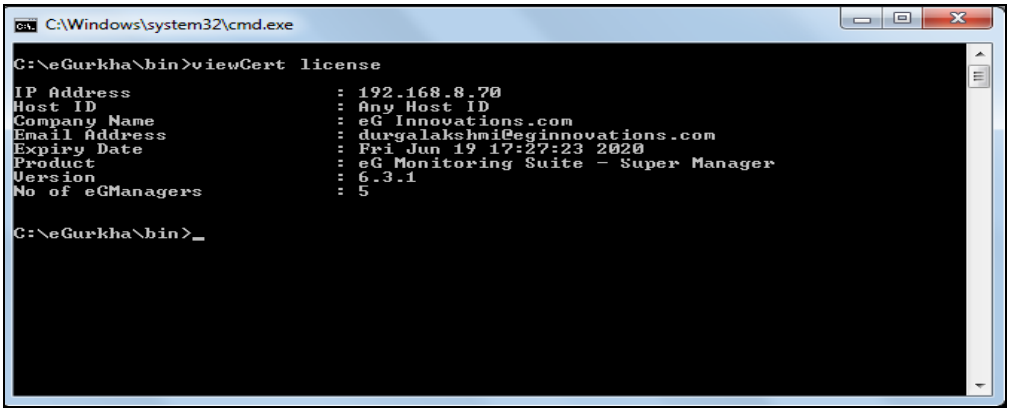


Figure 2.31: Sample license

The **IP address**, if specified, restricts the eG SuperManager to a specific host. The **Host ID**, if specified, restricts the eG SuperManager to a host that has a specific host ID. On Windows systems, look for the physical address specification in the output of the **ipconfig /all** command. The host ID specified in the license must match one of the physical addresses of the host (ignore any dashes (-) in the physical address). The **Company Name** indicates the name of the company that is licensed to use the SuperManager, and the **Email Address** is the email ID to which license expiry mails are to be sent. The date on which the license will become invalid is set against **Expiry Date**, and the name of the **Product** and its **Version** is also displayed.

The license also controls the maximum number of individual eG managers that a SuperManager is licensed to handle. For example, in Figure 2.31, the **No. of eGManagers** is set to **5**, which means that the eG system will not allow administrators to configure more than **5** eG managers for this SuperManager. **Though any number of eG managers can be handled by the eG SuperManager, it is recommended that a maximum of 10 eG managers are configured for each eG SuperManager.** This would optimally scale the eG SuperManager as well as provide better performance.

Starting the eG SuperManager

To start an eG SuperManager, 'administrator' privileges are required. In this case therefore, follow the *Start -> Programs -> eG Monitoring Suite -> eG Manager* menu sequence, right-click on the **Start Manager** menu option, and pick the **Run as administrator** option.

Figure 2.32: Starting the eG SuperManager

If the eG SuperManager starts successfully, the following message appears:

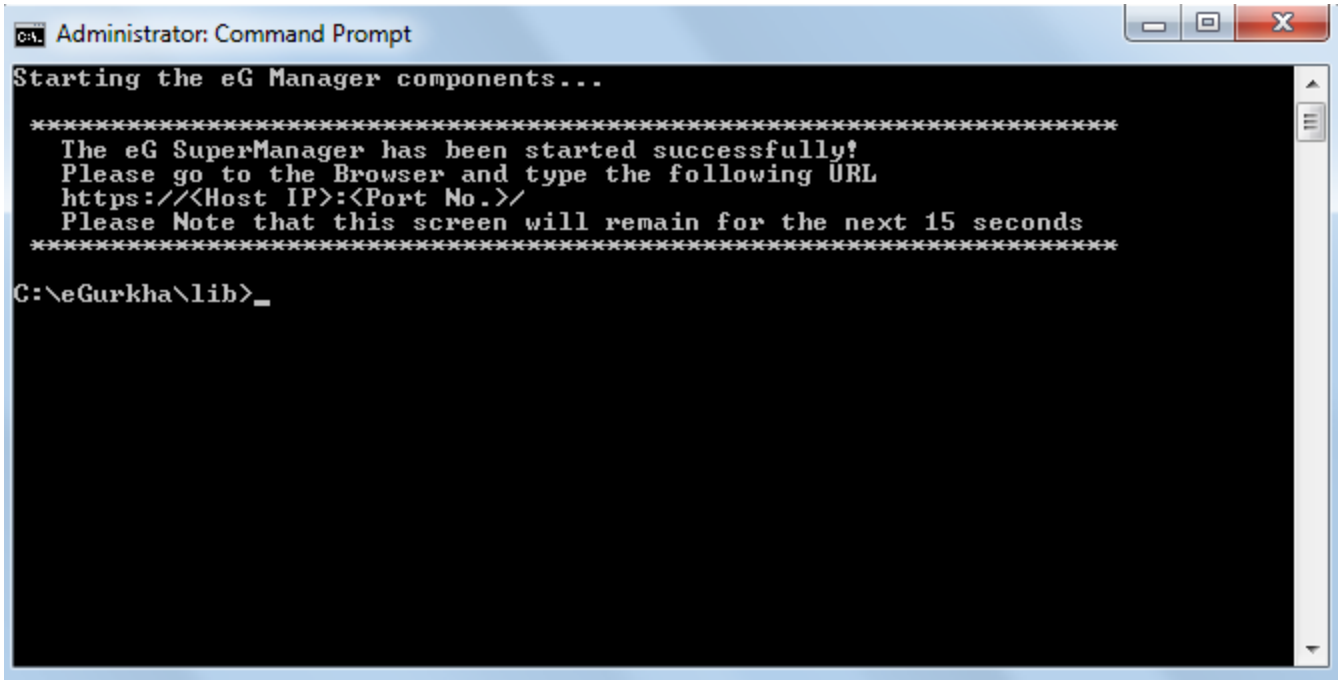


Figure 2.33: Message indicating that the SuperManager has been started successfully

Alternately, you can start an eG SuperManager on a Windows environment using the command prompt.

Upon starting the eG SuperManager, the following services get started:

• eGmon (manager recovery process)

• eGurkhaTomcat (core manager process)

Please check the services running on your system. If the status corresponding to the service eGurkhaTomcat and eGmon is “Started”, then the SuperManager has been started successfully. If the SuperManager fails to start, the following message appears.

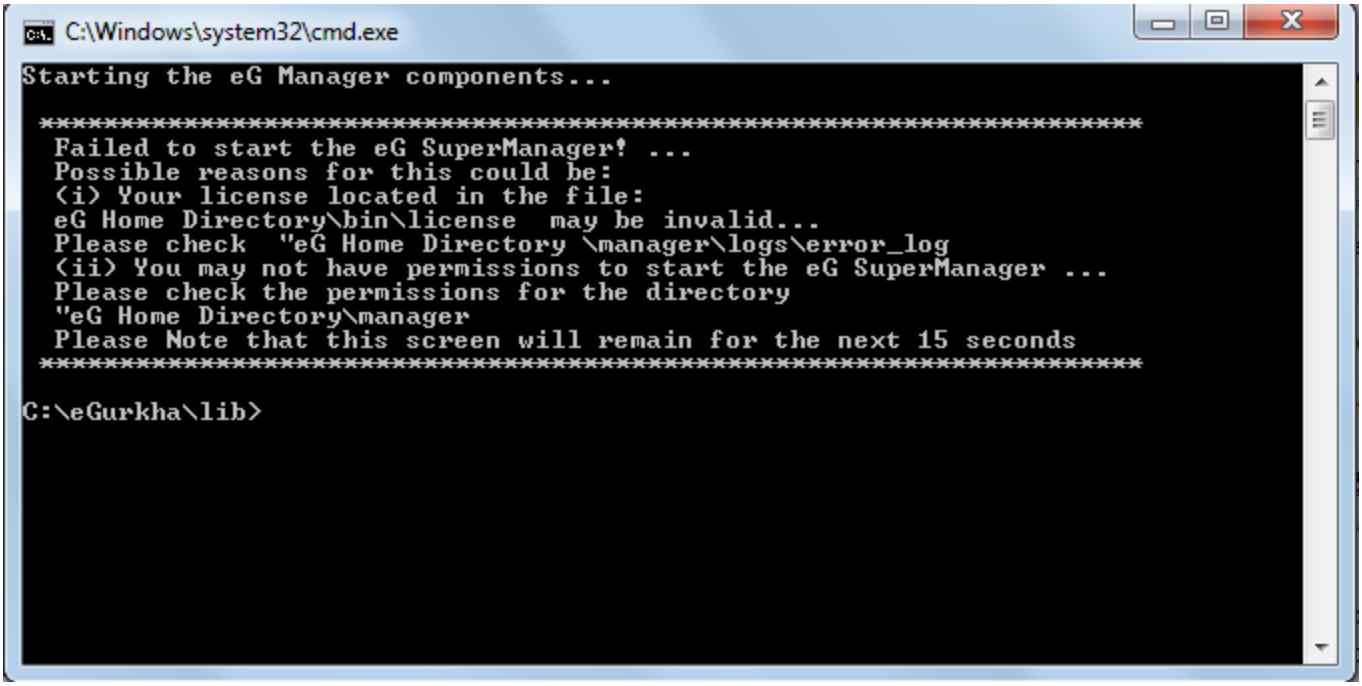


Figure 2.34: Message indicating that the eG SuperManager failed to start

Stopping the eG SuperManager

To stop the eG SuperManager, follow the menu sequence depicted by Figure 2.35:

Figure 2.35: Stopping the eG SuperManager

Alternately, to stop the eG manager, you can use the command prompt.

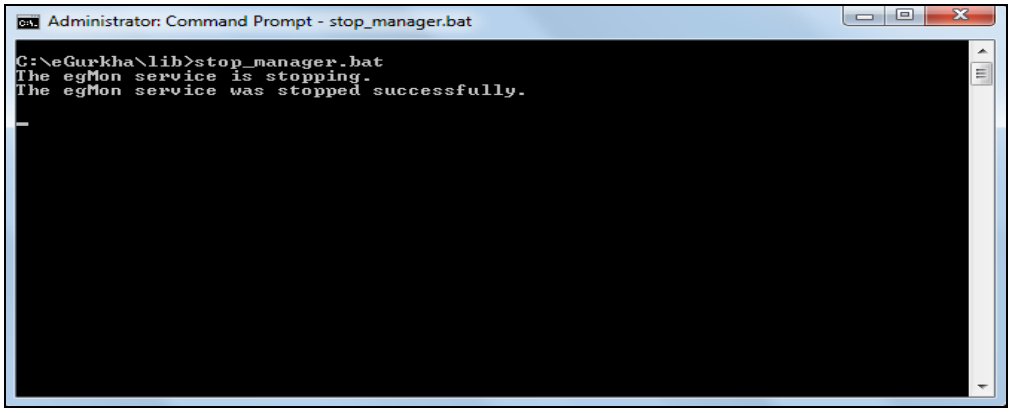


Figure 2.36: Message indicating that the eG SuperManager has been stopped successfully

2.6 Accessing the SuperManager Console

To access the eG SuperManager console, eG Enterprise offers a default *egsm* user. This user has the complete rights to access the eG SuperManager. Apart from this user, the users of the individual eG Managers that are configured to report to the eG SuperManager are also entitled to login to the eG SuperManager. Except for the egsm user, all other users have limited access to the eG

SuperManager i.e., they are entitled to view only the entities assigned to them for monitoring from the SuperManager console.

Though the egsm user is capable of viewing all the entities collected by the eG managers, the configuration settings of the eG managers are different from that of the eG SuperManager. For example, the eG SuperManager can view the User Experience dashboard of a virtual user but cannot view the widgets customized in the dashboard by a user logged into the eG manager.

2.7 Uninstalling the eG SuperManager

To uninstall the eG SuperManager installed on a Windows host, do the following:

1. Stop the eG SuperManager.
2. Begin uninstallation by following the menu sequence depicted by Figure 2.37.

Figure 2.37: Uninstalling the eG SuperManager

3. Figure 2.38 will then appear. Select the **Remove** option from Figure 2.38, and then, click the **Next** button.

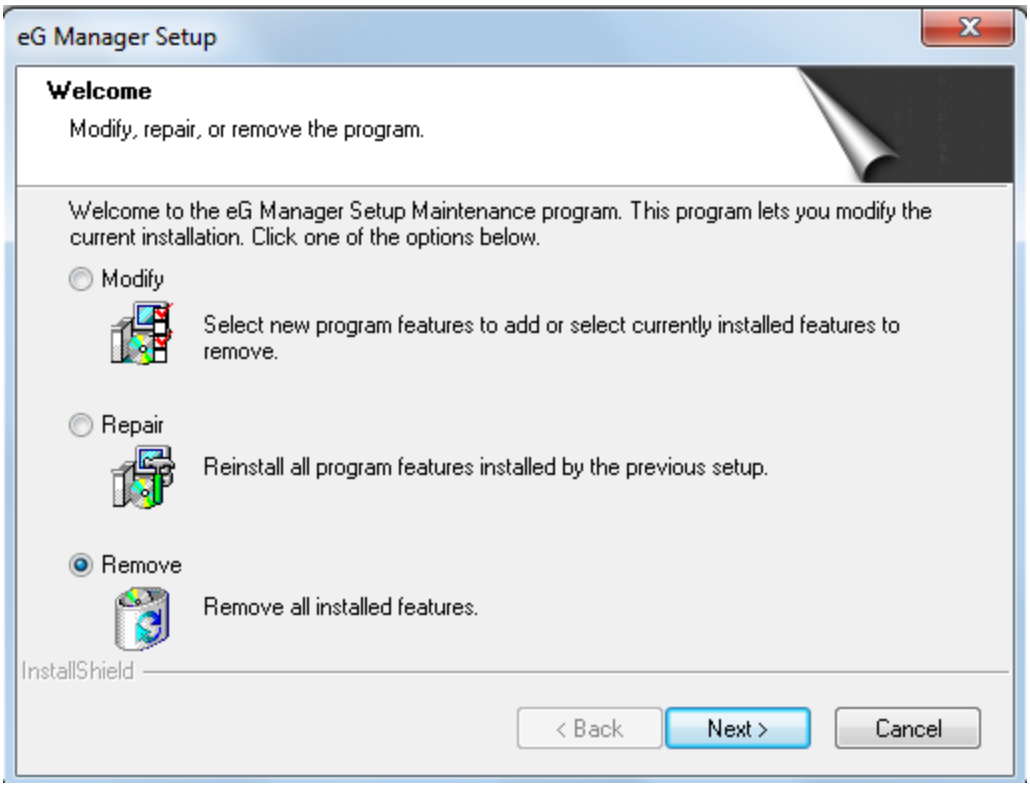


Figure 2.38: Deleting the option to remove the SuperManager

4. Next, click the **OK** button in Figure 2.39 to begin uninstallation.

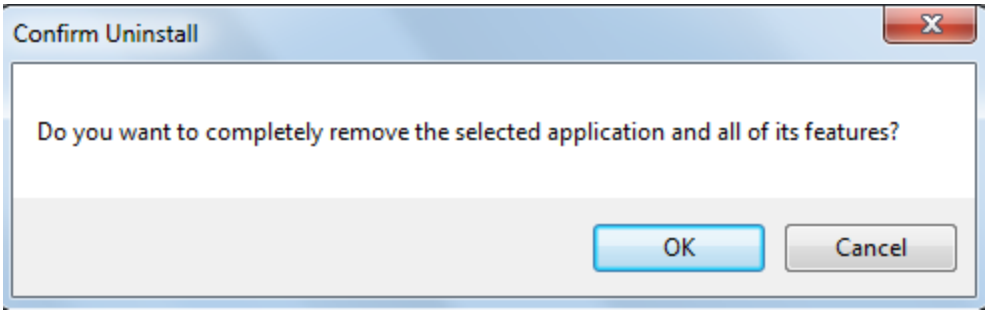


Figure 2.39: Confirming removal of the SuperManager

Chapter 3: Licensing of the eG SuperManager

In the eG Enterprise architecture, the license is centrally controlled on the eG SuperManager. The license on the eG SuperManager is typically node-locked. That is, if you need to move the supermanager to a different IP address or host, you will need to get a new license for the supermanager. The details of the license deployed on an eG SuperManager can be viewed from the **LICENSE INFORMATION** page of the eG administration console (see Figure 3.1).

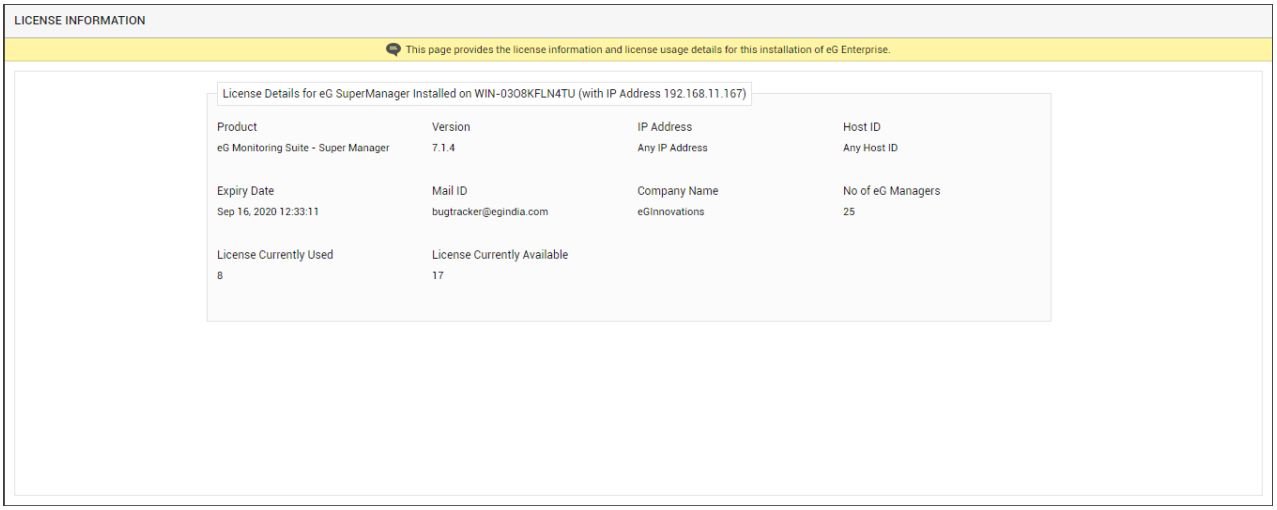


Figure 3.1: The eG SuperManager license

For the eG SuperManager to function, the license must support the IP address and MAC of the system on which the eG SuperManager is installed. The version of the eG license should also match the version of the eG SuperManager that is it deployed on. For example, a version 6.1 license should not be used to operate an eG manager v 6.2.1.

If the eG SuperManager fails to start, please check the error_log file in the <EG_INSTALL_DIR>\manager\logs folder. An error *"LicenseMgr – Invalid License"* indicates that the license you have deployed on the eG SuperManager is not valid.

If the eG SuperManager does not start, you will not be able to view the license details from the eG administration interface. In such cases, a command line utility "viewCert" is included in the eG SuperManager package to view the license details. To run this command, do the following:

1. Login to the eG SuperManager host.
2. On a Windows host, switch to the <EG_INSTALL_DIR>\bin directory.

3. To view the license, issue the following command: **viewCert license**

Chapter 4: Administering the eG SuperManager

An important step in installing and configuring the eG SuperManager is to administer the eG SuperManager system. During this process, an administrator configures which managers are monitored by the eG SuperManager system, how many managers are currently running, what are the components that are configured for each manager, what are the tests that are executed for each component, and how the measurements reported by the tests are to be interpreted. The administrator is also responsible for determining which users are allowed access to the eG SuperManager system. This chapter describes the various functions that an eG administrator can perform with the eG SuperManager system.

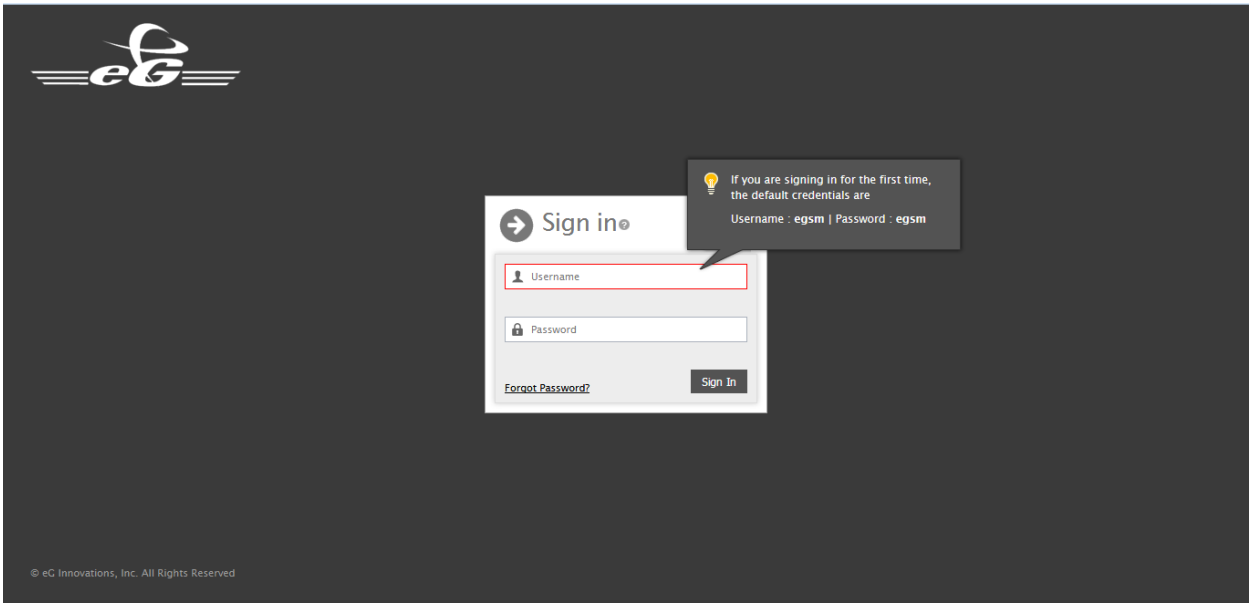


Figure 4.1: The eG SuperManager login screen

To access the eG SuperManager system using a web browser, connect to the URL **http://<IP of the SuperManager>:<Port number of the SuperManager>/**, if the SuperManager is configured without SSL. Alternately, if the SuperManager is configured with SSL, connect to the URL **https://<IP of the SuperManager>:<Port number of the SuperManager>/**. Figure 4.1 shows the eG SuperManager login window. The user has to login from this window in order to access the eG SuperManager system. The eG SuperManager system is predefined with a default user - egsm. Therefore, you are required to login with the username *egsm* and password *egsm*.

While specifying the URL, please take care of the following aspects:

1. If the host name was provided when installing the SuperManager, use this name (and not the IP address) for accessing the user interface via the web browser.
2. If the host name is provided, make sure that forward and reverse lookups for this name are enabled via the DNS service in the target environment.
3. If an administrator forgets the login **Password**, he/she should contact the eG Enterprise to retrieve the password.

If eG managers reporting to the SuperManager are integrated with Active Directory servers, then an additional **Domain** list appears in the login page. The domain users who login to the eG managers are allowed to login to the SuperManager by selecting the **Domain** to which the user belongs to.

Figure 4.2: The SuperManager login allowing users to login with Domain credentials

4.1 The Admin Home Page

The first page that will be displayed on navigating into the administrative interface of the eG SuperManager system is the **LIST OF MANAGERS** page (see Figure 4.3).

This page enables the administrator to understand, at a glance, the status of the managers that are managed by the eG SuperManager. If you access this page soon after installing the eG SuperManager, then, a message to that effect appears as shown in Figure 4.3.

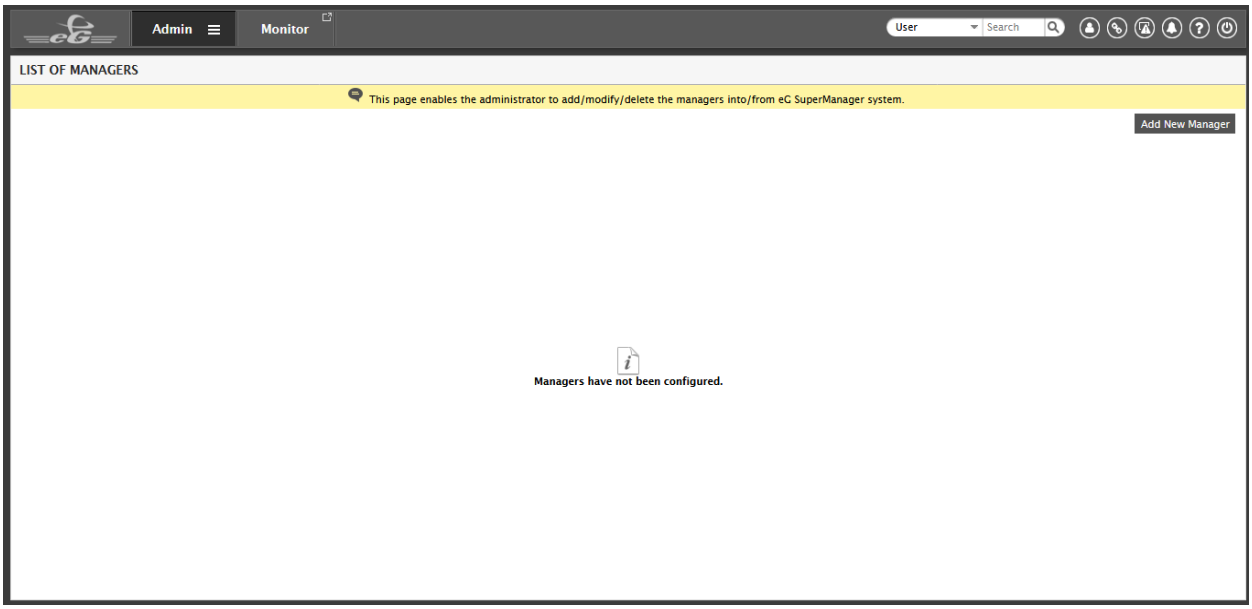


Figure 4.3: The Admin Home page of the eG SuperManager system

To manage an eG manager to report to the eG SuperManager, click the **Add New Manager** button in Figure 4.3. Figure 4.4 then appears.

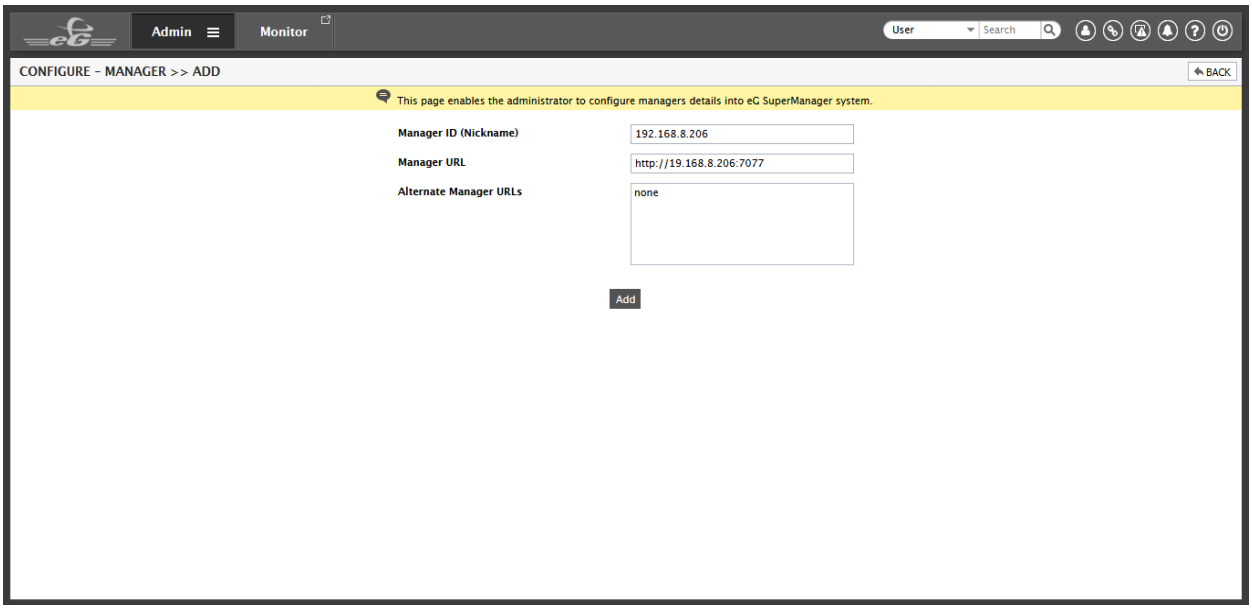


Figure 4.4: Adding a new eG manager to be managed by the eG SuperManager

In Figure 4.4, specify the nickname of the eG manager that you wish to be managed by the eG SuperManager against the **Manager ID (Nickname)** field. Specify the URL of the eG manager against the **Manager URL** field. If the eG manager to be managed contains any alternate URLs

using which the eG SuperManager can communicate with the eG manager, then specify such alternate URL against the **Alternate Manager URLs** text box. By default, *none* is specified against this text box.

Note:

If the primary eG manager in a redundant cluster is installed via proxy installation, then such eG manager will not report to the eG SuperManager.

Clicking the **Add** button in Figure 4.4 populates the **LIST OF MANAGERS** page (see Figure 4.5) with the eG manager that you have managed for the eG SuperManager.

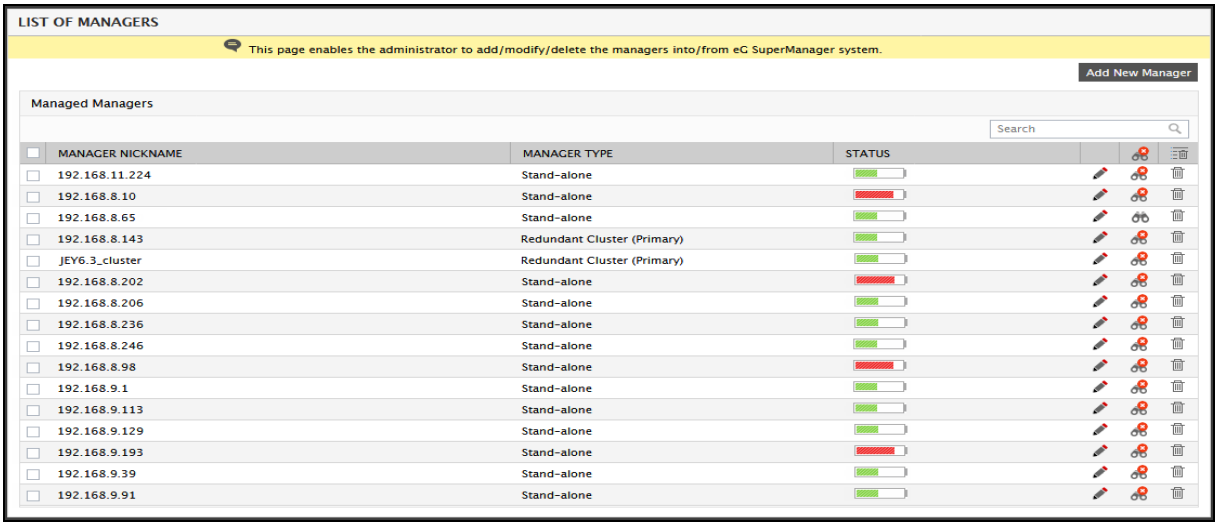


Figure 4.5: The list of manager added to report to the SuperManager

This **LIST OF MANAGERS** page can also be accessed using the menu sequence *Admin -> Manager Details*.

By default, this page lists the nickname of the eG manager managed to report to the eG SuperManager. eG Enterprise is capable of automatically detecting the type of the eG manager (whether stand alone or in a redundant cluster) and for each eG manager, the type is displayed in the **MANAGER TYPE** column (see Figure 4.5).

The status of the eG manager (whether running or stopped) can be detected at a single glance using the battery bar as shown in Figure 4.5.

To modify the details of the eG manager managed to report to the SuperManager, click the button in this page. Figure 4.6 then appears.

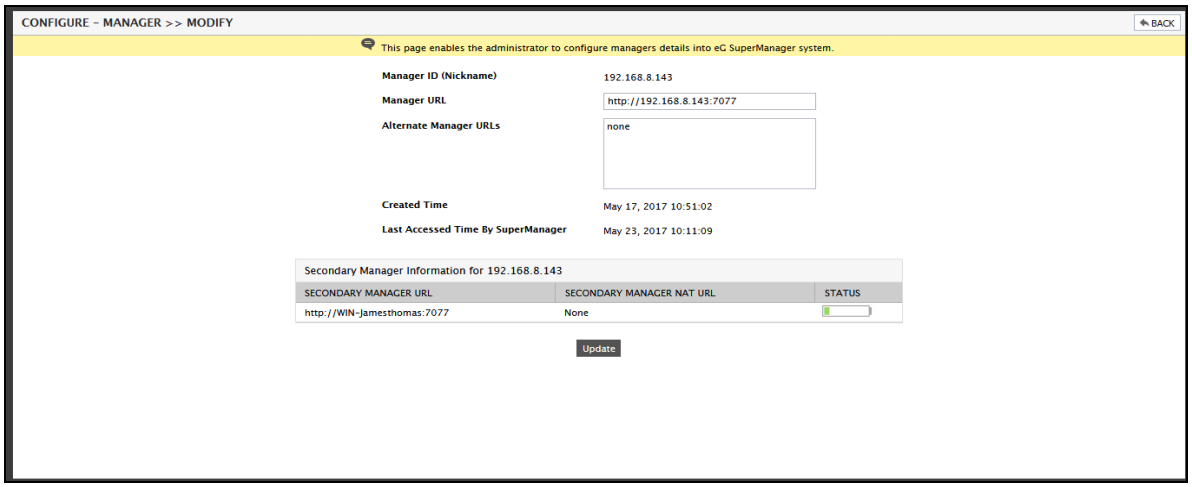


Figure 4.6: Modifying an eG manager in a redundant cluster

In Figure 4.6, you are allowed to specify the **Manager URL** and a comma-separated list of **Alternate Manager URLs**.

Sometimes, you may want to unconfigure the eG manager from reporting to the SuperManager but do not want to delete it completely. To achieve this, click on the icon against the manager in Figure 4.5. If the manager is unconfigured, the icon will be displayed against the manager. If a manager is unconfigured, then, the SuperManager will check only for the status of the manager but the manager will not report crucial statistics to the SuperManager. If you want to configure the unconfigured manager, simply click on the icon against the manager. To unconfigure/configure all the eG managers reporting to the eG SuperManager, click on the / against the **MANAGER NICKNAME** label.

To delete an eG manager reporting to the eG SuperManager, simply click the icon against the manager in Figure 4.5. To delete all the eG managers reporting to the eG SuperManager, select the check box against the **MANAGER NICKNAME** label and click the icon.

Figure 4.7: Deleting the managers reporting to the SuperManager

Figure 4.7 then appears asking you to confirm the delete operation. This delete operation is permanent and cannot be recovered. Clicking **Yes** deletes the information of all the eG managers reporting to the eG SuperManager.

4.2 The Admin Menu and Toolbar

The **Admin** menu is available as tiles and can be invoked by clicking the icon adjacent to the tab labelled **Admin**. The tiles that appear and the options they offer are as follows:

- **Infrastructure**: This menu enables the administrator to discover, manage, and add/modify components to the eG Enterprise system, configure zones, services, segments, component groups, and component topologies.
- **Audits**: eG Enterprise can be optionally configured to log every user action performed on the eG SuperManager user interface. Using the **Audits** menu, a variety of reports can then be generated based on the details logged, so as to enable the administrator to audit the following:
  - User logins to the eG Enterprise system
  - Failed login attempts to the eG Enterprise system
  - Configuration changes effected by users to the eG administrative interface
  - User activities with respect to the eG monitoring console

  By default, the 'audit logging' capability of the eG SuperManager is disabled. Therefore, the **Audits** menu will not be available by default.

  At the right, top corner of the **Admin** interface, you will find a tool bar. The table below briefly describes the tools provided by this tool bar:

Tool	Tool Name	Purpose
	Current user	Move your mouse pointer over this tool to know who is currently logged in. Click on the tool to edit the profile of the user logged in.
	Quick links	This feature is not available for the SuperManager.
	SuperManager notification	Click here to pull down a message board, where the eG SuperManager displays useful messages for the administrator. Such messages may intimate administrator of agents that may not be running, or

Tool	Tool Name	Purpose
		components recently managed and awaiting test configuration.
	Quick alerts	You can click on this icon from anywhere in the eG management console to take a quick look at the current alarms.
	Help	Click here for a context-sensitive help page providing useful information pertaining to the page that is currently open.
	Signout	Click here to sign out of the eG administrative interface.

If your user profile has monitoring rights, then a **Monitor** tab will appear, clicking on which will enable you to login to the eG monitoring console, without having to log out of the admin interface. By default, clicking on the tab will open the monitor interface in the currently open window itself. If you want the console to open in a separate window instead, click on the  symbol next to the tab page name **Monitor**.

In addition to the tools mentioned above, the eG management console now embeds an intelligent search capability. Regardless of which interface you are on (admin/monitor) or what you are doing, you can instantly check on the status of the mission-critical servers, services, segments, and zones using this intuitive search engine. All you need to do is use any of eG's pre-configured search prefixes and add your search condition to it, and upon clicking the **Search** icon, within seconds, the element you are searching for and its current status will be made available to you. The default pre-configured search prefixes are **Service**, **Segment**, **Component**, **Zone**, **VM/Desktop** and **User**. The **User** search is limited to the users who are currently logged into the VM/Desktop.

4.2.1 The User Profile Window

Whenever a user logs into the eG administrative interface, he/she can view/edit his/her profile by clicking the  tool in the toolbar of the eG management console. The **USER PROFILE** drop-down window then appears (see Figure 4.8). This window allows the user who is logged into the eG management console to quickly edit his/her profile.

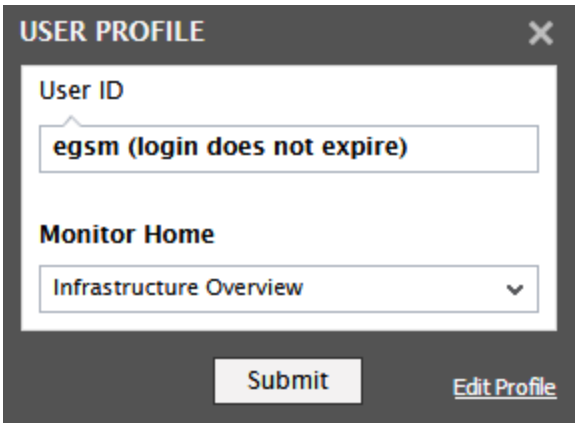


Figure 4.8: The User Profile window

By default, Figure 4.8 shows the current settings of the user. The **User ID** text box displays the login ID of the user. The default page that the user needs to view upon navigating to the eG monitoring console is displayed in the **Monitor Home** list. By default, the **Infrastructure Overview** is chosen from this list. If the user has not configured any of the above, then he/she can configure the same from this window and click the **Submit** button. If the user wishes to edit his/her profile, then, he/she can click the **Edit Profile** link in Figure 4.8.

Upon clicking the **Edit Profile** link in Figure 4.8, Figure 4.9 appears.

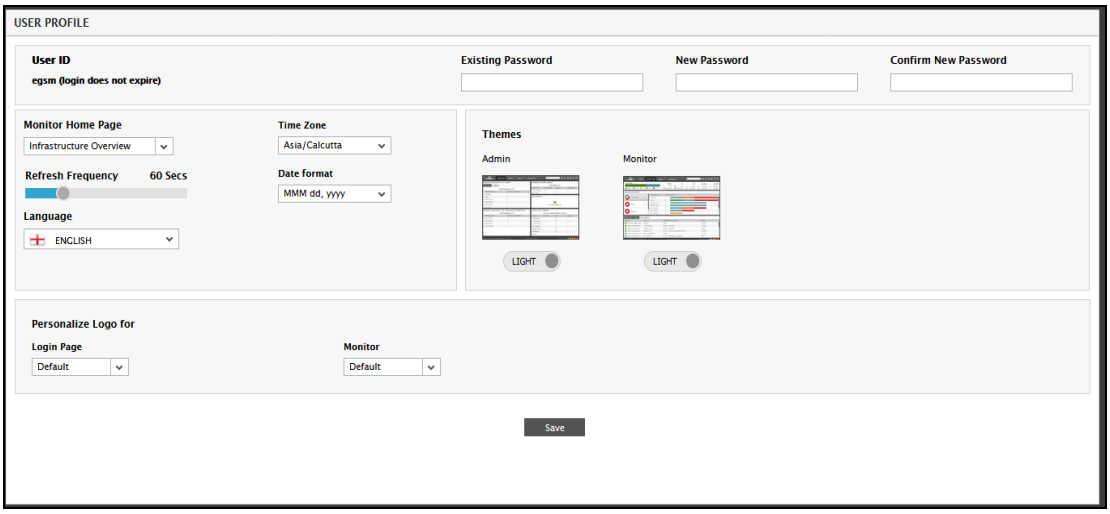


Figure 4.9: The USER PROFILE page that is used to edit the user preferences

Using Figure 4.9, the user is allowed to change his/her password. To provide a new password, the user should specify the **Existing Password** and then specify a password in the **New Password**

text box. To confirm the password, it is necessary to enter the new password in the **Confirm Password** text box.

Monitor Home Page: By default, the **Infrastructure Overview** appears as the home page of the eG monitoring console - i.e., as soon as a user logs into the monitoring console, the **Infrastructure Overview** appears as the first page by default. eG Enterprise however, allows administrators to set any page they deem fit as the Monitor Home Page for individual users to the eG monitoring console. This way, every user, upon logging into the eG monitor interface, is enabled to view straight up the information that interests him/her the most, thereby saving time and minimizing the mouse clicks that may be required to navigate to that information!

The home page preference is typically driven by the monitoring needs of specific users and the roles assigned to them. For instance, a service manager, who is responsible for minimizing/eliminating service outages, would want to know on login how all the critical services in the environment are performing currently, and which services are in an abnormal state. For this purpose, administrators may want to set the Service List as the home page of such users.

Refresh Frequency: Indicates how often the web pages of the eG monitor module need to be refreshed. By default, this is set to 60 seconds.

Date format to be used: The default date format for the eG user interface is MMM dd, yyyy. This date format can be changed depending upon the country in which the user being created lives, by selecting a different format from the Date format list. Whenever this user logs in, the eG user interface will display dates in the chosen format only. This is particularly useful in MSP environments, where customers of the MSP could be separated by geographies and may require performance and problem reports of their hosted enivonments to be delivered in the date format that applies to their geography.

Language: The eG SuperManager provides multi-language support, but the default language is 'ENGLISH'. To configure the eG SuperManager to support a different language by default, select the language of your choice from the **Language** list.

Time Zone: eG Enterprise is often deployed to manage servers in different geographies and time zones. For example, a large enterprise may have a central eG Enterprise management console to which agents from different locations can be reporting. In a managed service provider environment, multiple customer infrastructures can be monitored from the same eG SuperManager. In such situations, users (administrators in different geographies, customers of an MSP in different regions) prefer to see the performance metrics reported in their respective time zones. eG Enterprise allows time zones to be associated to each user's profile. By default, all users are associated with the local time zone of the location where the eG SuperManager is hosted. However, an administrator can

change the time zone preferences of a user to suit that user's requirements. For this, when creating a user profile, the administrator can pick a Time zone for that user. When that user logs into the eG Enterprise console, all the metrics, alerts, and reports that the user accesses will be displayed in the respective local time zone. This capability ensures that eG Enterprise users receive a completely 'local' experience, regardless of which part of the world the eG SuperManager is located in.

Themes: eG Enterprise has a refreshing new user interface. Designed based on Web 2.0 concepts, the eG Enterprise interface is visually appealing, easier to navigate, intuitive, and fluid. The interface is designed to be pleasing on the eye, to be easier to navigate, so that users can get to the tasks they need to perform faster, and to function well over local and wide area networks and on any device (including tablets and big screens). A clear separation between the visual representation and the data that is rendered ensures that only changes in data values are sent over the network, leading to bandwidth optimization. Users can now choose between a light and dark color theme based on their tastes for all the modules offered by the eG Enterprise. If the user wishes to choose a dark theme for the monitor module, then he/she may click the **Light** button below the **Monitor** option.

Personalize Logo for: Each user of the eG Enterprise system is allowed to configure a custom logo that is displayed in the eG user interface on all the modules. This way, different users can see different logos in the eG user interface. Accordingly, the user can set a different logo for the login screen and set another logo for the different modules offered by the eG Enterprise system. By default, the **Default** option is chosen from the **Login Page**. If **Custom** option is chosen from this list, then an **Upload** button appears.

Clicking the **Upload** button opens Figure 4.10 where the user would be allowed to upload the image of his/her choice. In the **Custom Logo** text box, the user can specify the full path to the image file to be uploaded using the **Browse** button therein and click the **Upload** button.

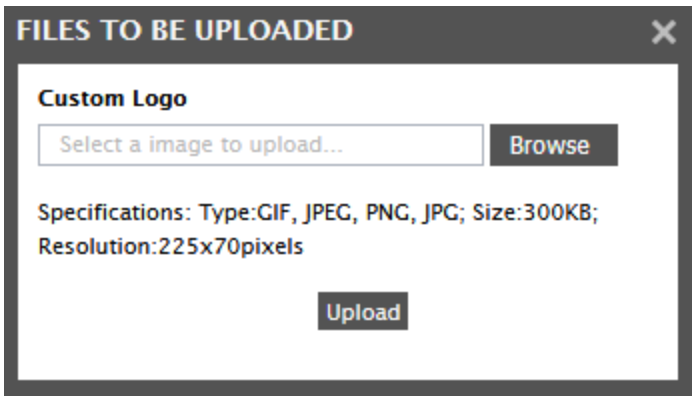


Figure 4.10: Uploading a custom logo

Similarly, the custom logo can be applied for the **Admin/Monitor** consoles of the eG Enterprise system. By default, the check box against the **Apply to other modules** option is checked implying that the logo that is uploaded would apply to other modules too. If the user wishes to upload for a particular module alone, then he/she can uncheck this check box.

Clicking the **Save** button will register the changes made.

Note:

The *egsm* user is alone entitled to modify the user profile settings. The same settings are applicable to all other users logging into the eG SuperManager.

4.2.2 The SuperManager Notification Window

As soon as a user logs into the eG administrative interface of the eG SuperManager, a **SUPERMANAGER NOTIFICATION** window (see Figure 4.11) automatically pops up. This window serves as a message board where critical messages of significance to an eG administrator will be published.

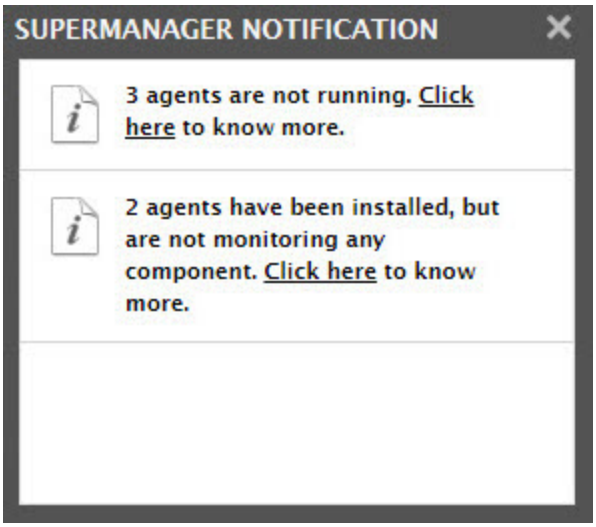


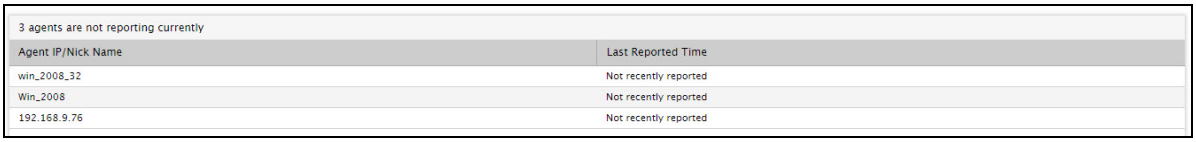
Figure 4.11: The Manager Notification window

An administrator can configure the type of messages that he/she wants displayed in the board. By default, the notification window alerts administrators to the following:

- eG license expiry
- Exhaustion of eG agent licenses
- Agents not running

- Components newly discovered
- Agents awaiting test configuration

At any given point in time, administrators can click on the **Click here** hyperlink accompanying a message in the **SUPERMANAGER NOTIFICATION** window (see Figure 4.11) for more details on a particular alert. For instance, Figure 4.11 indicates that 3 agents are not running. Clicking on the **Click here** hyperlink alongside this message in Figure 4.11 will lead the administrator to Figure 4.12, which displays the list of agents that are not running currently.



3 agents are not reporting currently

Agent IP/Nick Name	Last Reported Time
win_2008_32	Not recently reported
Win_2008	Not recently reported
192.168.9.76	Not recently reported

Figure 4.12: A page displaying the list of agents that are not running

To close the **SUPERMANAGER NOTIFICATION** window, you can either move your mouse pointer over the window or click the **X** button at its right, top corner. Once closed, you can invoke the **SUPERMANAGER NOTIFICATION** window yet again by clicking the button in the **Admin** toolbar (at the right, top corner of the eG admin interface).

4.2.3 Quick Alerts

eG Enterprise brings problems to the attention of administrators via multiple modes such as the eG monitoring console, emails, SMS, and SNMP traps. The latest addition to this list is the optional, **Quick Alerts**. The **Quick Alerts** mechanism introduced by eG Enterprise, saves administrator of the eG SuperManager the time and trouble involved in switching to the eG monitoring console, everytime he/she needs a quick update on the problems affecting the infrastructure. This feature helps administrators track problems continuously by displaying the number and details of current alarms when the icon at the right, top corner of the eG management console is clicked.

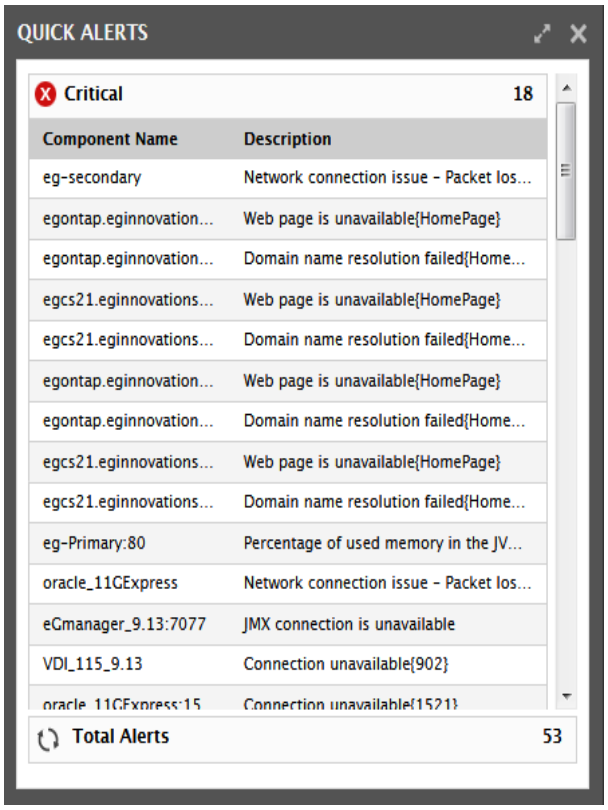


Figure 4.13: Quick Alerts

The **QUICK ALERTS** window that appears (see Figure 4.13) groups alarms by priority and displays the count and details of alarms of each priority. Clicking on an alarm here will lead the user to the layer model of the problem component, which will reveal the exact layer that is affected by the problem, the test that reported the problem, and the problematic measure.

This way, a user can receive instant updates on performance issues and can even drill down to ascertain the exact nature of the issue, regardless of which eG module he is logged into currently.

Note:

The **QUICK ALERTS** window will display the alarms pertaining to only those components that have been assigned to the user (who is currently logged into eG SuperManager) for monitoring.

4.3 Viewing the Infrastructure of the managed eG managers

Multiple eG managers may be simultaneously reporting to the SuperManager. The administrator of the SuperManager or the *egsm* user may want to know the infrastructure of each eG manager in detail. To cater to the needs of such administrators, eG Enterprise provides a

MANAGED INFRASTRUCTURE page. This page can be accessed by following the menu sequence: *Admin -> Overview*. (see Figure 4.14)

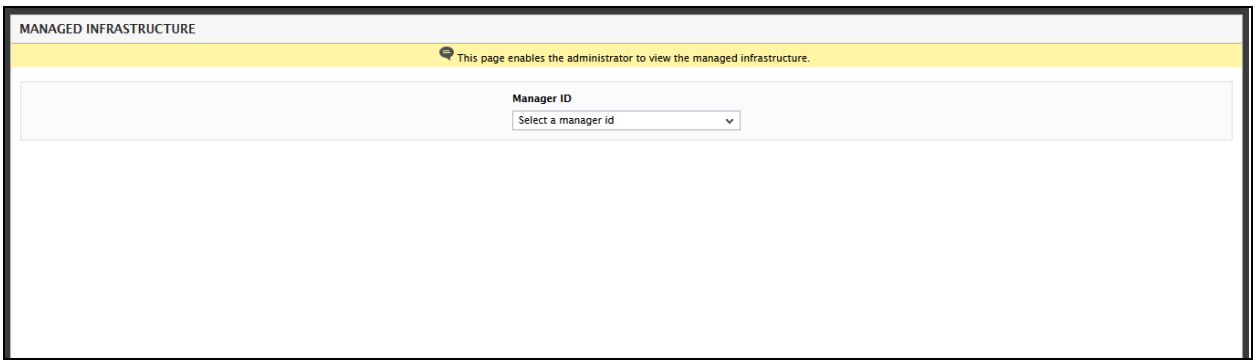


Figure 4.14: Selecting the Manager ID

Select a **Manager ID** from Figure 4.14. Figure 4.15 then appears. From the **View** list, select an element of your choice. If zones/services/segments/service groups/aggregated components/components are managed in the chosen manager, then all the options will be listed as shown in Figure 4.15.

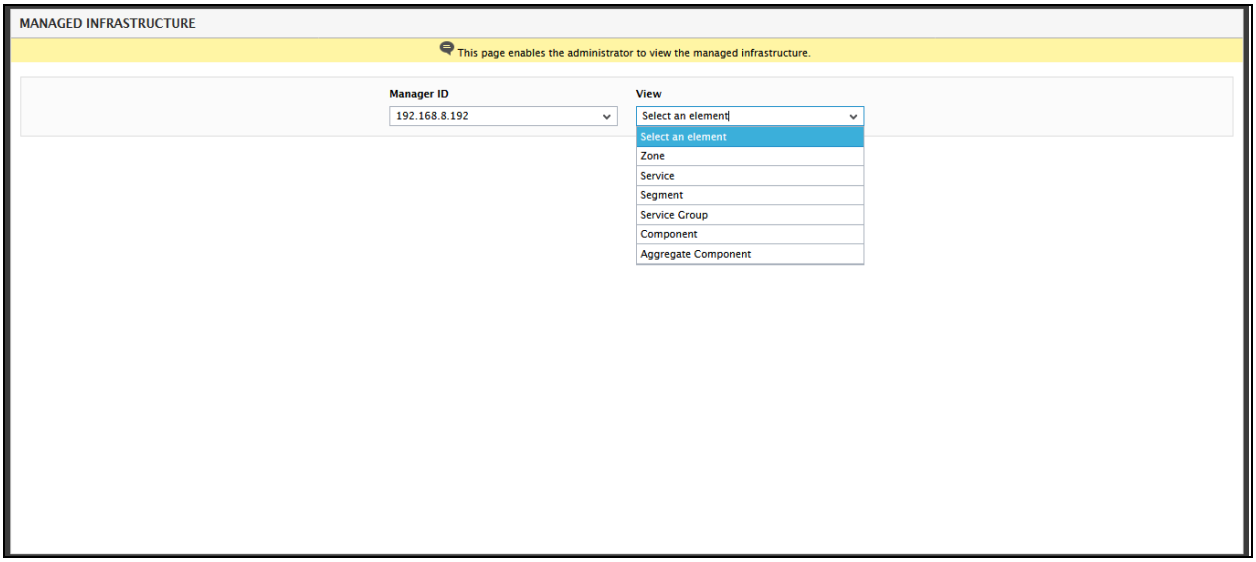


Figure 4.15: Choosing an element of your choice

If **Service** is chosen from the **View** list, then Figure 4.16 will appear displaying the services associated with the chosen eG manager.

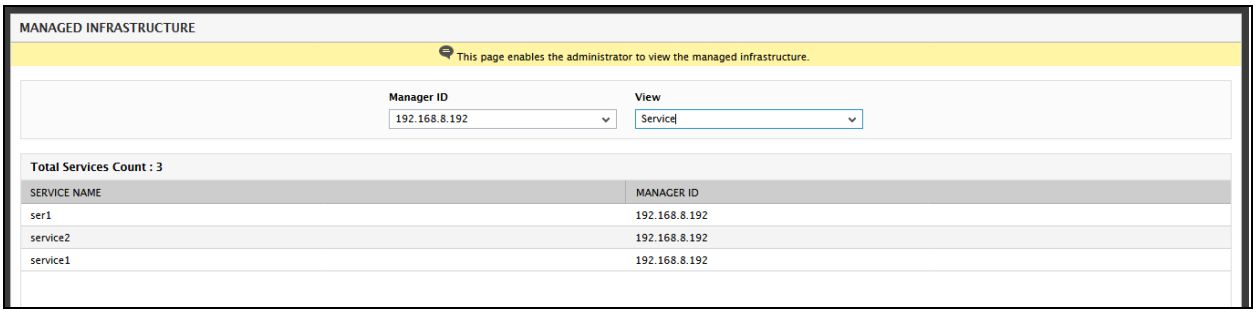


Figure 4.16: Viewing the services associated with the managers managed by the SuperManager

If the **Component** option is chosen from the **View** list, then an additional **Component Type** list will appear using which you can pick and choose to view the components of your choice. If *ALL* option is chosen from the **Manager ID** list, **Component** option is chosen from the **View** list and *ALL* option is chosen from the **Component Type** list, then, Figure 4.17 appears listing all the components with the manager ID.

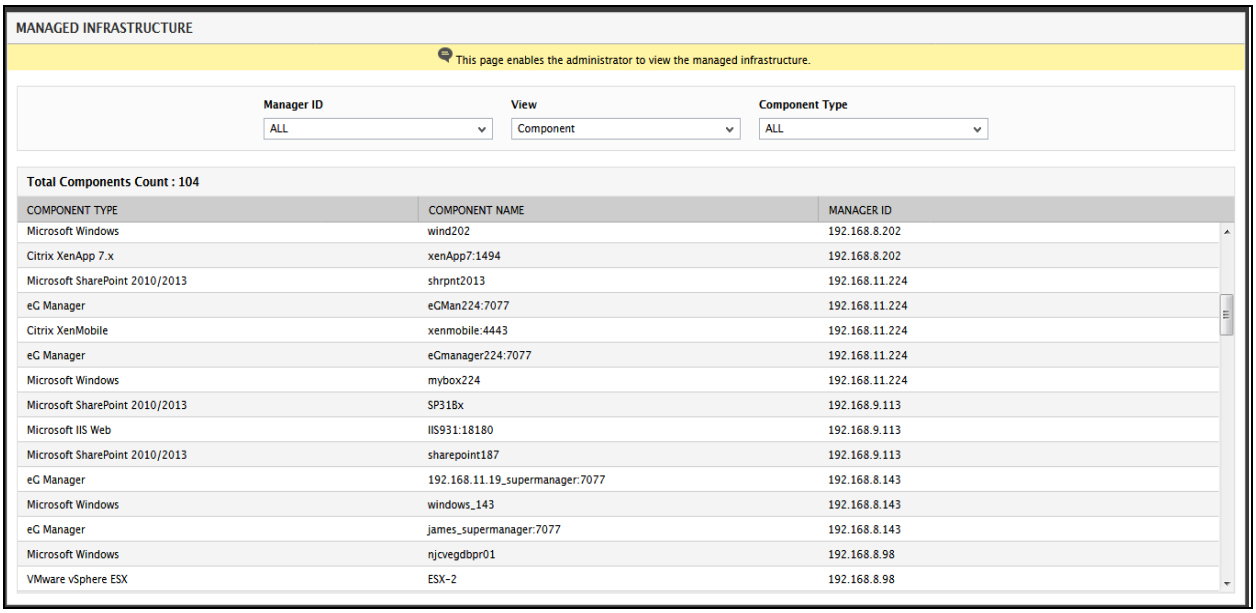


Figure 4.17: Viewing the Components in all the managers managed by the SuperManager

4.4 Audit Logging

An audit log can be best described as a simple log of changes, typically used for tracking temporal information. The eG SuperManager is configured to create and maintain audit logs in the eG SuperManager database, so that all key configuration changes to the eG SuperManager system, which have been effected via the eG user interface, are tracked.

The eG audit logs reveal critical change details such as what has changed, who did the change, and when the change occurred, so that administrators are able to quickly and accurately identify unauthorized accesses/modifications to the eG SuperManager system.

By default, audit logging capability is disabled for the SuperManager. If for any reason you want to enable this capability, follow the steps given below:

- Open the **eg_ services.ini** available in the **<eG_ SUPERMANAGER_ INSTALL_ DIR>\manager\config** folder.
- Set the **AuditlogEnabled** flag in to **yes**.
- Save the **eg_services.ini** file.

By default, every configuration change that the user makes will be automatically logged in the SuperManager database. To view the details logged and analyze their implications, eG SuperManager system provides an exclusive **Audits** menu in its administrative interface, using which you can generate a variety of audit log reports.

The following sections deal with each one of these report types.

4.4.1 Auditing Successful User Logons

To view the details of a chosen user's sessions with the eG SuperManager system, use the **SUCCESSFUL LOGON REPORTS**. This report enables administrators to determine which user (s) was actively using the eG SuperManager system during periods when the target environment was experiencing performance issues or exhibiting a strange behavior. Unauthorized accesses and rogue users can thus be identified quickly. Moreover, these reports embed a special drill-down feature, which allows you a quick look at the actions performed by a particular user during the period of his/her access. This sheds light on changes effected by the user, which could have caused problems.

To access the **SUCCESSFUL LOGON REPORTS** page, follow the menu sequence: *Audits -> Successful Logons*. Figure 4.18 then appears.

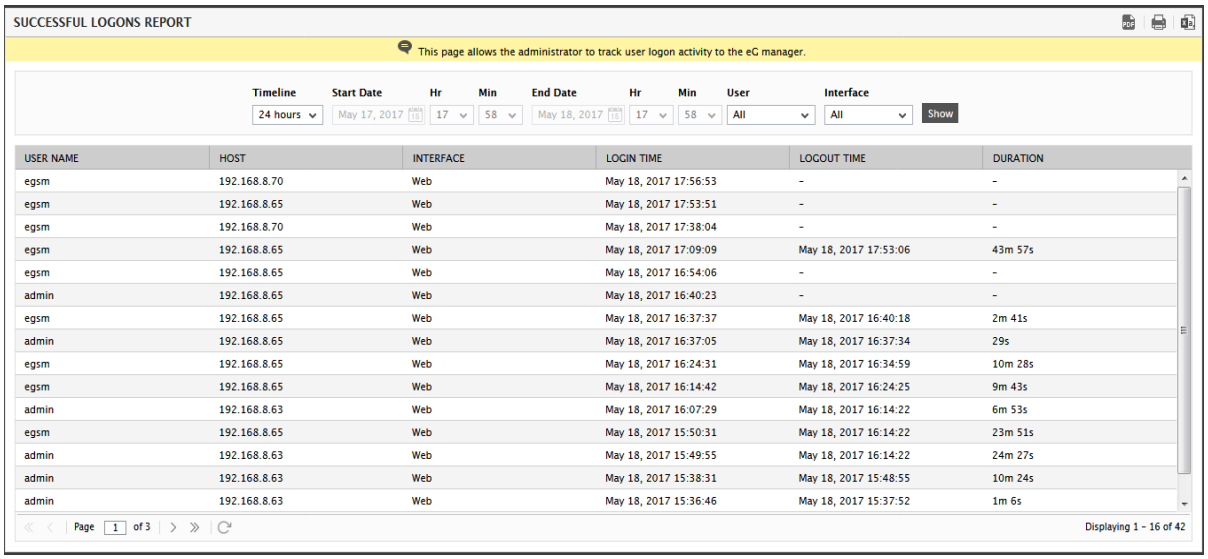


Figure 4.18: Successful logons

To generate a report on successful logons using this page, do the following:

1. Select a **Timeline** for the report. The default **Timeline** for the report is *24 hours*. You can choose any other fixed period from the **Timeline** list, or select the **Any** option from this list. Choosing the **Any** timeline, allows you to provide a **Start Date** and **End Date** date and time for report generation. You can even choose the exact time using the **Hr** and **Min** lists.
2. Next, select the **User** whose accesses you want to audit. By default, the **All** option is displayed here, indicating that the report provides the details of the sessions of all users to the eG SuperManager system. However, if only one user has successfully logged into the eG SuperManager system till date, then, by default, that user's name is displayed in the **User** list.
3. By default, the report displays a maximum of *15* records per page. You can override this default setting, by specifying a different value against the **Row_multiplier** parameter in the **[AUDIT_LOG_SETTINGS]** section of the **eg_ui.ini** file (in the {EG_INSTALL_DIR}\manager\config directory). For instance, if 10 is specified against **Row_multiplier**, then this report displays 10 records per page.
4. Finally, click the **Show** button to generate the report.

   The resulting report provides details of every successful login made by the chosen user(s). These details include:

- the name of the user
- the IP address of the host from which the user accessed the eG SuperManager
- the exact time of login
- the accurate time of logout
- the duration of the user access

5. Clicking on a user name in this page leads you to the details of what configuration changes were made by that user during the period of his/her access.
6. If the report runs across pages, then the **Page** box and the **>**, **>>**, **<**, and **<<** links at the bottom of the page will aid navigation.
7. You can print the report by clicking on the icon in Figure 4.18, or save the report as a PDF file by clicking on the icon. You can even save the report as a CSV file by clicking on the icon in Figure 4.18
8. Clicking on a user name in Figure 4.18 leads you to Figure 4.19, which reveals what configuration changes were made by that user during the period of his/her access.

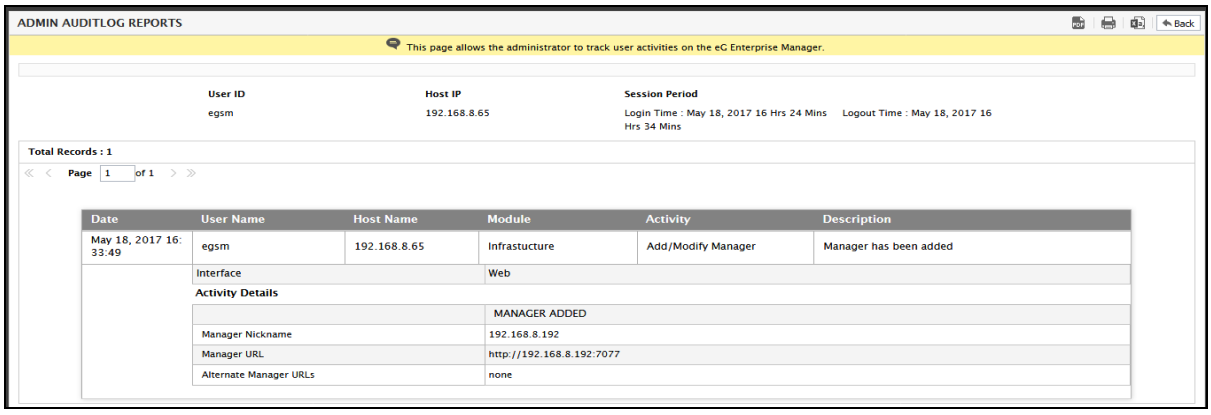


Figure 4.19: The page that appears upon clicking the username

4.4.2 Auditing Failed Logons

To view the details of user logons to the eG SuperManager system that failed, use the **FAILED LOGON** reports. Using such a report, you can figure out which were the login attempts that failed and why. The reasons can bring to light network connection issues that need to be repaired, or login attempts that are rather 'suspect'.

To access the **FAILED LOGON REPORTS** page, follow the menu sequence: Audits -> Failed Logons. Figure 4.20 will then appear.

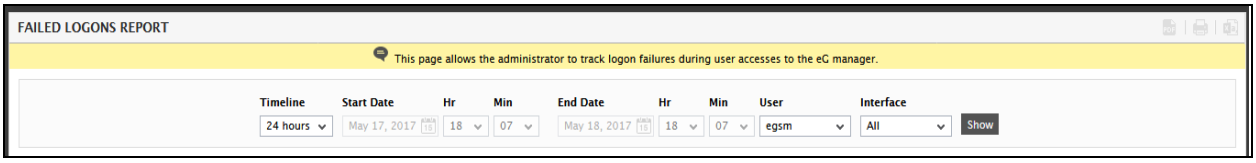


Figure 4.20: The Failed Logon Reports page

To generate a report on failed logons using Figure 4.20, do the following:

1. Select a **Timeline** for the report. The default **Timeline** for the report is 24 hours. You can choose any other fixed period from the **Timeline** list, or select the **Any** option from this list. Choosing the **Any** timeline, allows you to provide a **Start Date** and **End Date** and time for report generation. You can even choose the exact time using the **Hr** and **Min** lists.
2. Next, select the **User** whose login attempts you want to audit. By default, the **All** option is displayed here, indicating that the report provides the details of failed login attempts of all users to the eG SuperManager system. However, if only one user had problems logging in till date, then, by default, that user's name is displayed in the **User** list.
3. By default, the report displays a maximum of *15* records per page. You can override this default setting, by specifying a different value against the **Row_multiplier** parameter in the **[AUDIT_LOG_SETTINGS]** section of the **eg_ui.ini** file (in the {EG_INSTALL_DIR}\manager\config directory). For instance, if 10 is specified against **Row_multiplier**, then this report displays 10 records per page.
4. Finally, click the **Show** button to generate the report. Figure 4.21 will then appear.

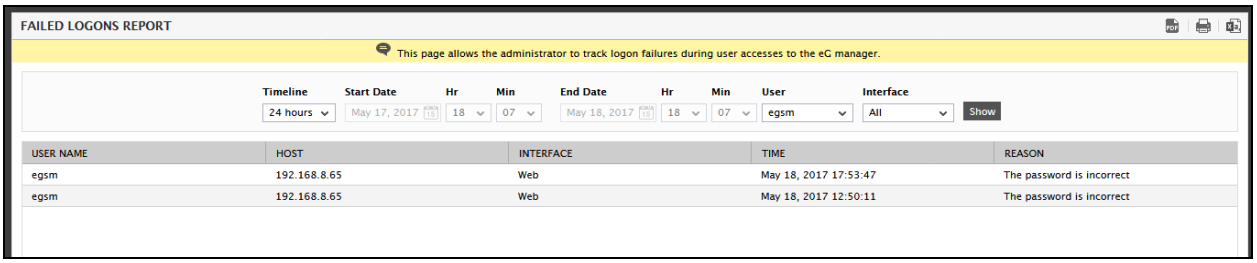


Figure 4.21: The report generated for failed logons

5. The resulting report as shown in Figure 4.21 provides details of every login made by the chosen user(s) that failed. These details include:

- the name of the user
- the IP address of the host from which the user attempted to login to the eG management console
- the exact time of login attempt
- the reason for the login failure

6. If the report runs across pages, then the **Page** box and the **>**, **>>**, **<**, and **<<** links at the bottom of the page will aid navigation.
7. You can print the report by clicking on the icon in Figure 4.21, or save the report as a PDF file by clicking on the icon. You can even save the report as a CSV file by clicking on the icon in Figure 4.21.

4.4.3 Auditing Configuration Changes made using the eG SuperManager Administrative Interface

Generally, you can generate audit log reports that enable an administrator to keep tab on critical configuration changes made using the eG admin interface. These changes could be password changes, new manager additions, unmanaging a manager from the SuperManager etc., which can significantly alter the way the eG SuperManager system performs monitoring. Sometimes, these configuration changes, if not done properly or if carried out by unauthorized/unqualified personnel, can cause the eG Enterprise system to generate false alerts and perform inaccurate diagnosis.

As these **AUDITLOG REPORTS** reveal what admin settings were modified by which user, along with the details of the original settings, they greatly help administrators in quickly identifying and rectifying errors (if any) in configuration.

To generate the **Admin** related audit log reports, do the following:

1. Follow the menu sequence: *Audits -> Admin*. Figure 4.22 will then appear where you can provide the credentials to generate the report of your choice.

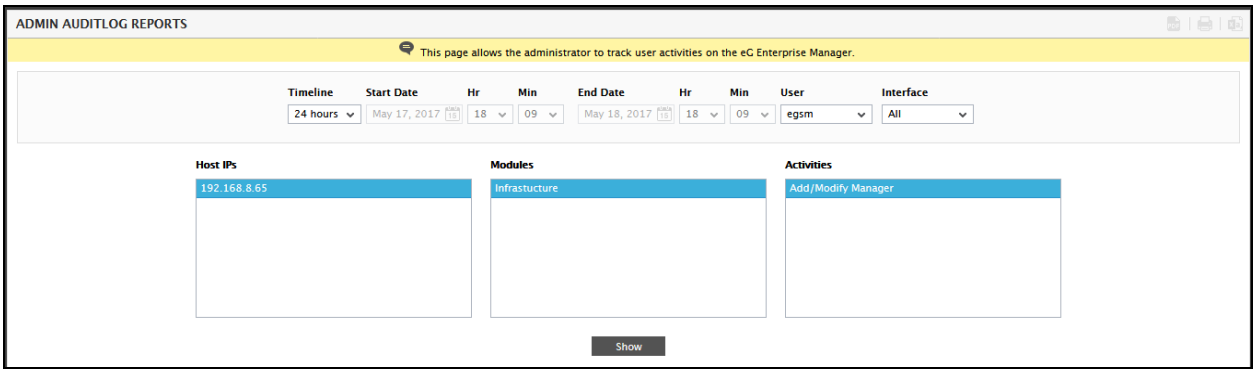


Figure 4.22: Generating an auditlog report

2. In Figure 4.22, select a **Timeline** for the report. The default **Timeline** for the report is *24 hours*. You can choose any other fixed period from the **Timeline** list, or select the *Any* option from this list. Choosing the *Any* timeline, allows you to provide a **Start Date** and **End date** and time for report generation. You can even choose the exact time using the **Hr** and **Min** lists.

3. Next, select the **User** whose admin activities you want to audit. By default, the **All** option is displayed here, indicating that the report provides the details of all the users who have actively used the eG administrative interface till date. However, if only one user had extensively used the eG administrative interface of the SuperManager till date, then, by default, that user's name is displayed in the **User** list.

4. By default, the report displays a maximum of 15 records per page. You can override this default setting, by specifying a different value against the **Row_multiplier** parameter in the **[AUDIT_LOG_SETTINGS]** section of the **eg_ui.ini** file (in the {EG_INSTALL_DIR}\manager\config directory). For instance, if 10 is specified against **Row_multiplier**, then this report displays 10 records per page.

5. The **Host IPs** list displays all the IP addresses from which the chosen user(s) has accessed the eG administrative interface of the SuperManager. If you are looking for information on the admin accesses from specific IPs, select those IP addresses alone from the **Host IPs** list.

6. After the selection, the **Modules** list will be populated with those admin modules that the chosen user(s) worked with while accessing the eG admin interface of the SuperManager from the selected Host IPs. If you want the details of changes that the user made in specific admin modules, select those modules alone from the **Modules** list.

7. Based on the **Modules** selection, the **Activities** list will be populated. While working with the eG admin interface, the selected user(s) might have performed a few specific operations on the chosen **Modules**. eG Enterprise automatically discovers the operations that correspond to the chosen user-host IP-module combination from the audit logs, and populates the **Activities** list

with the operations so discovered. If you want the details of specific activities only, select the required options alone from the **Activities** list.

8. Finally, click the **Show** button to generate the report. Figure 4.23 will then appear with the generated report.

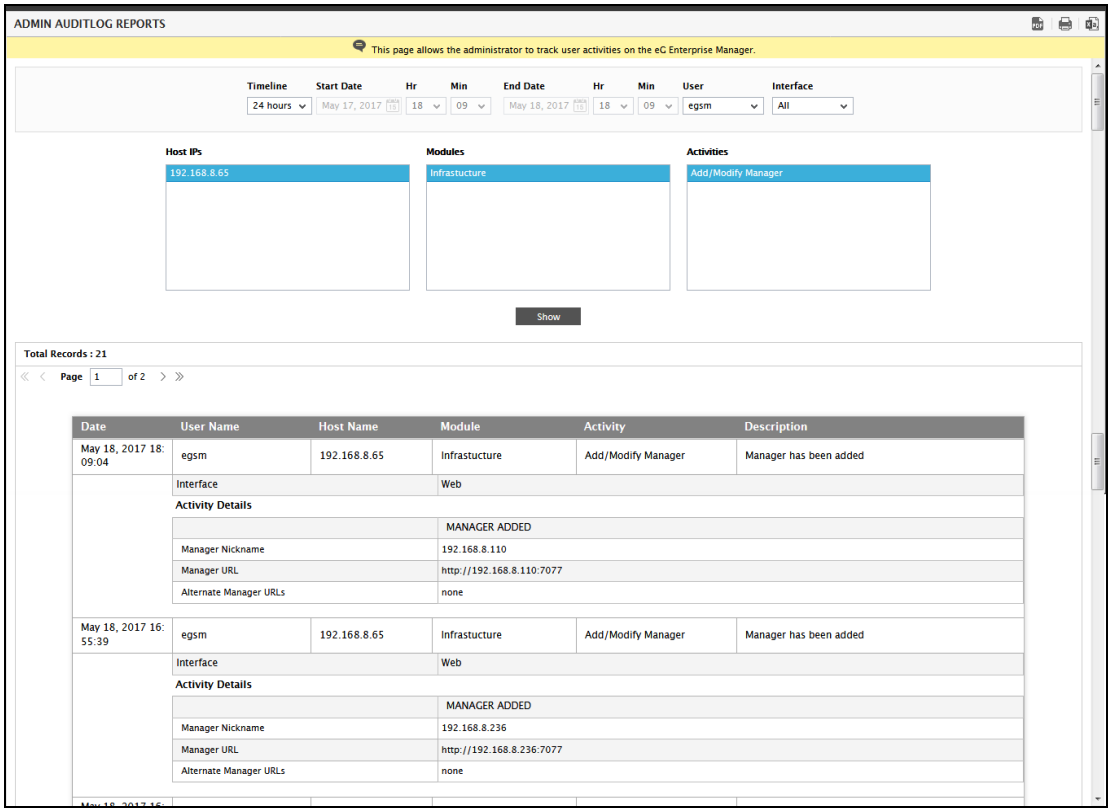


Figure 4.23: The auditlog reports

9. The resulting report as in Figure 4.23 provides the following details:

   - the date/time of the change
   - the name of the user who made the change
   - the IP address of the host from which the user accessed the eG admin interface of the SuperManager
   - the module that was accessed by the user
   - the specific operation/activity that was performed by the user on that module
   - the interface type used - whether web interface or command line interface

- the detailed description of the change, followed by a snapshot of the settings prior to change, and the settings after the change; if a configuration has been newly introduced (for e.g., a manager has been newly managed), then only the **Current Settings** will be displayed.

Note:

- By default, every change record that the report displays will be accompanied by the **Current** and **Previous** configuration settings. This can sometimes clutter the report view, making it difficult for you to read and analyze the report. You can therefore hide both these columns from the report, by setting the **ShowChanges** parameter in the **[AUDIT_LOG_SETTINGS]** section of the **eg_ui.ini** (in the {EG_INSTALL_DIR>\manager\config directory) file to **false**.
- In a redundant setup, the auditlog report will have an additional **MANAGER NAME** column, which displays the IP or host name of the manager to which a record pertains.

10. If the report runs across pages, then the **Page** box and the **>**, **>>**, **<**, and **<<** links at the bottom of the page will aid navigation.
11. You can print the report by clicking on the icon in Figure 4.23, or save the report as a PDF file by clicking on the icon. You can even save the report as a CSV file by clicking on the icon in Figure 4.23.

4.4.4 Auditing Configuration Changes made using the eG SuperManager Monitor Interface

The critical configuration changes made using the eG SuperManager Monitor system can be viewed using the *Audits -> Monitor* menu sequence. Generally, the monitor configuration changes like allowing alarm deletion, alarm acknowledgment for a particular user etc, can be identified easily and errors, if any can be rectified.

To generate the **Monitor** related audit log reports, do the following:

1. Follow the menu sequence: Audits -> Monitor. Figure 4.24 will then appear where you can provide the credentials to generate the report of your choice.

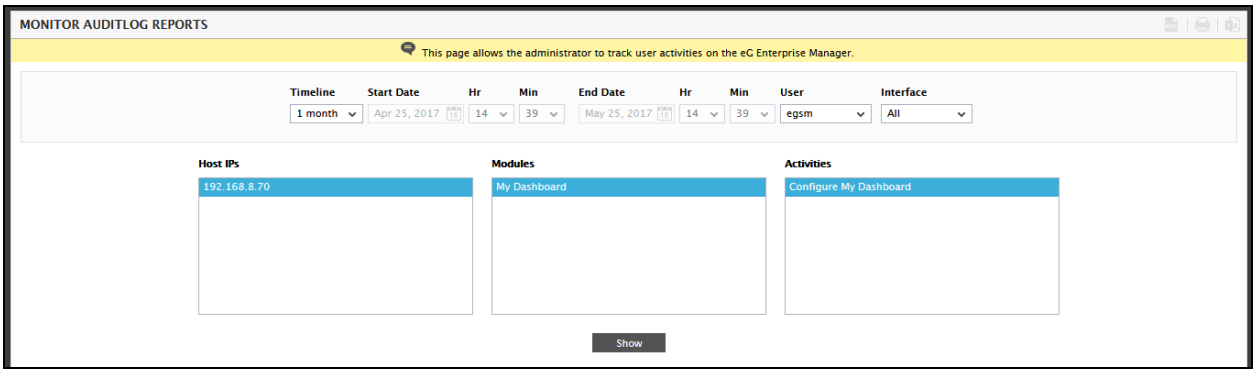


Figure 4.24: Generating an auditlog report

2. In Figure 4.24, select a **Timeline** for the report. The default **Timeline** for the report is 24 hours. You can choose any other fixed period from the **Timeline** list, or select the **Any** option from this list. Choosing the **Any** timeline, allows you to provide a **Start Date** and **End Date** and time for report generation. You can even choose the exact time using the **Hr** and **Min** lists.

3. Next, select the **User** whose monitor activities you want to audit. By default, the **egsm** option is displayed here, indicating that only the **egsm** user alone has actively used the eG administrative interface till date. However if more than one user has used the eG SuperManager monitor interface, then **All** option will be displayed, by default, from the **USER** list.

4. By default, the report displays a maximum of *15* records per page. You can override this default setting, by specifying a different value against the **Row_multiplier** parameter in the **[AUDIT_LOG_SETTINGS]** section of the **eg_ui.ini** file (in the {EG_INSTALL_DIR}\manager\config directory). For instance, if 10 is specified against **Row_multiplier**, then this report displays 10 records per page.

5. The **Host IPs** list displays all the IP addresses from which the chosen user(s) has accessed the eG monitor interface of the SuperManager. If you are looking for information on the monitor accesses from specific IPs, select those IP addresses alone from the **Host IPs** list.

6. After the selection, the **Modules** list will be populated with those monitor modules that the chosen user(s) worked with while accessing the eG monitor interface from the selected Host IPs. If you want the details of changes that the user made in specific admin modules, select those modules alone from the **Modules** list.

7. Based on the **Modules** selection, the **Activities** list will be populated. While working with the eG SuperManager admin interface, the selected user(s) might have performed a few specific operations on the chosen **Modules**. eG SuperManager system automatically discovers the operations that correspond to the chosen user-host IP-module combination from the audit logs,

and populates the **Activities** list with the operations so discovered. If you want the details of specific activities only, select the required options alone from the **Activities** list.

8. Finally, click the **Show** button to generate the report. Figure 4.25 will then appear with the generated report.

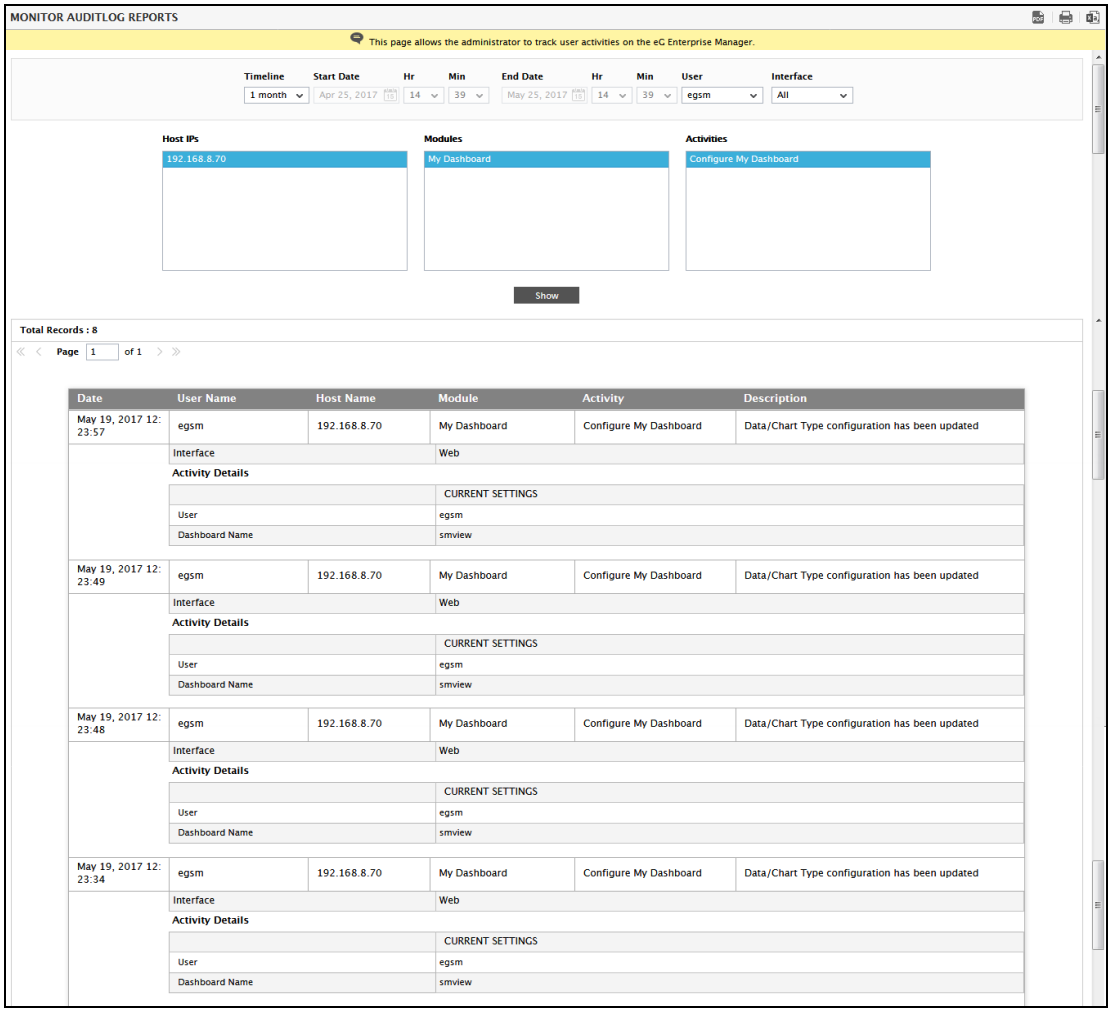


Figure 4.25: The auditlog reports for eG SuperManager monitor interface

9. The resulting report as in Figure 4.25 provides the following details:

   - the date/time of the change
   - the name of the user who made the change
   - the IP address of the host from which the user accessed the eG monitor interface of the SuperManager

- the module that was accessed by the user
- the specific operation/activity that was performed by the user on that module
- the interface type used - whether web interface or command line interface
- the detailed description of the change, followed by a snapshot of the settings prior to change, and the settings after the change; if a configuration has been newly introduced (for e.g., a manager has been newly managed), then only the **Current Settings** will be displayed.

Note:

- By default, every change record that the report displays will be accompanied by the **Current** and **Previous** configuration settings. This can sometimes clutter the report view, making it difficult for you to read and analyze the report. You can therefore hide both these columns from the report, by setting the **ShowChanges** parameter in the **[AUDIT_LOG_SETTINGS]** section of the **eg_ui.ini** (in the {EG_INSTALL_DIR>\manager\config directory) file to **No**.
- In a redundant setup, the auditlog report will have an additional **MANAGER NAME** column, which displays the IP or host name of the manager to which a record pertains.

10. If the report runs across pages, then the **Page** box and the **>**, **>>**, **<**, and **<<** links at the bottom of the page will aid navigation.
11. You can print the report by clicking on the icon in Figure 4.25, or save the report as a PDF file by clicking on the icon. You can even save the report as a CSV file by clicking on the icon in Figure 4.25.

Chapter 5: Working with the eG SuperManager

To understand the working of the eG SuperManager better, let us take the case of an environment that is distributed across New York and Ohio. Individual managers have been installed in New York and Ohio respectively, to monitor the status of IT operations in each of these cities. For an overall status report, an eG SuperManager has been configured at Chicago.

Prior to accessing the SuperManager, let us login to the New York and Ohio managers, to view their current status and current alarms. Figure 5.1 depicts the current issues affecting New York's performance.

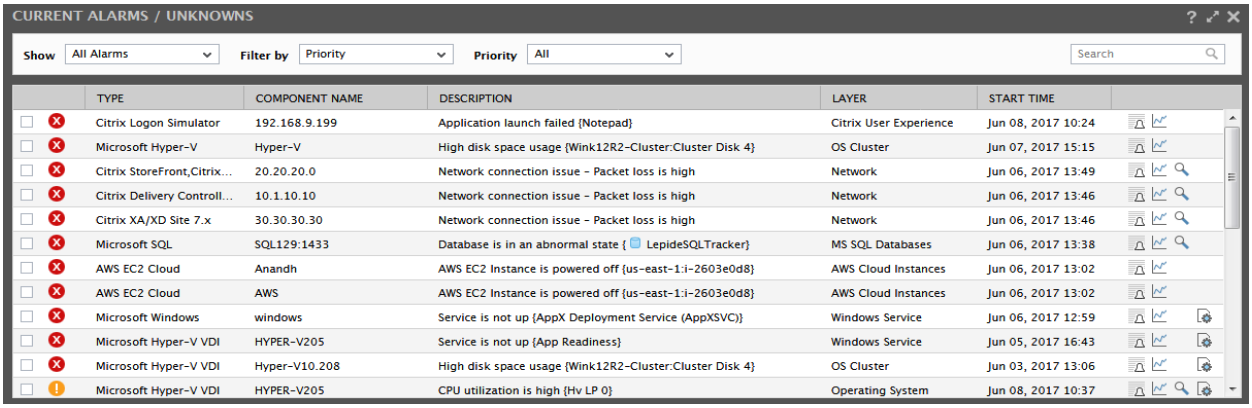


Figure 5.1: Alarms reported by the New York manager

Figure 5.2 depicts the issues reported by the Ohio manager.

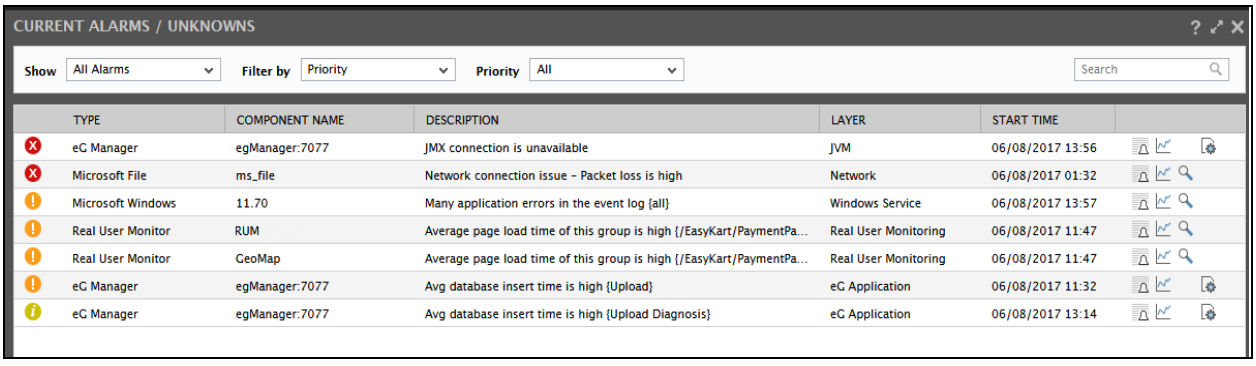


Figure 5.2: Alarms reported by the Ohio manager

Next, login to the eG SuperManager at Chicago. To do so, type the URL: http://<IP of the SuperManager>:<Port number of the SuperManager>. If the SuperManager is SSL-enabled, then replace http with https. Figure 5.3 will then appear.

Figure 5.3: The SuperManager login

5.1 An egsm User's View

The default user to the Monitor interface of the eG SuperManager is *egsm* with password *egsm*. This user has unrestricted rights to the SuperManager, and can view alarms/status information pertaining to all the individual managers that are being managed by the eG SuperManager.

When you login to the SuperManager as *egsm*, you will be welcomed by the **current alarms** window (see Figure 5.4).

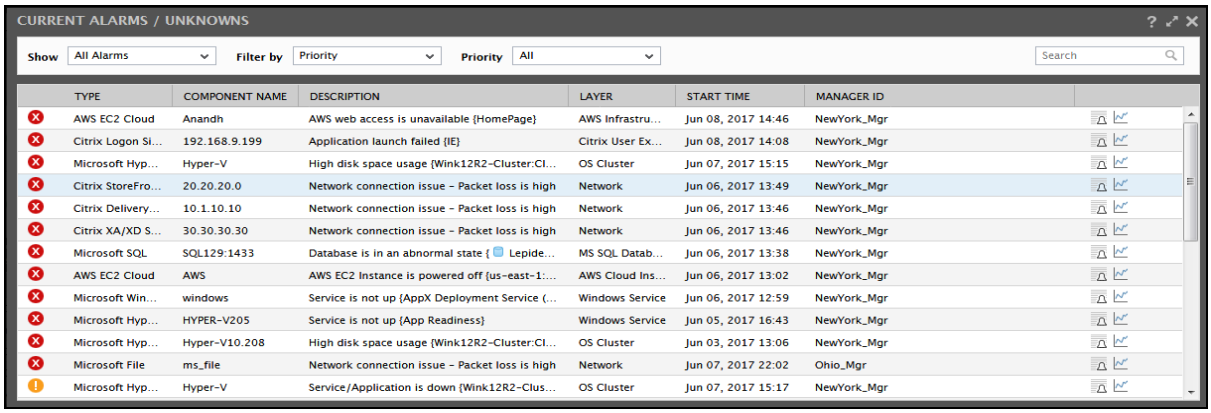


Figure 5.4: Consolidated list of alarms pertaining to the Ohio and New York managers

Figure 5.4 displays the consolidated list of issues encountered by both the New York and Ohio managers. The alarm details include the component type that has suffered performance degradation, the component name, a brief description of the issue, the problem layer, the problem

date and time, and the manager that reported the issue. For additional alarm information, simply click on the icon. Additional details such as the problem test and the service affected will appear as depicted by Figure 5.5 upon clicking the icon.

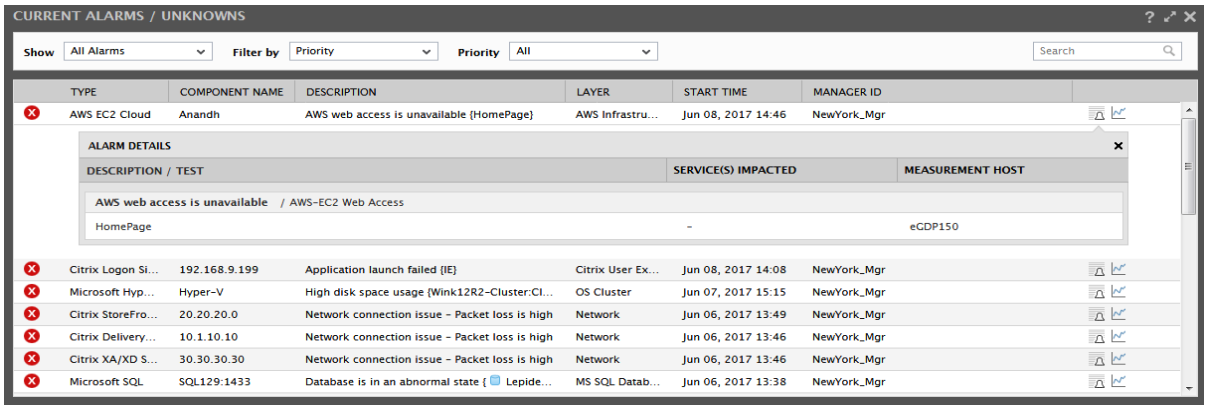


Figure 5.5: Additional alarm details

By default, the alarms displayed in the **CURRENT ALARMS** window are sorted in the descending order of the problem priority and problem date/time. This is why the **Filter by** list in Figure 5.5 is set to **Priority** by default. Typically, the alarms can be sorted in the ascending order of any of the following options – i.e., **Component Type**, **Component Name**, **Description**, **Layer**, or **Start Time**.

Also, though the **CURRENT ALARMS** window displays all the unresolved issues across managers by default, you can choose to view a specific priority of alarms alone by selecting the alarm priority of interest to you from the **Priority** list. The default selection in the **Priority** list is **All**. To view only the critical alarms, select the **Critical** option from the list. Figure 5.6 will then appear.

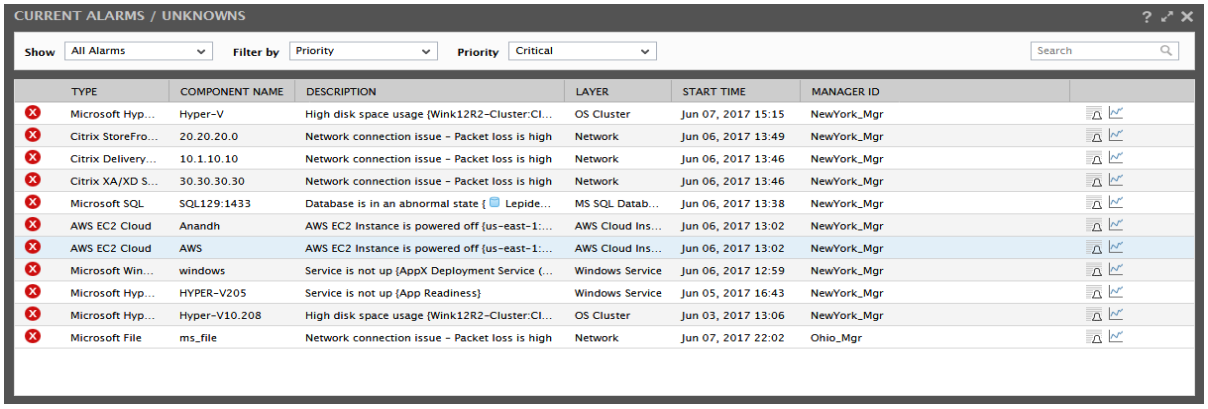


Figure 5.6: Viewing the Critical alarms alone

Likewise, you can choose to view **Critical & Major** alarms, **Major** alarms alone, or simply the **Minor** alarms.

Note:

The *egsm* user does not have either the rights to delete alarms nor possess alarm acknowledgement privileges.

If no alarms exist in the entire infrastructure, then the Monitor Home page is the first page that will be displayed in the monitor interface.

Besides open issues, you can also use the **CURRENT ALARMS** window to view the tests that are currently in an **UNKNOWN** state in the environment. A test can switch to an UNKNOWN state when the eG Enterprise system is unable to determine the state of one/more metrics that test reports - this could be because of any of the following reasons:

- The test could have been wrongly configured;
- The eG agent executing the test could have suddenly stopped;
- The eG agent may have been unable to pull out metrics from the server;
- The eG agent executing the test may not be able to transmit the metrics collected by that test to the eG manager, owing to say, poor network connectivity;

To enable administrators to receive a heads-up on the *Unknown* tests in the environment, so that issues such as the ones mentioned above can be isolated and resolved, the **Show** list in the left top corner of the **CURRENT ALARMS** window includes a special *Unknowns* option.

Selecting the *Unknowns* option from the **Show** list invokes Figure 5.7, where the **TEST**s in an indeterminate (i.e., **UNKNOWN**) state, the layers to which the tests are mapped, the names of the components they are associated with, and their corresponding component types will be listed.

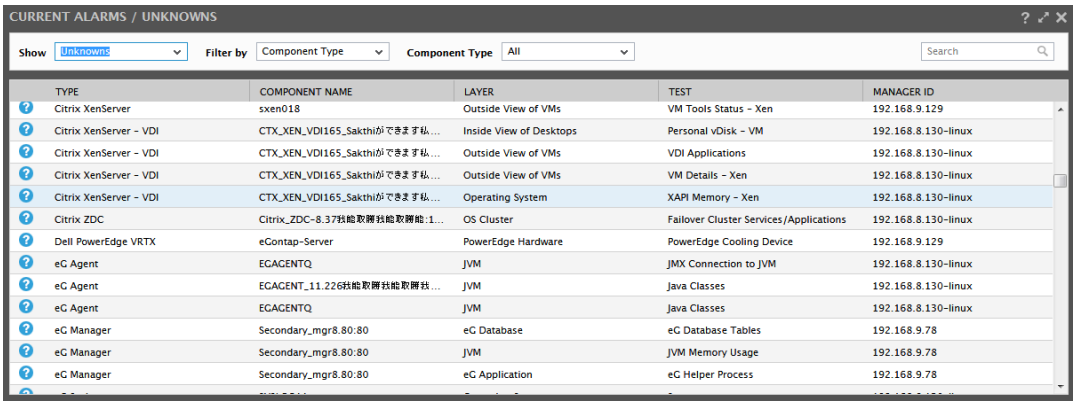


Figure 5.7: The components, tests, and metrics in an Unknown state

5.2 The Monitor Home Page

Behind the **CURRENT ALARMS** window is the monitor home page (see Figure 5.8). If no alarms exist in the environment, then this is the first page that will be displayed in the monitor interface for the egsm user.

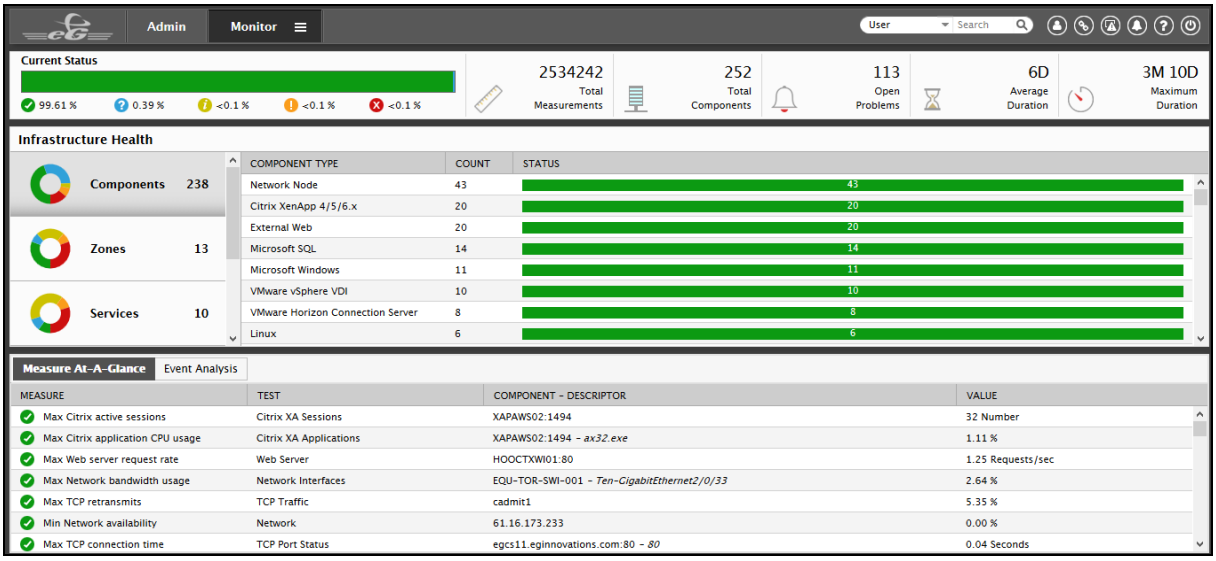


Figure 5.8: The Monitor Home page

This page quickly updates the egsm user with the overall health of his/her monitored environment. The page reveals the following information:

- The first section is the **Current Status** section that reveals at a glance, the status of the measurements reported to all the eG managers reproting to the eG SuperManager. Besides displaying the total number of monitored components and the number of performance metrics collected by the eG agents from these components, this section also reveals the percentage of total measurements that are in the critical, major, minor, normal, and unknown states. Using this information, an accurate assessment of the overall infrastructure performance can be made. Clicking on any of the states will take you to the **Current Alarms** window, where you can view all open alarms of the corresponding priority.
- Below the **Current Status** section, is the section that reveals the **Infrastructure Health**. Since the health of an infrastructure depends entirely upon the performance of each of its key ingredients - namely, the Components, Zones, Services, Service Groups and Segments - this section takes the help of a doughnut graph to clearly indicate the number of zones, services, service groups, segments, and components that are in the Critical, Major, Minor, Normal, and/or Unknown states. Clicking on a doughnut graph will reveal the complete list of

components/services/segments/zones/Aggregate Components in the section right to it in a context sensitive manner.

- Below the **Infrastructure Health** section you will find a **Measures At-A-Glance** section that provides the min/max values of critical measurements updated in real-time.

  Using the information provided by the **Measures At-A-Glance** section, the egsm user can receive instant status updates on sensitive performance parameters, and can also accurately determine, at a glance, the component on which the parameter is currently experiencing issues (if any), thereby simplifying problem identification.

  The **Event Analysis** tab page, when clicked, lists the top-5 layers that were most affected by performance issues.

  Corresponding to every layer name in the **Event Analysis** section, you will see the number of alarms that are currently open for that layer, the average duration of the open alarms, and the maximum duration for which an alarm had remained open.

- The menu at the top of this page permits monitor users to view the status of the monitored elements such as **Zones**, **Services**, **Segments**, and individual **Components** (see Figure 5.9).

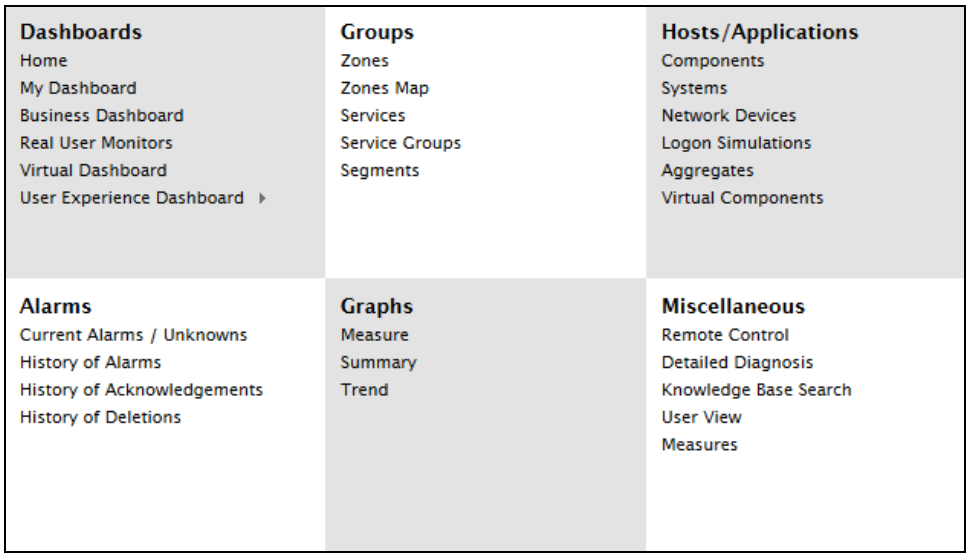


Figure 5.9: The Monitor menu

In addition to this, the menu also facilitates the following:

  - Switching to the monitor **Home** page from anywhere in the monitor interface
  - Browsing for any measure across the environment and focusing on its current status

- The viewing of the current alarms, and the complete alarm history
- The generation of a wide variety of graphs including, measure, summary, and trend graphs
- The viewing of detailed diagnostic measures and the execution of remote control on agent hosts

Note:

The detailed diagnosis and remote control capabilities will be available only if the license permits them.

To know more about the monitor home page, refer to The Monitor Home Page section of the *Monitoring Using eG Enterprise* document.

5.3 Time Zone Handling of the eG SuperManager Console

By default, the SuperManager time zone is displayed in the eG monitoring console of the SuperManager. The same time zone applies to metrics displayed and alarm generation from across all the eG managers. When a user logs into the SuperManager he/she would view the metrics and alarms in the time zone of the SuperManager. If the managers reporting to the SuperManager operate in a different time zone, then the metrics displayed in the eG managers and the SuperManager will be the same but the time zone will be that of the SuperManager.

Note that the SuperManager time zone applies to the users who have been assigned a different time zone in their respective eG managers.

5.4 Acknowledgement History

eG Enterprise stores and displays all the acknowledgement descriptions that are associated with a particular alarm, so that the help desk staff can consult with each other online, exchange views, and thus arrive at effective solutions to persistent performance issues with target components. The eG monitoring interface presents this acknowledgement history to you in various ways. While the **CURRENT ALARMS** window provides you with the complete acknowledgement history of a current issue, the **EVENT HISTORY** page leads you to all acknowledgements associated with a problem that occurred in the recent/distant past.

Sometimes however, to perform better problem diagnosis, you might want to review specific acknowledgment descriptions associated with an alarm and not all of them. For instance, while two users - *john* and *elvis* - may have acknowledged an alarm raised on an Oracle database server, you might only want to view user *john's* acknowledgement description. To facilitate such selective viewing of acknowledgement information, eG Enterprise provides a dedicated **ACKNOWLEDGEMENT HISTORY** page; this page provides a wide variety of filter options with the

help of which you can quickly and easily run a search across all alarm acknowledgements, and swiftly locate the acknowledgment information of interest to you.

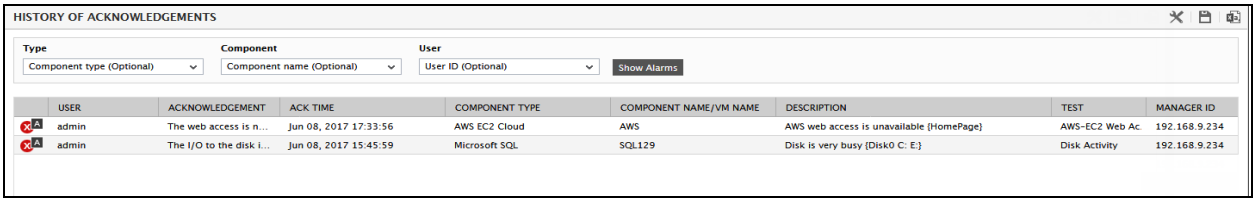


Figure 5.10: Viewing the history of alarm acknowledgements in the ACKNOWLEDGEMENT HISTORY page

To know more on how to access the **ACKNOWLEDGEMENT HISTORY** page and the options provided in that page, refer to the Acknowledgement History of the *Monitoring Using eG Enterprise* document.

5.5 Deletion History

Typically, in large, multi-user environments, multiple users may be granted the privilege to monitor a single component. In such environments, any of these users can delete an alarm raised on that component without the knowledge of the others, thereby causing confusion. To avoid this confusion, eG Enterprise provides users with the ability to track the deleted alarms. This may also be useful to an egsm user who needs to know which user deleted a particular alarm and at what time was the alarm deleted.

The **HISTORY OF ALARMS** page for instance has been embedded with the intelligence to indicate whether a past alarm was deleted or not. Sometimes, you might want to view the details of all alarms that were deleted by a particular user. Similarly, you might want to view only the details of those alarms that were deleted during the last 24 hours. Since the **HISTORY OF ALARMS** page allows you to search based on general alarm information alone and not on deleted alarms, this page cannot be used for performing the search operations mentioned above.

To zoom into the details of specific deleted alarms therefore, eG Enterprise offers a dedicated **DELETION HISTORY** page (see Figure 5.11). This page provides a variety of filter options using which you can quickly access the alarm deletion details that you may require.

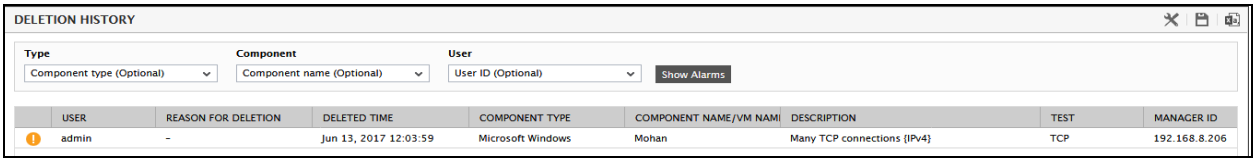


Figure 5.11: The DELETION HISTORY page

To know more about this page, refer to *Deletion History* section of the Monitoring Using eG Enterprise document.

5.6 The View Received by Other Users

Besides the default user *egsm*, the eG SuperManager supports all other users registered with each of the individual managers reporting to it. The access rights defined for them in their respective managers will automatically apply. Accordingly, the alarms displayed in this page are specific to the services/segments/components/zones being monitored by the current user. For instance, when a user who is assigned the AlarmViewer role logs into the SuperManager interface, he/she will receive a home page that only lists the alarms pertaining to those infrastructure elements that are associated with that user (see Figure 5.12).

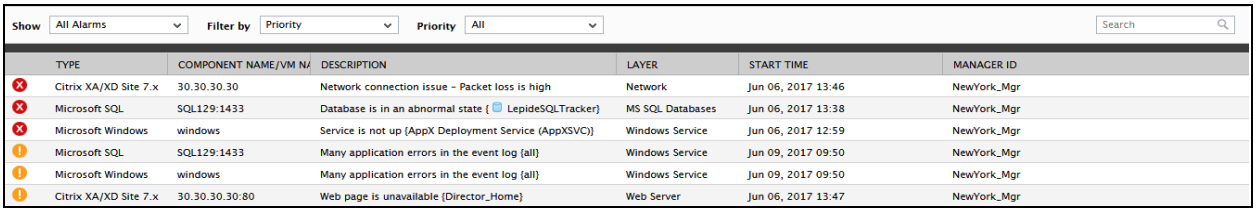


Figure 5.12: The AlarmViewer role

Moving your mouse pointer over an alarm will reveal additional alarm details along with the following options (see Figure 5.13):

- An option to view the history of fixes to the issue indicated by the alarm
- An option to add more fixes

Figure 5.13: The details of an alarm of an AlarmViewer along with Feedback and History options

In case of a *SuperAlarmViewer*, the only difference is that the list of alarms displayed in the home page will pertain to the monitored environment as a whole.

Also, if a particular user has been configured to view only a specific priority of alarms then this window will display alarms pertaining to that priority only.

Moreover, if the same user name and password are registered with multiple managers, then the eG SuperManager alarms window will display all the alarms pertaining to that user across all the managers to which he/she has access. For example, consider the case of user john who has been

created both in manager Newyork and manager Ohio, with Monitor user privileges. Some critical components of the infrastrucutre have been assigned to the user john registered with the New York manager and the Ohio manager. However, if the passwords of both the johns were the same, then the resulting **CURRENT ALARMS** window will list alarms pertaining to all the components assigned to the user across the infrastructure (see Figure 5.14).

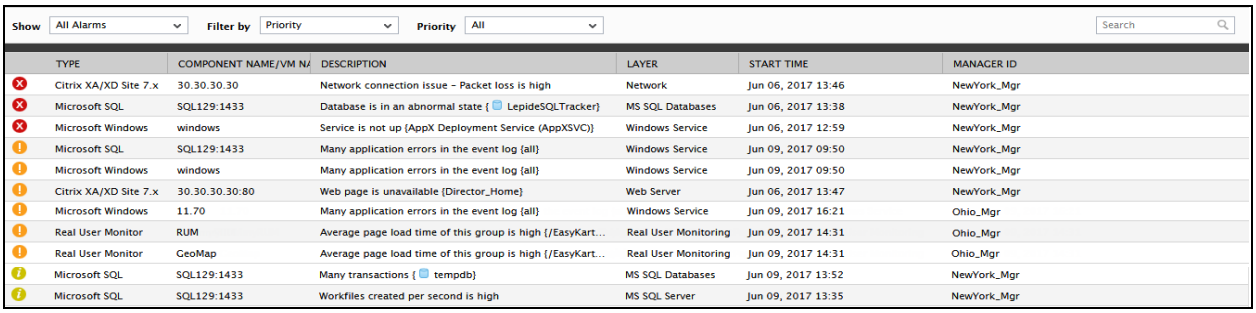


Figure 5.14: Alarms pertaining to both the 'johns'

Now, assume that a user named *repo* (password: *repo*) with 'Reporter-only' rights has been configured in both the NewYork and Ohio managers. When this user tries to log into the eG SuperManager interface, the login will not be validated and an warning message will appear (see Figure 5.15). This is because the reporter-only rights user will not have permission either to view the eG SuperManager admin interface or the eG SuperManager monitor interface.

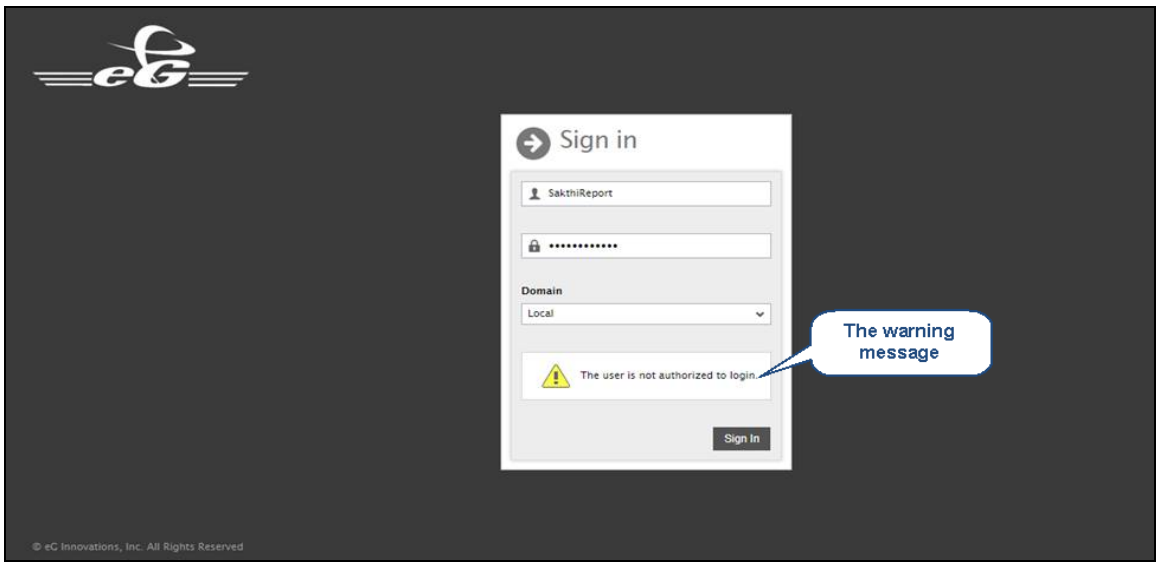


Figure 5.15: The pop up window stating that the reporter only user cannot access the eG SuperManager

If a component is managed with the same nick name by both the Ohio and NewYork managers, then, in the event of a problem with both the components, the component will appear twice in the **CURRENT ALARMS** window of the SuperManager interface. (see Figure 5.16)

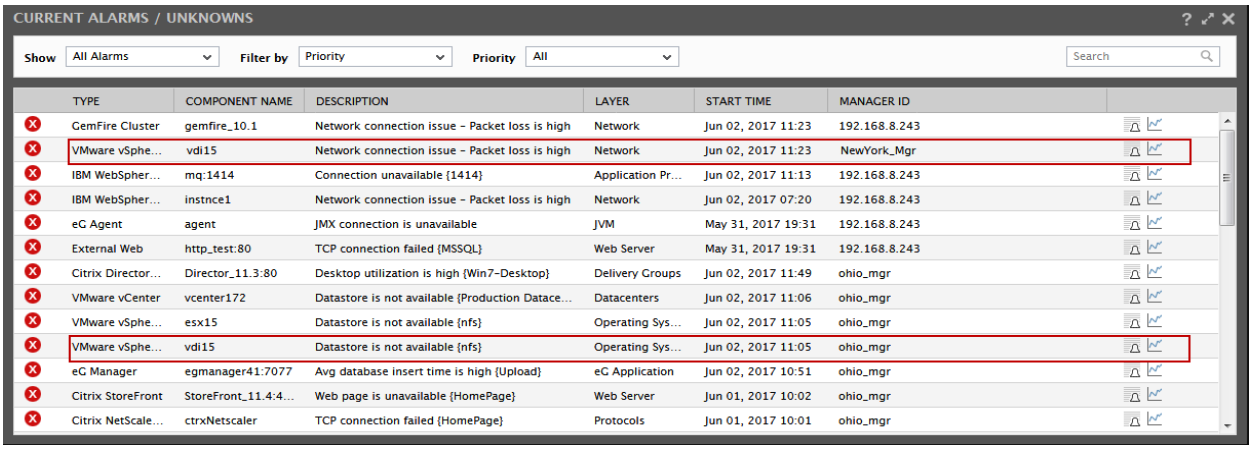


Figure 5.16: The component with the same nick name in both Ohio and New York managers

Note:

In order to avoid duplications, it is recommended that you develop standard naming conventions that would be applicable to the users/roles/components across all the managers in your environment.

If a user who has been assigned the *AlarmViewer* or the *SuperAlarmViewer* role logs into the eG SuperManager interface, then he/she will only be able to view the **CURRENT ALARMS** window only and not the home page.

5.7 Monitoring Components

To view the status of components that are managed by all the eG managers reporting to the eG SuperManager, select the **Components** option from the **Hosts/Applications** tile in the eG monitor interface. By default, the page that appears displays all the managed components across the environment, regardless of whether or not they are part of a segment, service or zone.

In this section, we will discuss the following topics:

- Monitoring Server Components
- Monitoring Virtual Components
- Monitoring Aggregate Components

5.7.1 Monitoring Components

To view the status of the components managed in your infrastructure, select the **Components** option from the **Hosts/Applications** menu in the eG monitor interface. By default, the page that appears lists the key performance metrics of a component that is managed in your infrastructure.

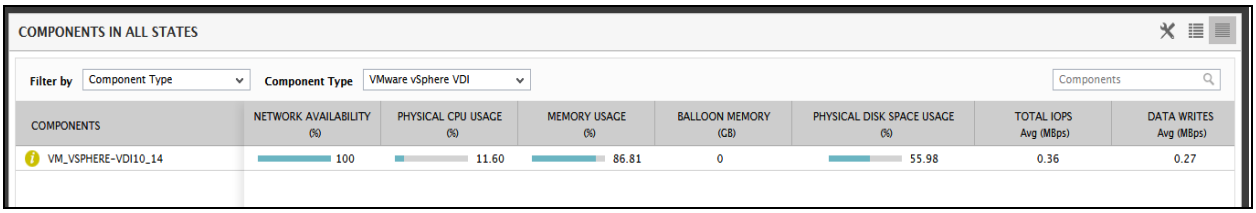


Figure 5.17: The COMPONENTS page displaying the key performance metrics

By default, the **Component Type** option is chosen from the **Filter by** list. If the zones/services/segments are created by the user who is accessing the eG monitor interface, then the components that are part of the zone/segment/service can be filtered using this list. The **Component Type** list box by default, lists all the components managed in the target infrastructure. When the **COMPONENTS** page is accessed for the very first time, the key performance metrics of the component type that comes first in the alphabetical order will be displayed against each component. Clicking on a component will lead you to the layer model page which displays the tests associated with the component and the measures corresponding to each test.

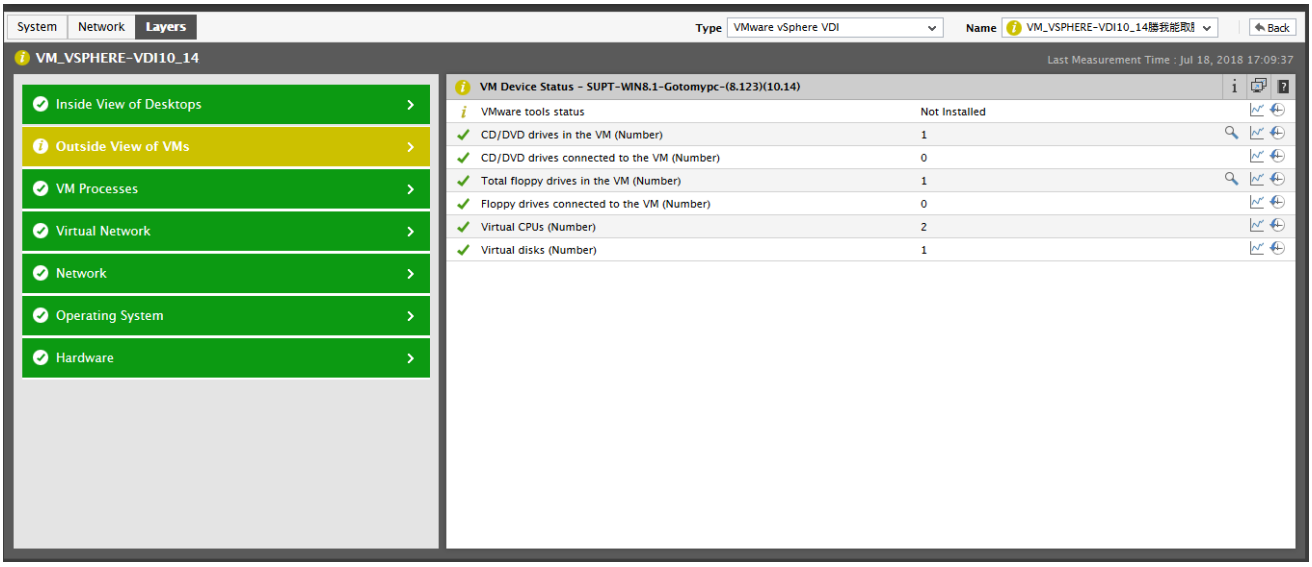


Figure 5.18: The layer model page

If the egsm user wants to know the manager on which the component is managed, he/she can click on the name of the component. Figure 5.19 then appears listing the URL of the manager on which the component is managed.

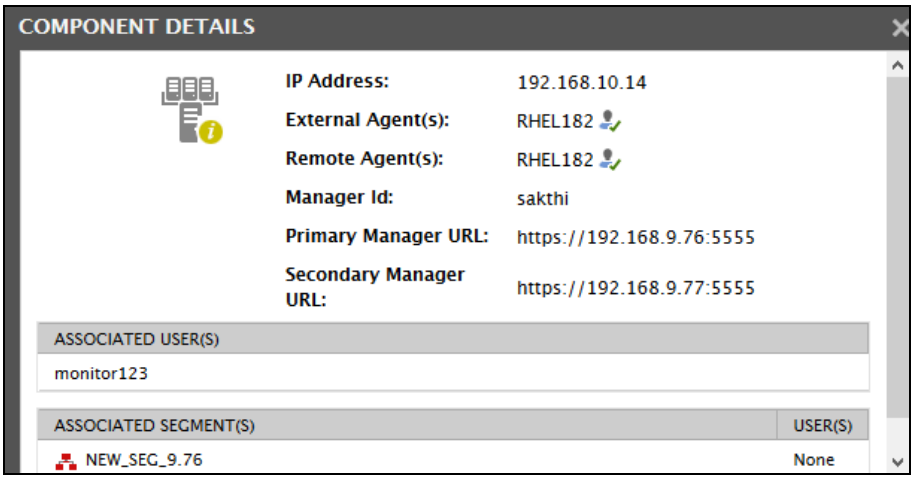


Figure 5.19: The URL of the manager on which the chosen component is managed

If the manager on which the component is managed is part of a redundant setup, then both the **Primary Manager URL** and the **Secondary Manager URL** will be displayed. Note that clicking on the URL will lead you to the login page of the manager on which the component is managed.

Note:

- If a maintenance policy is applied to a component by an administrator in an individual eG manager, then, the state of the component will automatically be reflected as *Normal* in the eG SuperManager while the details of the maintenance policy applied on the component cannot be viewed from the eG SuperManager monitor console.
- If a virtual server is monitored in one of the eG managers managed by the eG SuperManager, then, the virtual topology of that server cannot be viewed when you navigate from the layer model page of that server in the eG SuperManager monitor console.

To know more about the **COMPONENTS** page, refer to the *Monitoring Components* section of the *Monitoring Using eG Enterprise* document.

5.7.2 Monitoring System Components

While eG Enterprise focuses primarily on monitoring applications, many administrators still prefer to view their infrastructure from a hardware perspective - i.e., as systems they support. The eG monitoring console of individual eG managers provide a “system view”, which represents the overall health of systems in the target infrastructure, with a mapping of the applications that are executing on these systems. The same "system view" can now be viewed by the users logging into the eG monitor interface of the eG SuperManager.

To access the **SYSTEMS** page that provides the 'system view', click on the ☰ icon available in the **Monitor** tab. Then, select the **Systems** option from the **Hosts/Applications** tile.

The **SYSTEMS** page that appears, indicates the current state of those systems/hosts that have been assigned to the current user for monitoring along with the key performance metrics of each system/host.

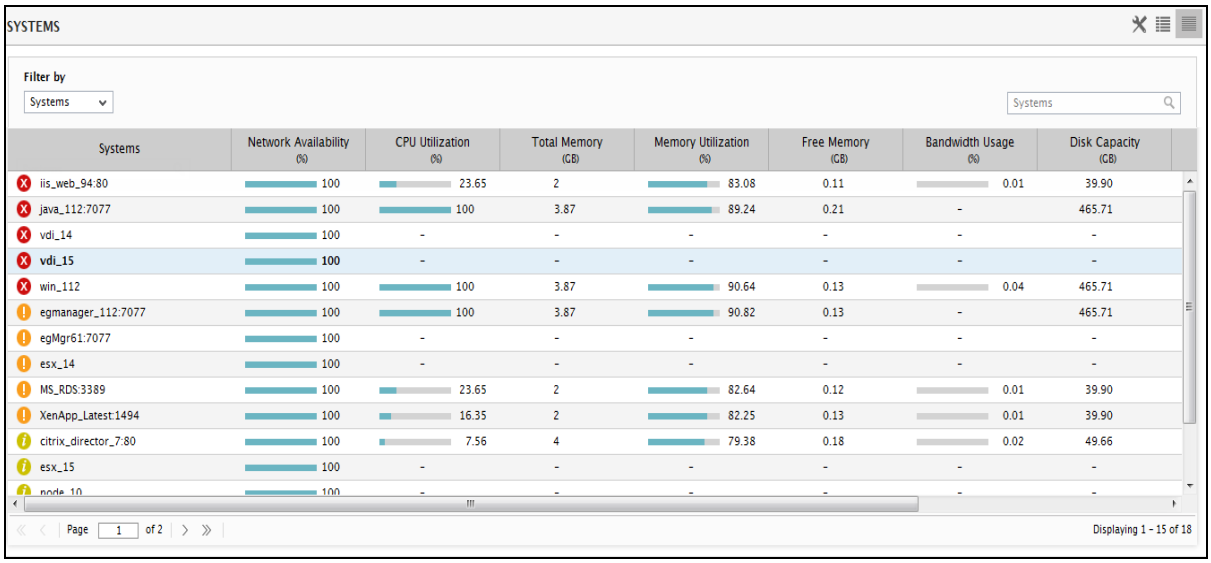


Figure 5.20: Viewing a host-wise list of system components and their state

To know more about Monitoring the System Components, refer to *Monitoring System Components* of the *Monitoring Using eG Enterprise Suite* document.

5.7.3 Monitoring Network Devices

If network devices have been configured for monitoring on any of the eG managers in your environment, then click on the ☰ icon available in the **Monitor** tab. Then, select the **Network Devices** option in the **Hosts/Applications** tile to view the current state of the Network devices managed by the eG Enterprise system (see Figure 5.21).

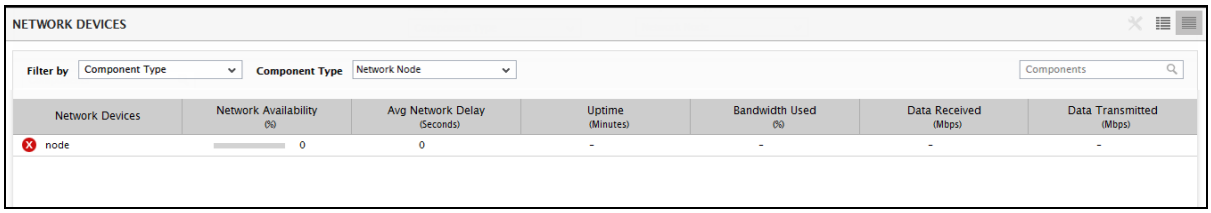


Figure 5.21: The Network Devices managed in your infrastructure

To know more about monitoring the Network Devices refer to the *Monitoring Network Devices* section of the *Monitoring Using eG Enterprise* document.

5.7.4 Monitoring Aggregate Components

eG Enterprise typically monitors every component of a type, separately. However, sometimes, administrators might want to receive an aggregated view of the performance of two/more components of a type. For instance, Citrix administrators might want to know the total number of users who are currently logged into all the Citrix servers in a farm, so that sudden spikes in the load on the farm (as a whole) can be accurately detected. Similarly, Windows administrators might want to figure out the average CPU usage across all the Windows servers in an environment, so that they can better plan the capacity of their Windows load-balancing clusters.

To provide such a consolidated view, eG Enterprise embeds a license-controlled **Metric Aggregation** capability. This feature, when enabled, allows administrators to group one or more components of a particular type and monitor the group as a single logical component, broadly termed as an aggregate component. The eG Enterprise system then automatically aggregates the metrics reported by the components in the group by applying pre-configured aggregate functions on them, and reports these metrics as if they were extracted from the managed *aggregate component*. Separate thresholds need to be set for the aggregated metrics to track deviations in the consolidated performance. The state of the *aggregate component* is governed by these exclusive thresholds, and not by the state of the components within the group.

The *egsm* user of the eG SuperManager can monitor all the aggregate components that are managed by the individual eG managers that are reporting to the SuperManager.

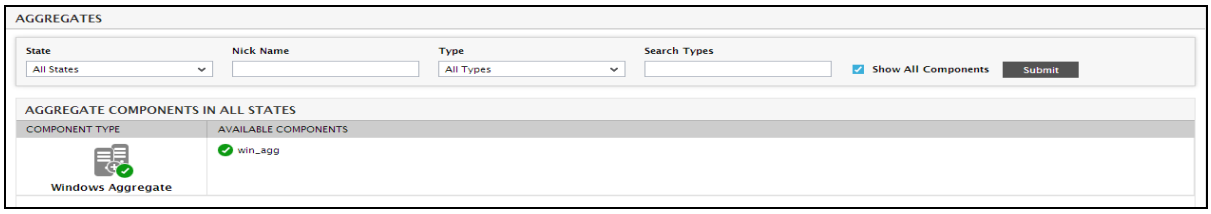


Figure 5.22: The AGGREGATES page in the eG SuperManager

To know more about monitoring the aggregate components in the overall infrastructure, refer to the *Monitoring Aggregate Components* section of the *Monitoring Using eG Enterprise* document.

5.7.5 Monitoring the Citrix Logon Simulations

For years, slow Citrix logons have been the most common complaint in Citrix infrastructures. For a Citrix user, slow logons can lead to frustration, lower productivity and efficiency. For a Citrix

administrator, Citrix logon slowness is a complex problem that takes a long time to resolve. There are dozens of steps involved in the Citrix logon process and they involve multiple components – Citrix StoreFront, Citrix Delivery Controller, Active Directory, Profile server, Citrix XenApp/XenDesktop, the Citrix data store and so on. Identifying exactly what is causing the slowdown is often time consuming and laborious.

To ensure great Citrix user experience, administrators need to monitor their infrastructure proactively and be alerted to issues in advance, before users notice and complain. In order to do so, administrators need a consistent measure of Citrix logon performance – one that is available 24x7, even when there are no users accessing the farm.

Collecting logon metrics of real user activity is challenging. Metrics have to collected from the different tiers involved. Even then, it is a difficult to get a consistent assessment of Citrix logon performance because different users have different profiles and policies associated with them. Furthermore, there will be times when no one is logging in to the Citrix farm, and at those times, it is important to know if Citrix logon is working and whether users can launch their applications and desktops successfully.

The eG Logon Simulator, a part of the eG Enterprise suite, is a purpose-built solution for delivering proactive visibility into the logon performance in Citrix infrastructures. Using an agentless approach, the eG Citrix Logon Simulator simulates a user logging in to a Citrix StoreFront or NetScaler gateway through a browser, reviewing the list of applications/desktops accessible, clicking on a selected application or desktop, launching it in Citrix Receiver by initiating a session and then logging off. By emulating the exact same process that users go through when they logon to Citrix XenApp or XenDesktop, the eG Citrix Logon Simulator provides a realistic measure of the user experience during Citrix logon. Since every simulation tests the entire Citrix delivery infrastructure (Citrix NetScaler, Citrix StoreFront, Citrix Delivery Controller, Citrix XenApp Server, VDI, etc.), the results represent the cumulative health of all of the tiers supporting Citrix logons.

Unlike traditional simulation tools that require recording of a script that captures the typical steps a user performs, the eG Citrix Logon Simulator requires no recording and hence, is simple to implement. Installed on any desktop that has a browser (Internet Explorer or Chrome) and Citrix Receiver configured, the simulator targets the configured Citrix logon URL and application/desktop 24x7 at pre-configured intervals and tests the Citrix logon availability and performance. When a problem is detected, the offending step is clearly highlighted, so administrators can start working on a resolution immediately.

The simulation can be configured to run from different remote locations, to understand the logon performance from each location. By testing the simulated session from different locations and at

different times, administrators can diagnose and resolve logon issues before users experience them and call up the helpdesk.

In complex citrix environments where the eG managers monitoring the Citrix Logon Simulations report to an eG SuperManager, the egsm user of the SuperManager has the exclusive rights to view all the Citrix logon simulations of that environment. This helps the egsm user to understand the underlying problems in that environment with ease and resolve those problems before users experience slowdowns.

Where multiple Citrix Logon Simulator components are managed, clicking on the *Citrix Logon Simulations* under the Hosts/Applications tile of the Monitor dashboard automatically opens the **Citrix Logon Simulation Dashboard**.

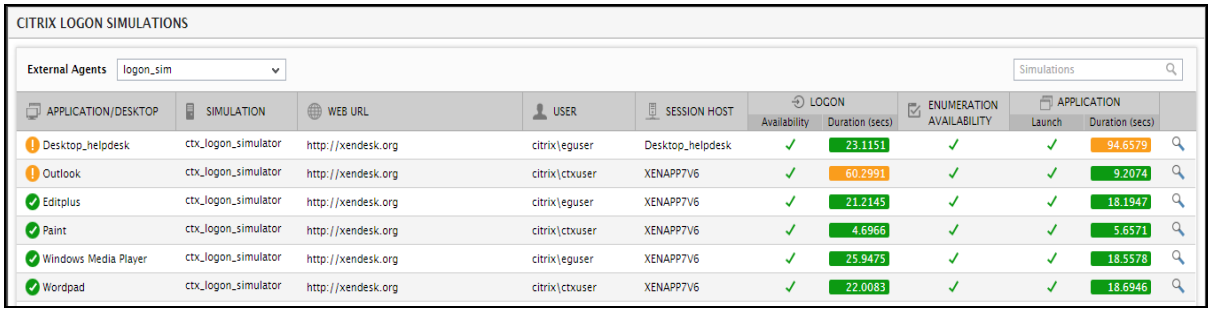


Figure 5.23: The Simulator Dashboard

To know more on the Citrix Logon Simulator dashboard, refer to the *Simulator Dashboard* section of *The eG Citrix Logon Simulator* document.

5.7.6 Monitoring Virtual Servers

If individual eG managers in your environment monitors virtualized components, then, the eG SuperManager is also capable of monitoring the virtualized components. To monitor the virtualized components, click the icon available in the **Monitor** tab. Then, select the **Virtual Components** option in the **Hosts/Applications** tile to view the current state of the VMware ESX hosts, Solaris virtual servers, XenServer hosts, Oracle virtual server hosts and Microsoft RDS server hosts that are managed by the eG Enterprise system (see Figure 5.24).

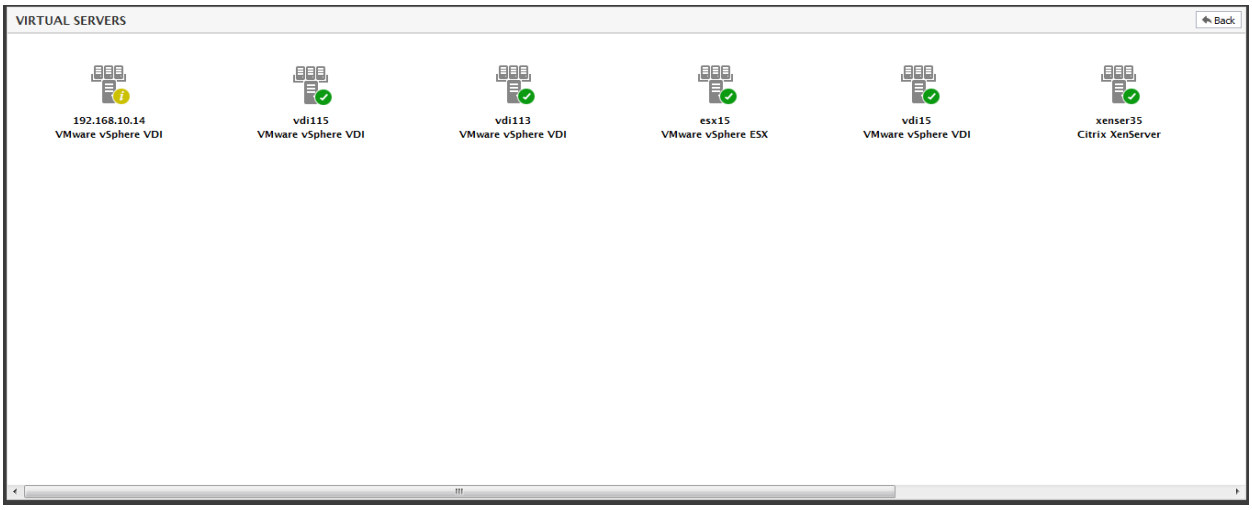


Figure 5.24: The state of virtual hosts

To know more on how to monitor the virtualized components, refer to *Monitoring Virtual Servers* section of the *Monitoring Using eG Enterprise Suite* document.

5.8 Monitoring Segments

eG Enterprise can also be used to monitor components that are not associated with services. For monitoring components that are a part of the component topology configured in each eG manager managed by the SuperManager, choose the **Segments** option shown in Figure 5.8.

This will result in the display of the different segments configured for the target infrastructure of all the managers managed by the eG SuperManager, and their respective states (see Figure 5.25). Each segment will be accompanied by the IP/hostname and state of the segment components associated with that segment.

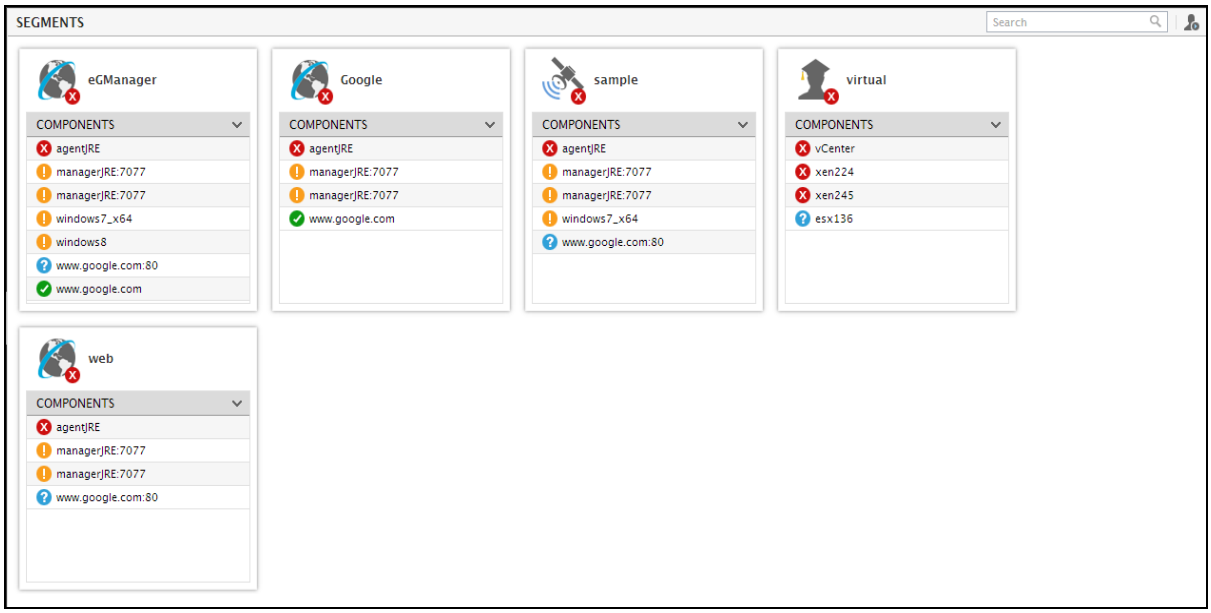


Figure 5.25: The Segments page

To know more on how to monitor the configured segments, refer to *Monitoring Segments* Chapter of the *Monitoring Using eG Enterprise* document.

5.9 Monitoring Services and Service Groups

5.9.1 Monitoring Services

A service is a collection of infrastructure components that work together to perform a specific set of functions – e.g., a mobile payment gateway service, an online banking service, a web site, etc. eG Enterprise allows administrators to add one/more services for monitoring. The procedure to configure such services using the eG administrative interface has been described in the *Administering the eG Enterprise* document.

Upon logging into the eG SuperManager monitor interface, click on the **Services** menu option from the **Groups** tile; this will lead you to the **SERVICES** page that lists the services that you are privileged to monitor and the current state of these services. Generally, all the services associated with the managers managed by the eG SuperManager will be listed in the **SERVICES** page (see Figure 5.26).

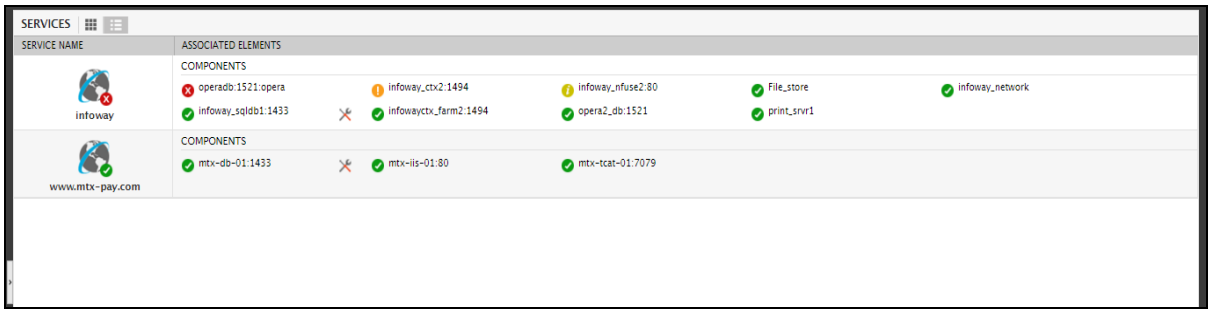


Figure 5.26: The Services page

To know more about how to navigate through the **SERVICES** page, refer to *Monitoring Services* chapter of the *Monitoring Using eG Enterprise* document.

5.9.2 Monitoring Service Groups

Once you are in the eG SuperManager monitoring interface, you will find that the **Infrastructure Health** section of the eG SuperManager monitoring console displays the number of configured service groups and the current state of these groups. Clicking on the **Service Group** label here will lead you to Figure 5.27, which lists all the service groups that are configured for the managers managed by the eG SuperManager and their current state. Against every service group, the services included in that group and the current state of each of the services will be available so that, you can instantly identify the services that are responsible for the abnormal state of the service group. Clicking on a service here will allow you to preview the topology of that service, using which you can identify the root-cause of the problems associated with that service.

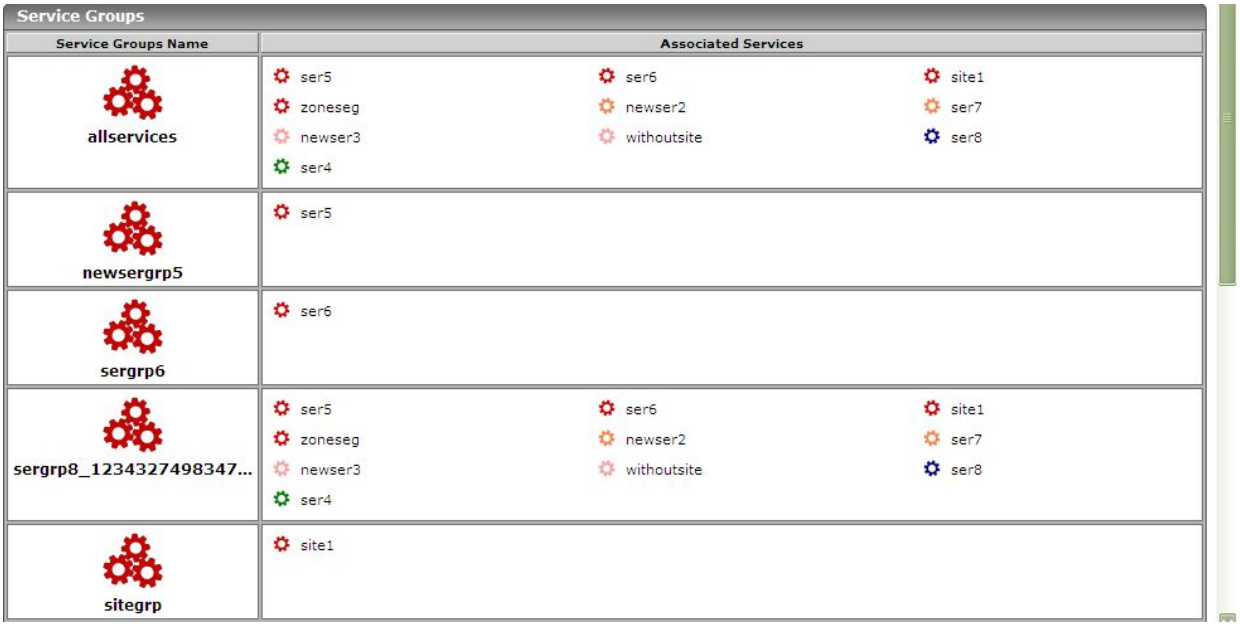


Figure 5.27: List of configured service groups and their current state

To know more about how to monitor the service groups, refer to *Monitoring Service Groups* section of the *Monitoring Using eG Enterprise* document.

5.10 Monitoring Zones using the eG SuperManager

Large infrastructures spanning geographies can pose quite a monitoring challenge owing to the number of components involved and their wide distribution. Administrators of such infrastructures might therefore prefer to monitor the infrastructure by viewing it as smaller, more manageable business units. In eG parlance, these business units are termed **ZONES**. A zone can typically comprise of individual components, segments, services, and/or other zones that require monitoring. For example, in the case of an infrastructure that is spread across the UK, USA, and Singapore, a zone named USA can be created consisting of all the components, segments, and services that are operating in the US branch alone. The USA zone can further contain an East-coast zone and a West-coast zone to represent infrastructure and services being supported on the two coasts of the US.

While a service/segment contains a group of inter-related components with inter-dependencies between them, a zone contains a group of components, services, segments, or zones that may/may not have inter-dependencies.

To quickly determine the state of the configured zones in each of the managers managed by the eG SuperManager, you can login to the eG SuperManager monitor interface and just click the **Zones** option under the **Groups** tile.

The **ZONES** page then appears listing the zones that have been configured for monitoring on all the managers managed by the eG SuperManager, along with their states.

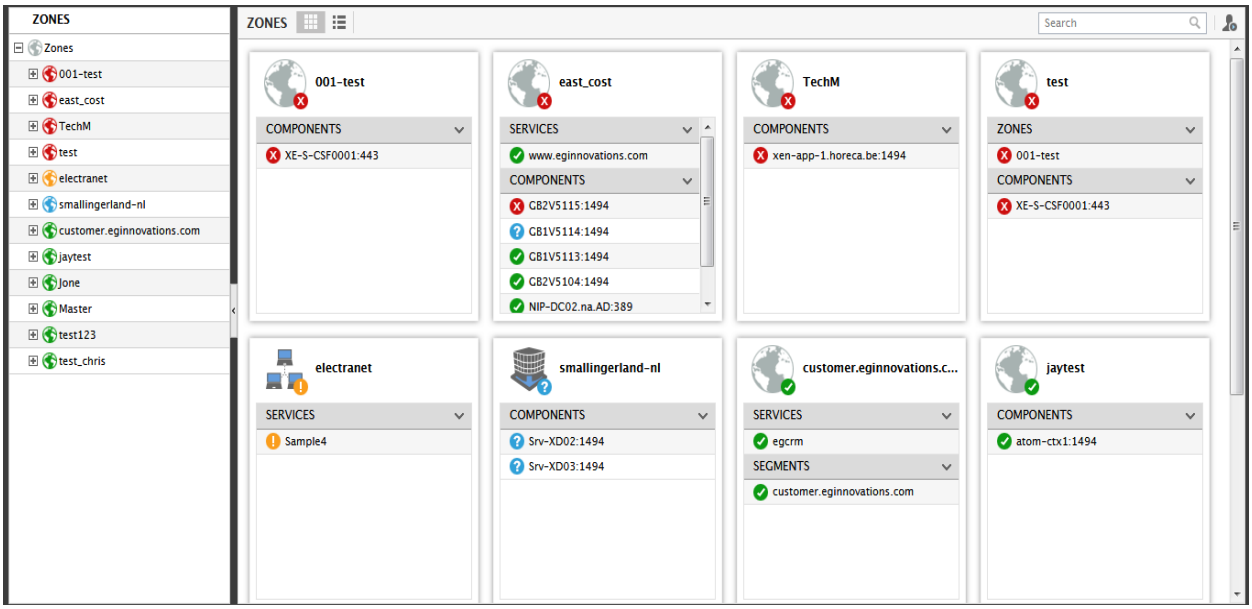


Figure 5.28: The state of all the zones being monitored

To know more about monitoring the individual zones, refer to *Monitoring Zones* of the *Monitoring Using eG Enterprise* document.

5.10.1 Zones Map

Typically, zones are associated with different geographies. While monitoring large infrastructures therefore, eG Enterprise allows you to drill down to view the exact geographic area where a zone operates, and instantly evaluate the performance of the different zones spread across the different locations worldwide. If multiple eG managers are reporting to an eG SuperManager, the *egsm* user may want to know the performance of all the zones that are managed in each of the managers. To access the map interface that provides this visual treat to the egsm user, select the **Zones Map** option from the **Groups** tile of Figure 5.9. This map interface provides a consolidated view of all the zones associated with each of the eG managers reporting to the eG SuperManager. Figure 5.29 then appears indicating the zone locations and their current state. The geographic display of the maps within the eG Enterprise console is achieved through the integration of the eG management console with Google maps.

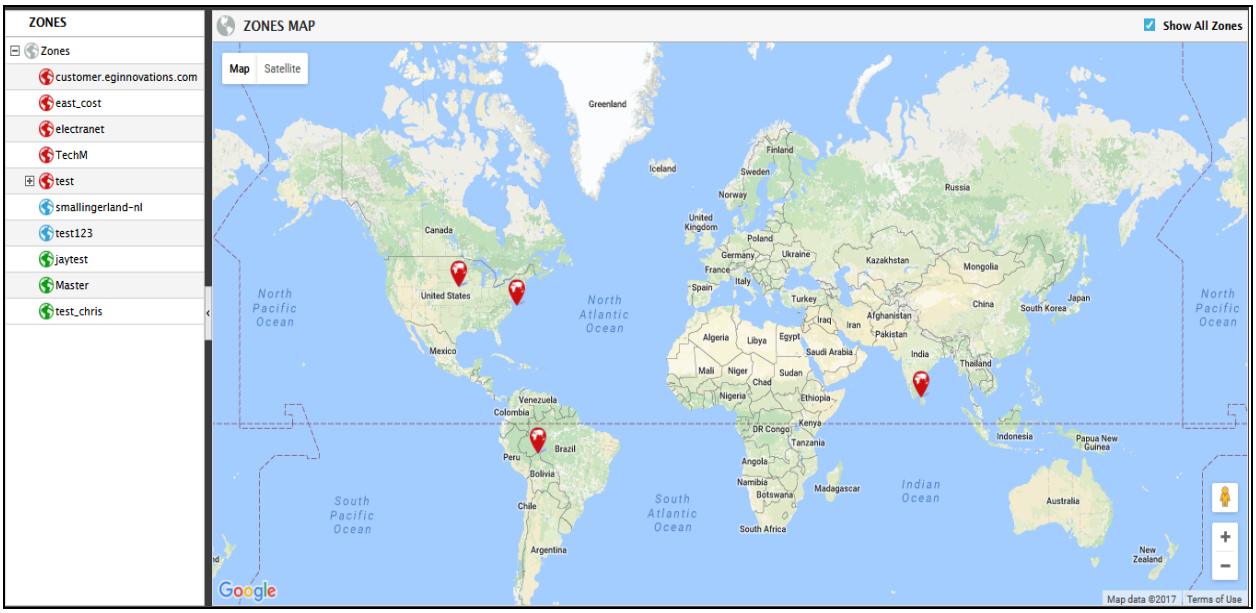


Figure 5.29: The map interface revealing the zone locations and state

Refer to the *Zone Maps* section of the *Monitoring Using eG Enterprise* document page to know more about the association of zones with different geographies.

5.11 Dashboards

eG Enterprise includes specialized dashboards for network, system, and application monitoring. In addition to the layer model, administrators can access key metrics at the network, system, and application layers directly from the dashboards. For example, in the system dashboard, administrators can view at a glance, the CPU utilization, memory utilization, disk usage, current system configuration, top CPU and memory consuming processes, and other key system metrics.

Thus, these dashboards:

- Serve as a single, central console that not only depict the current state of a layer, but also instantly indicate the root- cause of issues pertaining to that layer, thereby enabling administrators to go from problem effect to the problem source in no time!
- Combine both raw and graphically represented data, and facilitate an in-depth analysis of not just live performance, but also the historical performance of a particular layer, thus shedding light on potential anomalies;
- Aid administrators in effectively analyzing the past trends in the performance of a layer, so that they can easily forecast future performance;

- Enable service level audits on-the-fly, and thus help administrators accurately determine when a layer slipped from the desired performance levels.

While network and system dashboards are provided for all the supported application types, the application specific dashboards are available for selected applications only. Future releases of eG Enterprise will include dashboards for additional applications. While the network and system dashboards are similar for different applications, the contents of the application dashboards and their look and feel are different for different applications.

By default, the layer model representation of every application is accompanied by a **System Dashboard** and a **Network Dashboard**. In addition to these dashboards, a few selected applications are provided with an **Application Dashboard** as well.

When an egsm user logs into the eG monitor interface, he/she would be able to view the System, Network and Application Dashboards of all the components and analyze the problems in a more effective way!

To know more about the System dashboard, refer to *The System Dashboard* section of the *Monitoring Using eG Enterprise* document.

To know more about the Network dashboard, refer to *The Network Dashboard* of the *Monitoring Using eG Enterprise* document.

To know more about the Application Dashboard, refer to *The Application Dashboard* of the *Monitoring Using the eG Enterprise* document.

5.11.1 The Virtual Dashboard

Large virtualized environments are typically characterized by hundreds of virtual hosts, with tens of VMs configured on each host. In such environments, if a mission-critical application executing on a VM experiences a slowdown, the key challenge for the administrator is to determine what caused the slowdown - is it because the VM is under-sized? is it owing to a resource contention at the virtual host level? Is it because of other resource-hungry VMs? or is it owing to resource-intensive processes spawned by the target application itself? Also, as VM migration would be rampant in such environments, administrators are required to know when, why, and to which virtual host a VM was migrated, and even assess the impact of such a shift on the source and the destination hosts.

eG Enterprise provides dedicated monitoring models for a variety of virtualization platforms to enable administrators to address the performance concerns cited above. By analyzing the resource usage of VMs from inside and outside, and using an intelligent correlation engine to differentiate problem symptoms from sources, these models accurately point to the root-cause of slowdowns

experienced by a virtual application. In addition, these models are also capable of tracking the movement of VMs from one host to another and alerting administrators to the same. However, the key limitation of these models is that the aforesaid capabilities are 'hidden' inside the layers, tests, and measures offered by the models. To bring these capabilities to light, administrators would have to invest a considerable amount of time and mouse clicks!

A quicker, 'single glance' alternative to this is the **Virtual Dashboard**. The Virtual Dashboard provides administrators of virtualized environments the wherewithal to accurately diagnose the cause for slowdowns experienced by a virtual application, with minimal effort and time! This dashboard collates critical resource usage data from the host operating system and from 'inside' and 'outside' all the VMs on a virtual server, presents them in graphical and tabulated formats in a single interface in the eG monitoring console, and thus aids instant and effective performance analysis. In the event of a problem situation therefore, administrators can use the **Virtual Dashboard** to rapidly find answers to the following questions:

- Is the host experiencing a resource crunch? If so, which resource is being drained - CPU/memory/disk? Which processes executing on the host could be causing the resource bottleneck?
- How are the VMs using the physical resources of the host? Is any VM consuming resources excessively? If so, which VM is it?
- Were sufficient resources allocated to the VMs? How are the VMs using the resources allocated to them?
- Are resource-intensive processes executing on any VM? If so, which VM is being impacted, and what are the rogue processes?
- Did any VM migrate during the last hour (by default)? If so, which VM is it? Which server was it migrated to? How is the VM handling the physical and allocated resources in the destination host?

In addition to current problems, the dashboard also sheds light on the probable causes for issues that occurred in the past, thus paving the way for effective post-mortem analysis.

In virtualized environments where multiple administrators monitor the VMs using different eG managers, some key issues may not be addressed immediately since all the administrators may not be aware of the underlying issues reported by all the eG managers. It is therefore necessary to configure all such eG managers to an eG SuperManager. When all such eG managers are configured, the egsm user of the eG SuperManager has a holistic view of all the VMs that are available for monitoring by the individual eG managers. This helps the egsm user to instantly identify the problematic VMs and the root-cause of the problems.

To view the virtual dashboard,click the **Virtual Dashboard** from the **Dashboards** tile of the eG monitor interface.

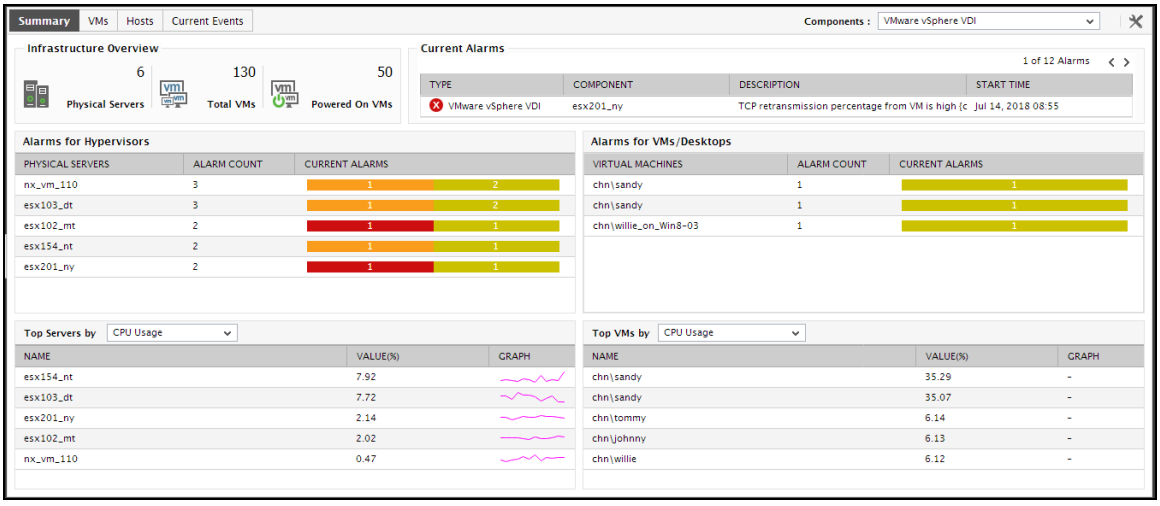


Figure 5.30: The Virtual Dashboard

Note:

- The egsm user has "read-only" access to the virtual dashboard.
- A user with administrator privileges can add, read and modify the virtual dashboard.

To know more about the virtual dashboard, refer to *Virtual Dashboard* section of the *Monitoring Using eG Enterprise* document.

5.11.2 Business Dashboard

The administrator of the eG SuperManager (the default egsm user) often require a high-level view of the performance of the mission-critical business services in their infrastructure. This may comprise of all the business services on all the eG managers reporting to the eG SuperManager. The **Business Dashboard** provides this view in a form that is easy to comprehend and analyze. This dashboard quickly compares service demand with resource consumption and service quality to enable the administrator of the SuperManager to swiftly determine where service performance is most likely bottlenecked – at the demand level? resource consumption level? or user experience level? Moreover, it allows administrators to rapidly triage performance issues tier-wise, so that they can accurately isolate the tier where the problem originated.

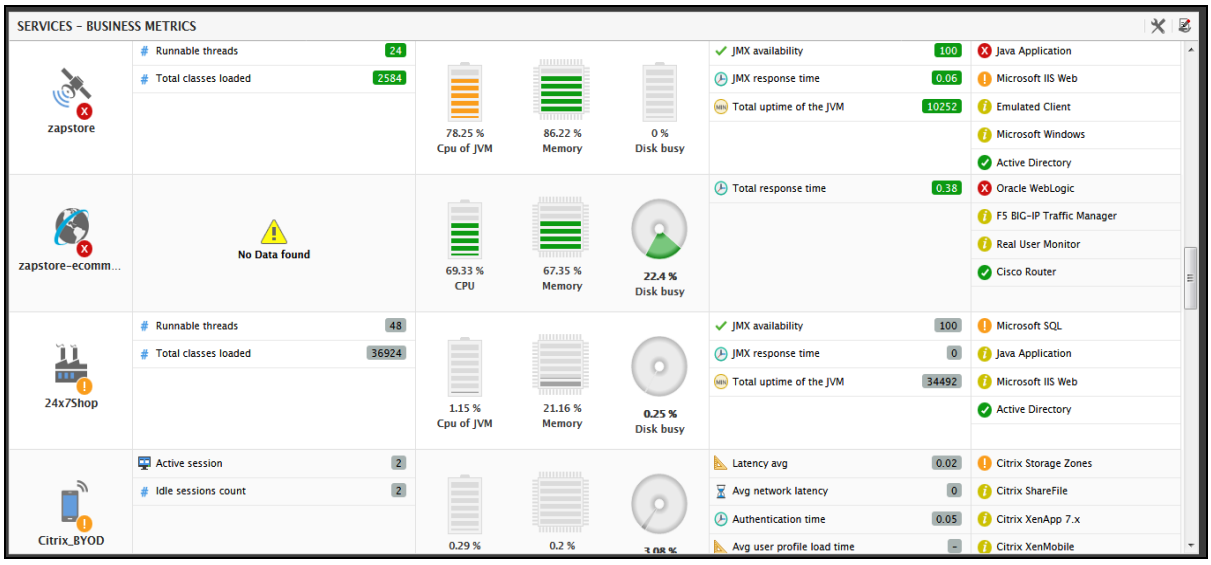


Figure 5.31: The Business Dashboard

You can customize the Business Dashboard to include demand, consumption, and quality indicators of your choice. To know more on how to customize the Business Dashboard, refer to *Business Dashboard* section of the *Monitoring using eG Enterprise* document.

5.12 My Dashboard

With eG Enterprise, the egsm user has the option to build a custom dashboard, using which he/she can graphically compare current and historical performance of multiple applications of his/her interest. This dashboard not only allows the egsm user to choose the components to focus on, but also pick the measures and even descriptors that should be featured in it. To build an application-independent custom dashboard, click on the icon available in the **Monitor** tab and then select the **My Dashboard** option from the **Dashboards** tile.

Note:

- The dashboard created by the *egsm* user cannot be viewed / modified / deleted by any other user.
- The dashboard created by the *egsm* user cannot be shared with other users.

To know how to add a My Dashboard, view the list of dashboards, refer to *Application-Independent My Dashboard* of the *Monitoring Using eG Enterprise* document.

Further, if you want to know on how to design a My Dashboard, refer to *Designing a My Dashboard* of the *Monitoring Using eG Enterprise* document.

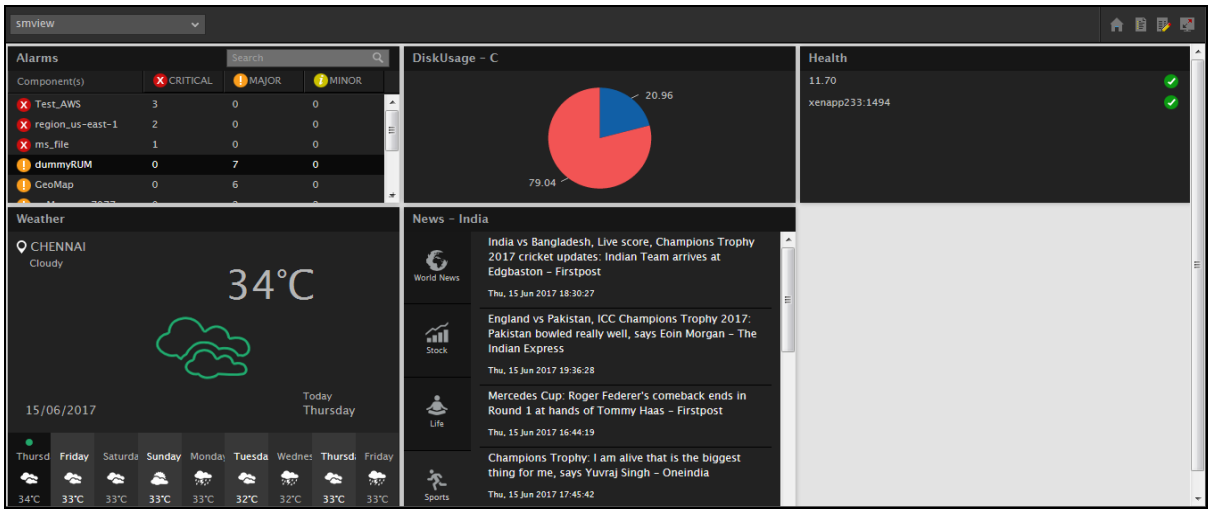


Figure 5.32: A My Dashboard created by the egsm user

5.12.1 Real User Monitors

The Real User Monitoring is a passive monitoring technology that records all real (not emulated) user transactions to a website or web application. In the process, response time metrics are collected for every transaction of each user in real-time. When there is no load, response time will not be captured! This way, the Real User Monitor captures the true user experience with a web site/web application.

eG's Real User Monitor tracks LIVE, the transactions of real users (not emulated) to web sites/web applications, and measures the response time of each transaction – i.e., page view - in real-time. In the process, the eG Real User Monitor promptly alerts administrators to slow page views, and isolates the exact tier where user experience was bottlenecked – was it at the front end tier? backend tier? Or the network tier?

When an *egsm* user logs into the SuperManager, he/she has a holistic view of all the real user monitors that are monitored by individual eG managers reproting to the SuperManager. This helps the *egsm* user to pinpoint where exactly the problem lies and take remedial actions.

With the help of a bevy of visual tools – e.g., intuitive icons, color-coded values, miniature graphs, geo maps, etc. - this real-time dashboard helps administrators understand, from just a glance, the following:

- How is the traffic to the managed web sites/web applications in your environment? Is the traffic to any web site/web application suspiciously high or low?

- From which devices is this traffic coming from – desktops? Mobile phones? Or tablets? Which is the most popular device?
- Is the user experience with any managed web service poor presently? If so, what is causing service quality to degrade – delay in page loading? Or JavaScript errors?
- How many distinct users are currently connected to each web site / web application being monitored/ - this is a good indicator of the number of users who are truly contributing to the traffic on the web site.

This way, the dashboard facilitates the rapid identification of web sites/web applications in the overall environment that do not enjoy user confidence and the probable reasons for this unfavorable user perception.

To know more about the Real User Monitor dashboard, refer to *The Real User Monitor* document.

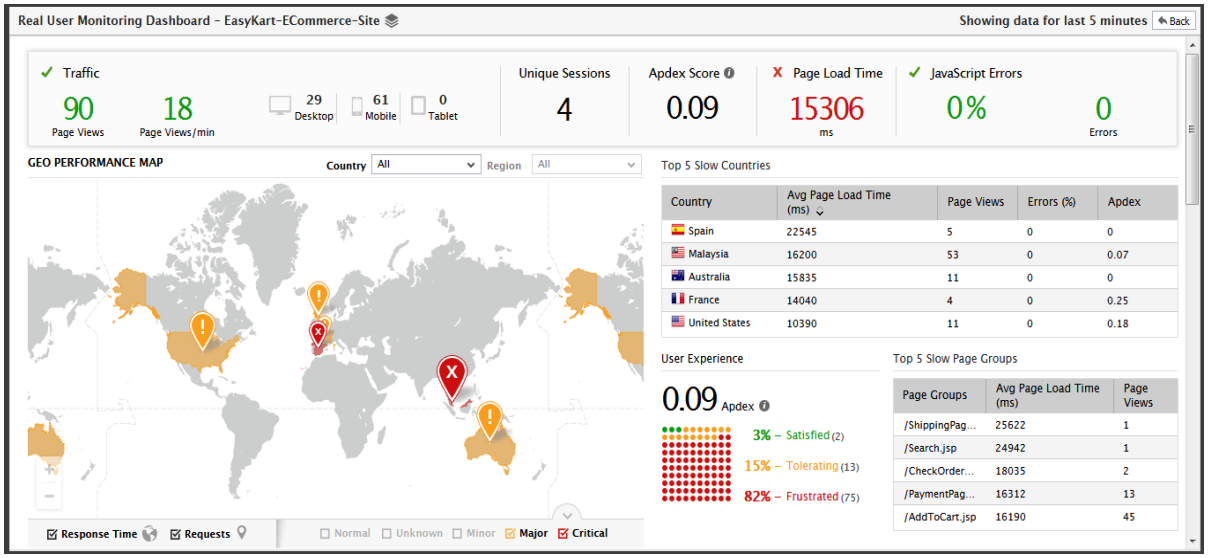


Figure 5.33: The Real User Monitor dashboard

5.12.2 User Experience Dashboard

One of the biggest challenges that Citrix/virtual/terminal desktop administrators have is that they often have to spend time troubleshooting problems that may be caused in other parts of the infrastructure that they do not control. For instance, a slowdown in the home network that a user is connecting from can impact the user experience when accessing a Citrix service. eG Enterprise includes a **User Experience Dashboard** that makes it possible for end-users themselves to view the performance metrics related to their access to the Citrix/VDI/Terminal server infrastructure. This way, end users can easily determine when they see a slowdown, is the problem being caused by

connectivity to the Citrix/VDI/Terminal server infrastructure, by any application(s) that they are using within a Citrix session, or by the Citrix infrastructure itself. If a performance problem is in the interconnecting network or in one of the applications the user has launched, the user can initiate corrective action (e.g., kill the offending process, contact the local network team, etc.) to alleviate the issue.

The self-service capability that the end-user performance dashboard provides results in fewer complaints and trouble calls to the Citrix/virtual desktop helpdesk. As a result, support costs are lower, end-users are less frustrated and the Citrix/virtual desktop deployment can proceed to successful completion.

Citrix/Virtual desktop/Terminal server administrators can also use the same dashboard to handle user complaints. When a specific user calls, they can view the performance dashboard for that user and determine what action needs to be taken to resolve the issue. This industry first end-user performance dashboard for Citrix/virtual desktop/terminal server infrastructures greatly simplifies the day to day operation of a Citrix/virtual desktop infrastructure. To access this dashboard, a Citrix/VDI/Terminal server administrator registered with the eG Enterprise system should first invoke the **Monitor** menu in the eG monitoring console, browse the **Dashboards** menu, move the mouse pointer over the **User Experience Dashboard** group, and pick the **VDI** or **XenApp** or **Terminal** option depending upon which user experience dashboard they want – the one for VDI users? or the one for XenApp users? or the one for the users logged into the terminal servers? (see 5.12.2)

Note:

The **VDI, XenApp** and **Terminal** options will be available only if the VDI, XenApp and Microsoft RDS components are managed in the monitored environment. If only one of the three is available – say, if only XenApp servers are managed in the environment - then, the **User Experience Dashboard** menu option will not display any sub-options. Instead, clicking on the **User Experience Dashboard** option will automatically lead administrators to the Overview dashboard of the XenApp environment.

If a SuperManager is engaged in managing the eG managers that are monitoring a slew of virtual components, in a virtual environment, then, each eG manager may contain separate User Experience Dashboards. It may become a tedious process for the egsm user of the SuperManager to login into each of the indiviudal managers to weigh the performance of the users of the virtual environments. Therefore it is essential for the egsm user to view the User Experience Dashboard of all the eG managers from the SuperManager console itself. The User Experience Dashboard option in the monitor interface of the eG SuperManager felicitates this.

An *egsm* user has the same view as that of the users who are eligible to login to the eG managers managed by the eG SuperManager. Apart from viewing the User Experience Dashboard of

individual users logged into the virtual desktops/VMs, the *egsm* user is also entitled to build the User Experience Dashboard of those individual users.

Note:

- The widgets added by the egsm user in the User Experience Dashboard is visible only to the egsm user in the monitor interface of the eG SuperManager. Individual users who login to the eG SuperManager will not have access to those widgets.
- The User Experience Dashboard viewed by the egsm user is the one with the default settings of the individual eG managers. If any user logging into the eG managers has overridden the default settings to customize his own settings, then, those customizations will not be visible to the eg sm user.

5.13 Graphs

eG Enterprise includes a variety of graphing capabilities for manual diagnosis. eG Enterprise supports the following graph types:

- Measure
- Summary
- Trend

To know more on the graphs and how the graphs help administrators in quickly analyzing the problems, refer to *Graphs* chapter of the *Monitoring Using the eG Enterprise* document.

5.14 Miscellaneous

5.14.1 User View

While managing a large number of users to the eG Enterprise system, the egsm user often find it very difficult to ascertain the overall health of a user's infrastructure, and whether there are any critical unresolved issues in that particular user environment. eG Enterprise provides a **USER VIEW** page that displays the number of segments/services/service groups/zones/components associated with a chosen user, and the alarms associated with these infrastructure elements. To access this page, follow the menu sequence: *Miscellaneous -> User View*.

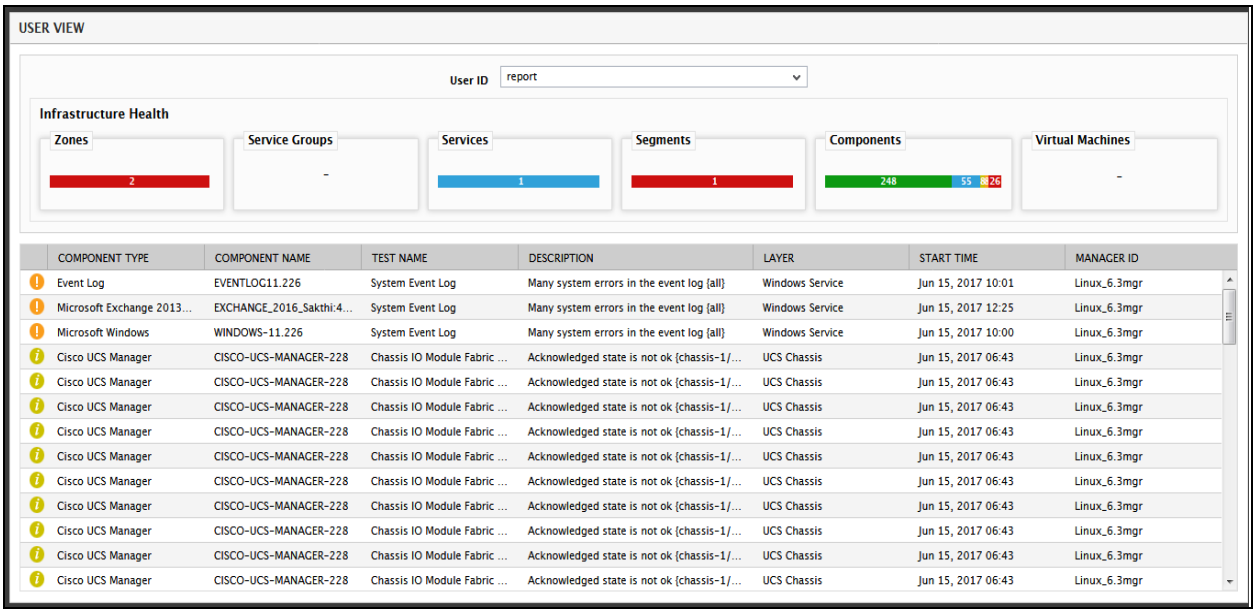


Figure 5.34: A selected user's view of the infrastructure monitored by the eG SuperManager

5.14.2 Control Actions

Monitoring solutions often provide the ability to alert an administrator over email, pager, SMS, etc., when problems occur. In response to an alert, the administrator has to perform domain-specific detailed analysis of the problem, often by running different commands on the target system. In this process, the administrator has to figure out and initiate corrective measures. Most monitoring solutions provide remote problem alerting capability, but the ability to **remotely login in a secure manner and perform detailed analysis and troubleshooting** is not available. To allow true anytime, anywhere management capability, such remote control of the target IT infrastructure must be possible using a web browser.

eG's Remote Control Action capability allows an administrator to remotely and securely access any monitored server in an IT infrastructure and to execute remote commands in order to perform detailed analysis of problems and to initiate corrective actions against them.

The benefits of eG's remote control actions are:

- Enable remote control in addition to routine monitoring, thereby offering a quick and easy way of initiating corrective actions
- Remote diagnosis and control of any component in the monitored infrastructure is enabled from anywhere, using just a web browser
- Remote control capability is selectively enabled for users based on their access rights

The control actions are enabled with no change in the eG architecture. The agents do not listen on any TCP ports. Hence, security risks in the target environment are minimum. Furthermore, since control actions can be initiated from a web browser, they can be triggered from anywhere, at any time.

The eG monitor interface also allows the egsm user to view the different eG agents and their modes of operation across all the eG managers reporting to the eG SuperManager. To do so, select the **Remote Control** option from the **Miscellaneous** tile of the eG monitor interface.

The resulting page (see Figure 5.35) lists the agents in the **Control** mode.

Figure 5.35: eG agents in the Control mode

To understand this concept better, refer to *Control Actions* section of the *Monitoring Using eG Enterprise* document.

5.14.3 Detailed Diagnosis

In order to view the detailed measures for a particular component in the monitored infrastructure, the *egsm* user will have to select the **Detailed Diagnosis** option from the **Miscellaneous** tile of the eG monitor interface.

To know more about the Detailed Diagnosis option refer to the *Detailed Diagnosis* section of the *Monitoring Using eG Enterprise* document.

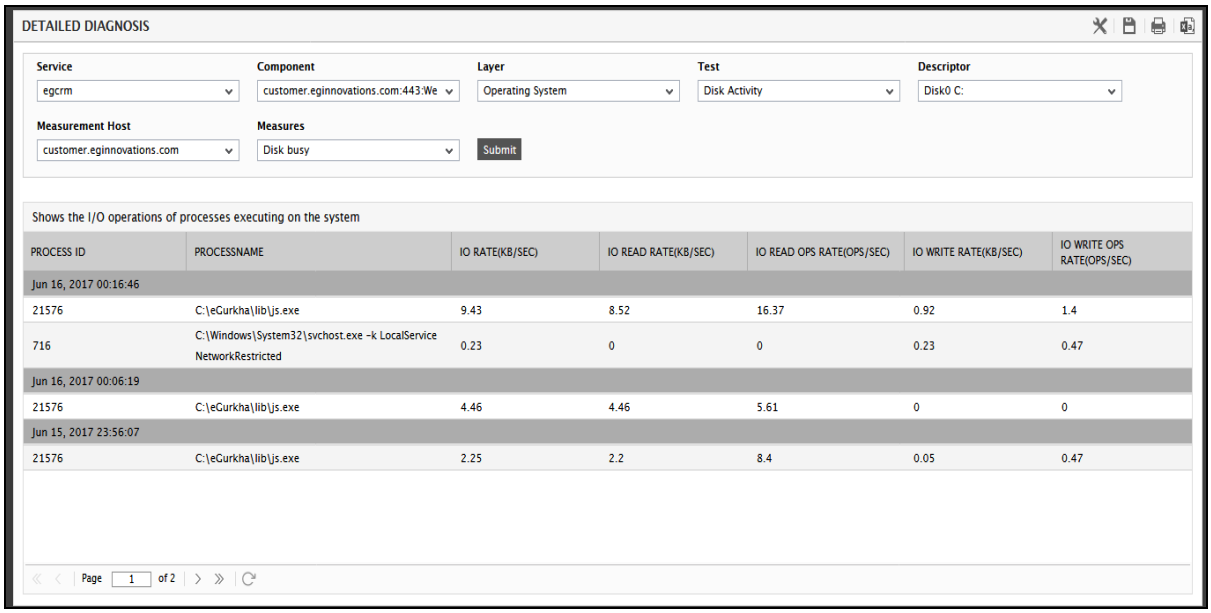


Figure 5.36: The detailed diagnosis of the Disk busy measure

5.14.4 Knowledge Base Search

The **Fix History** tab page allows you to view the details of fixes that are available for a chosen component, test, measure, and descriptor only. Administrators however, may require single-click access to the fixes related to all the managed components in the environment. They may also demand the flexibility to query the knowledge base for viewing only that problem/fix information that interests them. Therefore, to enable administrators to perform quick infrastructure-wide searches on the knowledge base and view the fix feedback of interest to them, the eG monitoring console offers the **KNOWLEDGE BASE SEARCH** page. In environments where multiple eG managers are deployed and a SuperManager is involved in monitoring the entire infrastructure, the *egsm* user may want to view the fix feedback of components of his/her interest. To such *egsm* users too the **KNOWLEDGE BASE SEARCH** page may be of great help!

To access this page, follow the *Miscellaneous -> Knowledge Base Search* menu sequence.

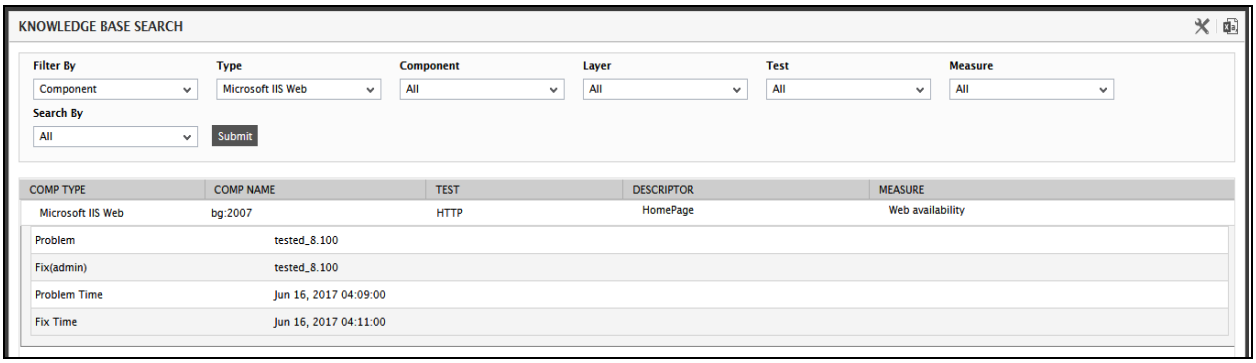


Figure 5.37: The Knowledge Base Search page

5.14.5 Measures Insight

eG agents are capable of extracting a wealth of performance information pertaining to the managed components. Larger the environment, larger will be the number of measures collected. The biggest challenge for the administrators of such large environments therefore, is to isolate and attend to the anomalies surrounding certain critical performance metrics. For instance, administrators of large, mission-critical Citrix environments might want to focus on some sensitive performance areas such as user sessions to the Citrix farm, resource usage by applications published on the farm, the rate of growth of the user profiles, etc. The metrics related to these areas are mapped to different layers and different tests of the Citrix monitoring model. Instead of taking the longer layer-test-measure route, administrators might prefer a single interface that provides a consolidated list of metrics collected from across the Citrix environment, so that they can easily pick and choose the metrics of interest to them. The **MEASURES** page (see Figure 5.38) that appears upon clicking the Measures menu option provides this much-needed measure focus.

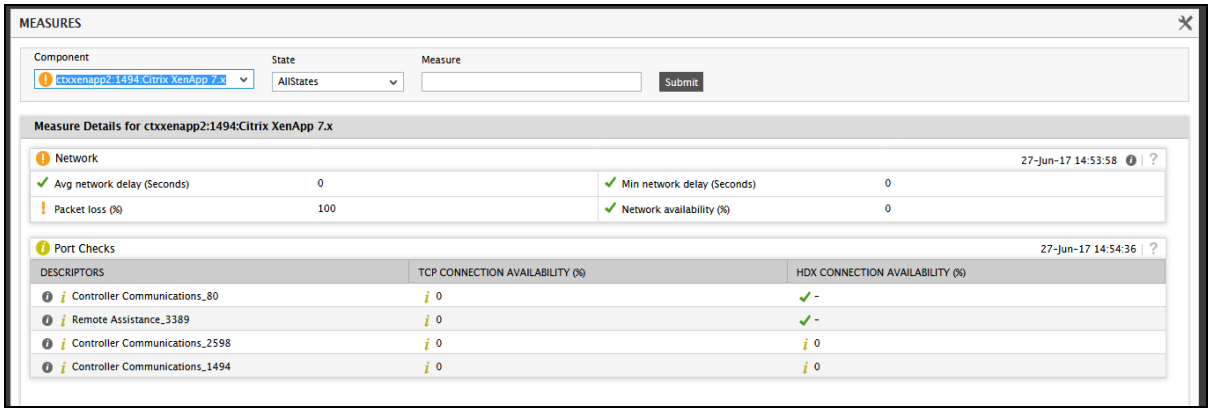


Figure 5.38: The MEASURES page

To know more about the **MEASURES** page, refer to *Measures Insight* section of the *Monitoring Using eG Enterprise* document.

Chapter 6: Conclusion

The **eG SuperManager** allows the eG Enterprise suite to efficiently handle large IT infrastructures spanning multiple geographies, different domains that are autonomous, and disparate networks. Besides scalability, the eG SuperManager brings the following additional benefits into the eG Enterprise suite:

Automatically consolidates the measure data distributed across a wide area, and displays it in a single interface; it thus saves the time, labor, and cost involved in manual data collection and consolidation; soes not require any backend support, thereby considerably reducing database maintenance overheads; is a flexible solution that can easily adapt to heterogeneous configurations of eG managers, reduces the bandwidth usage across geographies.

For more information about the eG SuperManager and the eG Enterprise suite, contact support@eginnovations.com.