Total Performance Visibility

eG Installation Guide

Table of Contents

Table of Figures

Chapter 1: eG Enterprise Architecture

eG Enterprise follows the manager-agent architecture that has been widely used in the past for designing monitoring systems. While the manager is a software component that controls what elements are monitored and how frequently they are monitored, the agents are software components that perform the monitoring functions. Figure 1.1 depicts the main components of eG Enterprise.

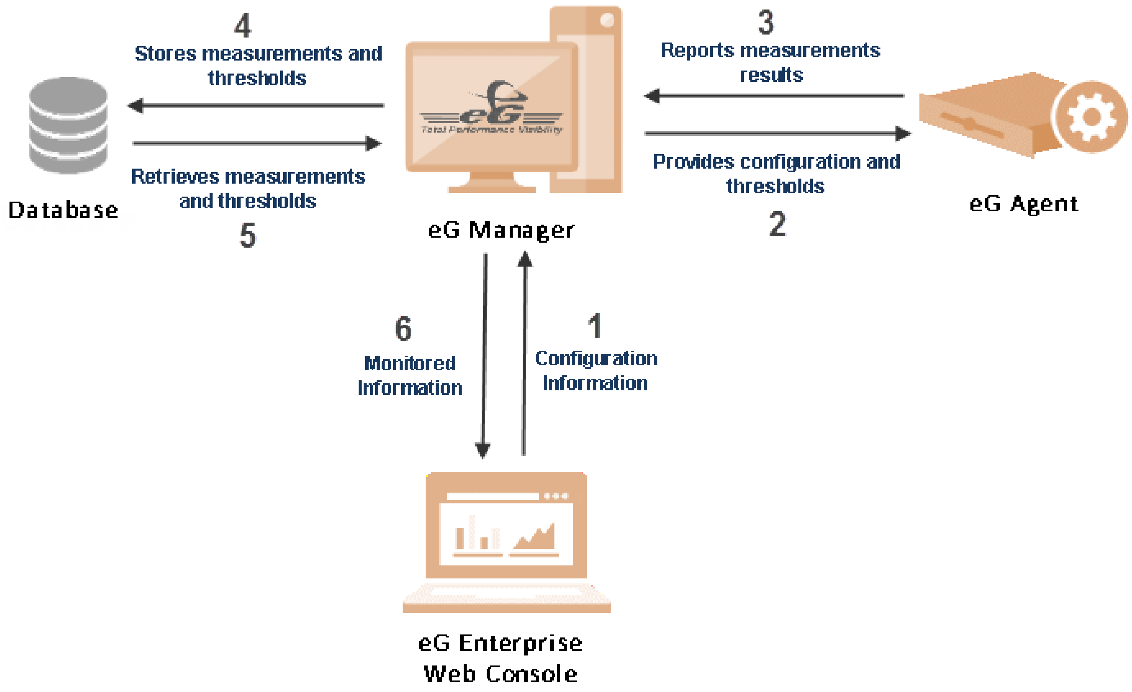

4
Stores measurements and thresholds
Database
Retrieves measurements and thresholds
5
3
Reports measurements results
Provides configuration and thresholds
2
eG Agent
eG Manager
6
Monitored Information
1
Configuration Information
eG Enterprise Web Console

Figure 1.1: The main components of eG Enterprise

The following topics sections describe these components in detail.

- Section **1.1**
- Section **1.2**
- Section **1.3**
- Section **1.4**

1.1 eG Manager

The eG manager is a software component responsible for coordinating the functioning of the agents, analyzing the reports from the agents to determine whether any problems exist, and for handling user requests to eG Enterprise. The main functions of the manager are:

- discovery of the target infrastructure,
- agent specification and control,
- database storage,
- threshold computation,
- alarm correlation, and
- user interactions.

1.2 eG Agent

The agents monitor the environment by running periodic **tests**. The outputs of the tests are called **measurements**. A measurement determines the state of a network / system / application / service element of the target environment. For example, a **Process test** reports the following measurements:

1. Number of processes of a specific type executing on a system.
2. The CPU utilization for these processes
3. The memory utilization for these processes

Agents use different approaches for testing the target environments. Based on the monitoring approach employed and where they are installed, agents are classified as follows:

- Section
- Section
- Section
- Internal agents
- Remote agents
- External agents

To know the details on the types, mechanisms used to collect performance metrics and installation procedure of agents have been elaborately discussed in **eG Agent Installation** chapter*Detailed Installation Guide*.

1.3 Database

The eG database is responsible for persistent storage of the measurement results. You can configure this database on an Oracle database server (version 11G / 12c / 18c / 19c) or a Microsoft SQL Server (version 2008 R2 / 2012 / 2014 / 2016 / 2017 / 2019). You also have the option of using an existing Microsoft Azure SQL Database (if any) as the eG backend. Note that you can configure this database on Microsoft SQL Server version 2016 (and above) installed on Linux operating system too. Separate tables are maintained in the eG database for each of the tests being executed by eG agents.

On a Microsoft SQL Server Enterprise Edition / Microsoft SQL 2016 (and above) SP1 Standard Edition / Microsoft SQL Azure, the eG manager automatically creates multiple **partitions** – one for each day – in every table. When storing data in the database, the manager automatically stores the data pertaining to a particular day into the partition created for that day.

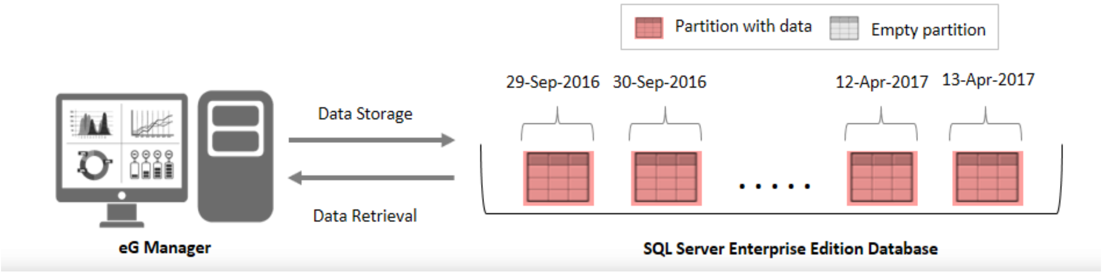


Figure 1.2: How database partitioning works

Note:

- The **Database Partitioning** feature is available only for the eG database hosted on Microsoft SQL Server Enterprise Edition, Microsoft SQL 2016 (and above) SP1 Standard Edition, or Microsoft SQL Azure.
- By default, 30 partitions are created in each table. You can override this default limit by changing the value of the *MaxPartitionDays* parameter in the [MANAGER_SETTINGS] section of the eg_db.ini file (in the <EG_INSTALL_DIR>\manager\config directory).
- You can even turn off the database partitioning feature, if required. For this, set the *EnableTablePartition* flag in the [DB_PROPERTIES] section of the eg_db.ini file (in the <EG_INSTALL_DIR>\manager\config directory) to **No**.

On Oracle 12c (and above), 'Partitioning' is a licensed capability. If your Oracle database server license enables partitioning support, then you can have the eG manager store performance and configuration metrics in partitions on the eG database. At the time of configuring the eG database on an Oracle database server 12c (or above), setup prompts you to confirm whether/not your DB license supports the Partitioning feature. If you confirm support, then setup will automatically create a partition and store metrics in it. If your DB license does not support the partitioning feature, then 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.

Note:

If you choose to store data in partitions on an Oracle database server, auto-indexing of the eG database will not be performed.

The database design provides a way to periodically purge old data from the database. The periodicity with which the data will be purged by the database is configurable by the user. Where the database partitioning feature is turned on, partitions for selected days are dropped during cleanup. In such environments therefore, cleanup will be fast and efficient.

Besides the measurement tables, the database hosts threshold tables for each test. A threshold table indicates the upper and lower ranges of the threshold values for each measurement.

1.4 eG Web Console

eG Web Console enables a user to interact with eG Enterprise. The recommended browser for the eG Web Console is Internet Explorer 10, 11, and Edge, Mozilla Firefox v18 or higher, and Chrome v28 (or above). The eG Web Console consists of **Admin**, **Monitor**, **Reporter** and **Configuration** tabs using which administrators can customize the configuration of eG Enterprise and monitor the IT environment. The options provided in the tab panes help administrators to do the following tasks without any hassle:

- Discovering and managing the components to be monitored,
- Configuring the tests for each component,
- Monitoring the measurements reported by the eG agent
- Creating and viewing dashboards
- Generating reports on how do the managed components perform in the environment?
- Troubleshooting the issues
- Integrating the eG Enterprise with third-party systems.

Broadly, the eG Web Console allows a user to first customize the configuration of eG Enterprise (i.e., what servers and web sites to monitor, how frequently to monitor, what specific tests to run, etc.) and subsequently to monitor the measurements made by the agents.

To avoid overwhelming users with the variety and amount of results being generated based on measurements made by the eG agents, the web console presents the results of the measurements in a logical and coherent manner. The eG manager's interpretation of the state of each element of an IT infrastructure is first displayed before the results of the individual measurements are made available - e.g., by displaying graphs indicating the change in value of the measurement with time of day. An alarm window immediately highlights the pending alarms in the target environment, prioritized based on the eG manager's assessment of the severity of the associated problems.

Chapter 2: eG Manager Installation

The eG manager is responsible for coordinating the functioning of the agents, analyzing the reports from the agents to determine whether any problems exist, and for handling user requests to eG Enterprise. The main functions of the manager are discovery of the target infrastructure, agent specification and control, database storage, threshold computation, alarm correlation, and user interactions.

The procedure for installing the eG manager differs depending on the operating system environment being used on the server on which the manager is to be installed.

- For detailed instructions of installing and configuring the manager on Windows operating systems, refer to **eG Manager on Windows**.
- For detailed instructions of installing and configuring the manager on Unix operating systems, refer to **eG Manager on Unix**.

Make sure that the pre-requisites given in the **Pre-requisites for Installing eG Manager** have been fulfilled before you start installing the eG manager.

Chapter 2: Pre-requisites for Installing eG Manager

A set of pre-requisites should be fulfilled before you start installing eG Manager in your environment. These requirements are clearly stated in the following sections:

2.0.1 For Windows Platforms

For the eG manager to function, the Windows system on which the manager is being installed should support:

1. Windows 2008 server (OR) Windows 7 (OR) Windows 8 (OR) Windows 2012 (OR) Windows 10 (OR) Windows 2016 (OR) Windows 2019
2. Only systems with a static IP address (i.e. no DHCP address) should be used for installing the eG manager
3. A minimum of 8 GB RAM would be required
4. A minimum of 100 GB disk space
5. For the eG database, use Oracle database server (version 11G / 12C / 18C / 19c) / Microsoft

SQL Server (version 2008 R2 / 2012 / 2014 / 2016 / 2017 / 2019) / Microsoft Azure SQL database / Microsoft SQL Server (version 2016 /2017) installed on Linux operating system.

Note:

- When using an Oracle database server / Microsoft SQL server as the eG backend, you can install the database on the same system as the eG manager, or on a separate system. However, for implementations with 100 monitors or more, the database should ideally be hosted on a separate system. Both the eG manager and the eG database can be hosted on virtual machines or physical machines.
- Moreover, when using a Microsoft SQL Server backend, ensure that the installation of the server is performed in the **case-insensitive** mode. Also, make sure that the **Simple Recovery** mode is set. Additionally, make sure that the requirements outlined in Section **2.0.3** are fulfilled.
- To ensure high availability of the eG database, you can optionally enable any of the following HA configurations for the eG database:
  - Oracle Real Application Cluster (Oracle RAC), for an eG database on Oracle;
  - Microsoft SQL Cluster / SQL AlwaysOn Availability Group, for an eG database on Microsoft SQL;

6. Internet Explorer 11 or Edge, Mozilla Firefox v18 or higher, or Chrome v28 or above as the browser. To ensure peak browser performance, ensure that the browser settings recommended in Section **2.0.4** are implemented.
7. A valid eG license

Note:

The eG manager is bundled with a Tomcat server. Before installing the eG manager therefore, make sure that no other Tomcat server pre-exists on the target manager host.

2.0.2 For Unix Platforms

For the eG manager to function effectively, the Unix system on which the manager is being installed should support:

- Red Hat Enterprise Linux 5 (or higher) (or) CentOS v5.2 (or above) (or) Oracle Linux v6.x (or higher) (or) Fedora Linux (or) Ubuntu (or) Debian (or) openSUSE
- For the eG database, use Oracle database server (version 11G / 12c / 18c / 19c) / Microsoft SQL

Server (version 2008 R2 / 2012 / 2014 / 2016 / 2017 / 2019) / Microsoft Azure SQL database / Microsoft SQL Server (version 2016 /2017) installed on Linux operating system.

Note:

- When using an Oracle database server / Microsoft SQL server as the eG backend, you can install the database on the same system as the eG manager, or on a separate system. However, for implementations with 100 monitors or more, the database should ideally be hosted on a separate system. Both the eG manager and the eG database can be hosted on virtual machines or physical machines.
- Moreover, when using a Microsoft SQL Server backend, ensure that the installation of the server is performed in the **case-insensitive** mode. Also, make sure that the **Simple Recovery** mode is set. Additionally, make sure that the requirements outlined in Section **2.0.3** are fulfilled.
- To ensure high availability of the eG database, you can optionally enable any of the following HA configurations for the eG database:
  - Oracle Real Application Cluster (Oracle RAC), for an eG database on Oracle;
  - Microsoft SQL Cluster / SQL AlwaysOn Availability Group, for an eG database on Microsoft SQL;

- A minimum of 8 GB RAM would be required
- A minimum of 100 GB of disk space free
- Internet Explorer 11 or Edge, Mozilla Firefox v18 or higher, or Chrome v28 or above as the browser. To ensure peak browser performance, ensure that the browser settings recommended in Section **2.0.4** are implemented.
- A valid eG license

Note:

The eG manager is bundled with a Tomcat server. Before installing the eG manager therefore, make sure that no other Tomcat server pre-exists on the target manager host.

A set of pre- requisites should be fulfilled before you start installing eG Enterprise in your environment. These requirements are clearly stated in the following tables:

Pre-requisites for Installing eG Manager

Operating Systems	**Unix** - Red Hat Enterprise Linux 5 (or higher), CentOS 5.2 (or higher), Oracle Linux v6.x (or higher), Fedora Linux, Ubuntu, Debian, openSUSE,

	Windows - Windows 2008 server (OR) Windows 7 (OR) Windows 8 (OR) Windows 10 (OR) Windows 2012 (OR) Windows 2016 (OR) Windows 2019
Database	For the eG database, use Oracle database server (version 11G / 12c / 18c / 19c) / Microsoft SQL Server (version 2008 R2 / 2012 / 2014 / 2016 / 2017 / 2019) / Microsoft Azure SQL database / Microsoft SQL Server (version 2016 /2017) installed on Linux operating system. **Note:** • When using an Oracle database server / Microsoft SQL server as the eG backend, you can install the database on the same system as the eG manager, or on a separate system. However, for implementations with 100 monitors or more, the database should ideally be hosted on a separate system. Both the eG manager and the eG database can be hosted on virtual machines or physical machines. • Moreover, when using a Microsoft SQL Server backend, ensure that the installation of the server is performed in the **case-insensitive** mode. Also, make sure that the **Simple Recovery** mode is set. Additionally, make sure that the requirements outlined in Section **2.0.3** are fulfilled. • To ensure high availability of the eG database, you can optionally enable any of the following HA configurations for the eG database: a. Oracle Real Application Cluster (Oracle RAC), for an eG database on Oracle; b. Microsoft SQL Cluster / SQL AlwaysOn Availability Group, for an eG database on Microsoft SQL;
Memory	A minimum of 8 GB RAM
Disk Space	A minimum of 1 GB of disk space free
Browsers	Internet Explorer 11 or Edge, Mozilla Firefox v18 or higher, or Chrome v28 or above as the browser For more details on the browser settings, refer to Section **2.0.4**
Other Requirements	Only systems with a static IP address (i.e. no DHCP address)

	should be used for installing the eG manager on Windows platforms

Note:

The eG manager is bundled with a Tomcat server. Before installing the eG manager therefore, make sure that no other Tomcat server pre-exists on the target manager host.

Pre-requisites for Installing eG Agent

Memory	A minimum of 512MB RAM
Disk Space	A minimum of 1 GB of disk space free
Operating Systems	**Unix** - Solaris 7 (or higher), Red Hat Enterprise Linux 5 (or higher), AIX 4.3.3 (or higher), HP-UX 10 (or higher), Free BSD 5.4, Tru64 5.1, openSUSE 11 (or above), CentOS 5.2 (or above), Fedora Linux, Oracle Linux v6.x (or higher), Ubuntu, Debian **Windows** - Windows 2008 server (OR) Windows Vista (OR) Windows 7 (OR) Windows 8 (OR) Windows 10 (OR) Windows 2012 (OR) Windows 2016 (OR) Windows 2019

Note:

- On Windows systems, the user account used to run the eG Agent on a system has to be a part of the local administrator group of that system. The two basic privileges that the user running the eG agent should have are “allow log on locally” and “log on as a service”. If the proper privileges are not provided to the user running the eG agent service, the eG agent will stop after running for a while.
- On Unix systems, the eG agent software has to be installed from a super-user account.

The detailed procedure for installing the eG manager and eG agent on different operating system platforms is elaborately discussed in the following chapters*Detailed Installation Guide*.

2.0.3 Pre-requisites for Configuring an eG Database on a Microsoft SQL Server

Before even commencing the configuration process of the eG manager using an Microsoft SQL Server database, ensure that the following are in place:

1. The Microsoft SQL Server should allow 'unlimited' concurrent connections

   Given below are the steps to be followed to fulfill this requirement on an Microsoft SQL Server 2014:

   - Login to the Microsoft SQL server that you want to use as the eG backend, as an *administrator*.
   - Open the **Microsoft SQL Server Management Studio**.
   - In the **Object Explorer** that appears next, right-click on the node that represents the SQL server you are logged into, and then select the **Properties** option from the shortcut menu that appears.

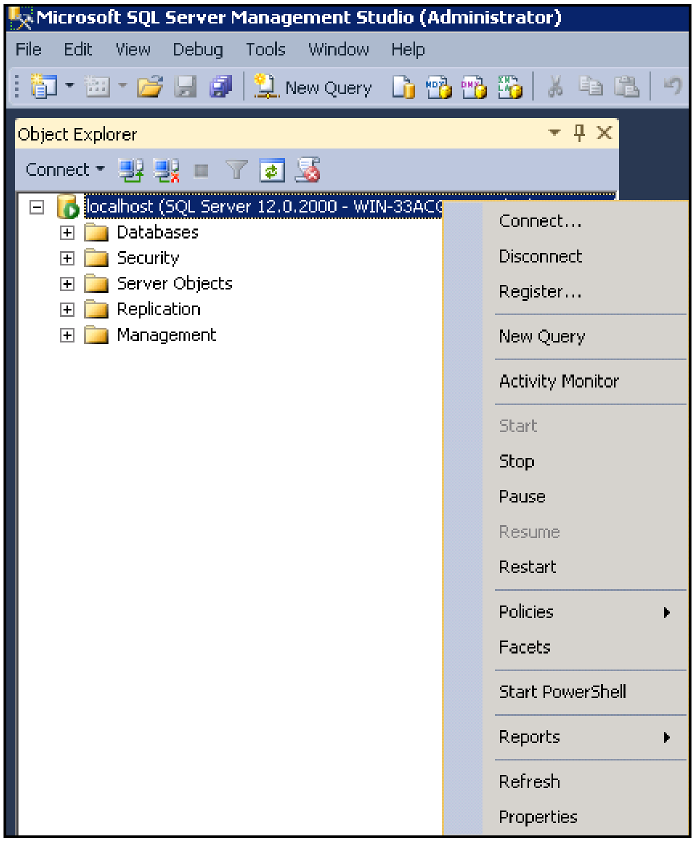
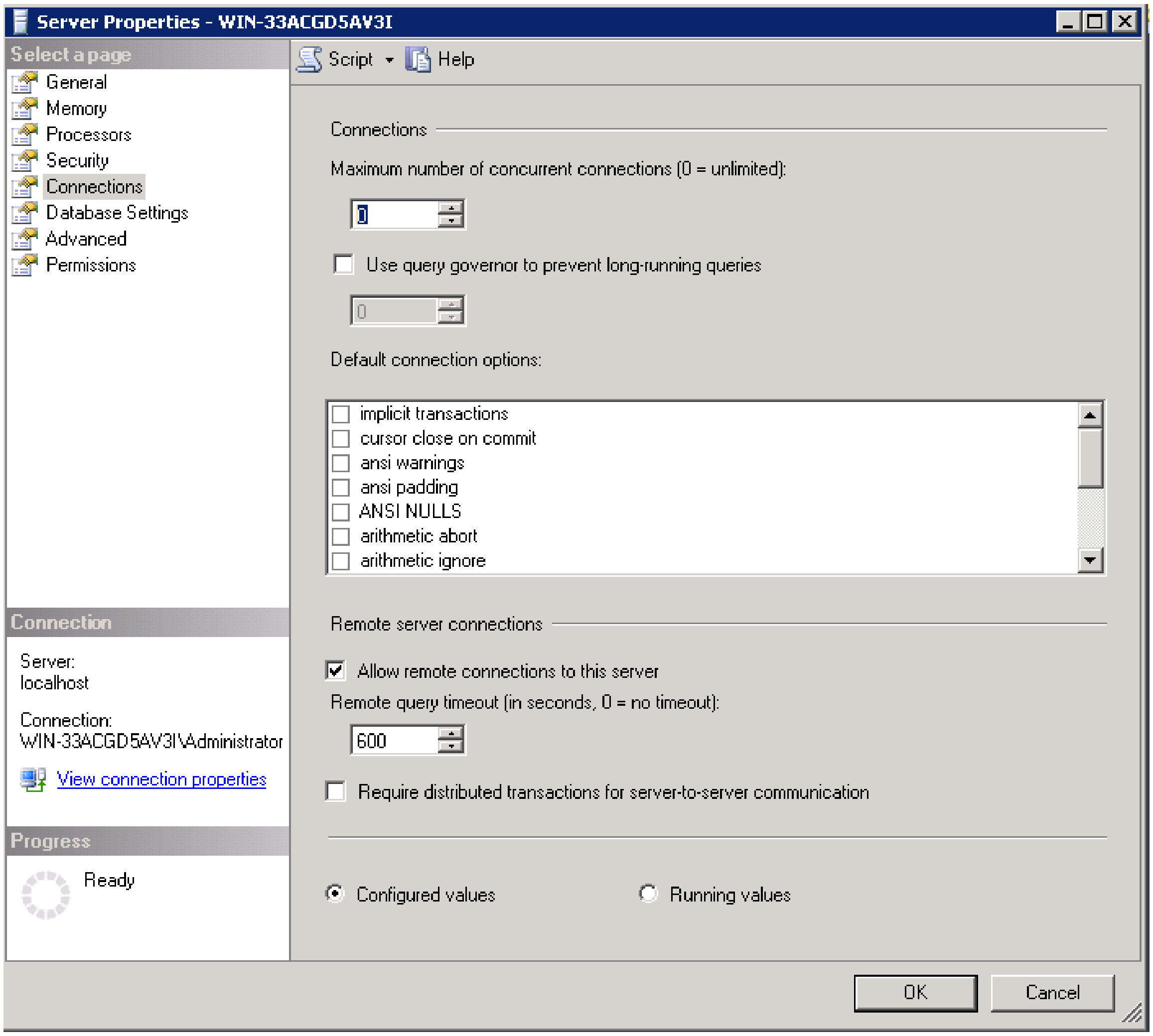


Figure 2.1: Selecting the Properties option from the server shortcut menu

   - The **Server Properties** dialog box will then appear. From the **Select a page** panel in the left, select the **Connections** page, as depicted by Figure 2.2. The right panel will then change to display many options.



Server: localhost

Connection: WIN-33ACGD5AV3I\Administrator

Connections

Maximum number of concurrent connections (0 = unlimited): 0

□ Use query governor to prevent long-running queries: 0

Default connection options:

- □ implicit transactions
- □ cursor close on commit
- □ ansi warnings
- □ ansi padding
- □ ANSI NULLS
- □ arithmetic abort
- □ arithmetic ignore

Remote server connections

☑ Allow remote connections to this server

Remote query timeout (in seconds, 0 = no timeout): 600

□ Require distributed transactions for server-to-server communication

● Configured values ○ Running values

Figure 2.2: Setting the maximum concurrent user connections

- In the right panel, make sure that the **Maximum concurrent user connections** field is set to **unlimited** (0).
- Then, click the **OK** button to save the settings and to close the dialog box.

2. Multi-protocol support should be configured on the Microsoft SQL server

   Ensure that **Multi-protocol** support is enabled on the Microsoft SQL server to be used as the backend for the eG manager. To ensure this, do the following:

   - Open the SQL Server Configuration Manager by following the menu sequence depicted by Figure 2.3.

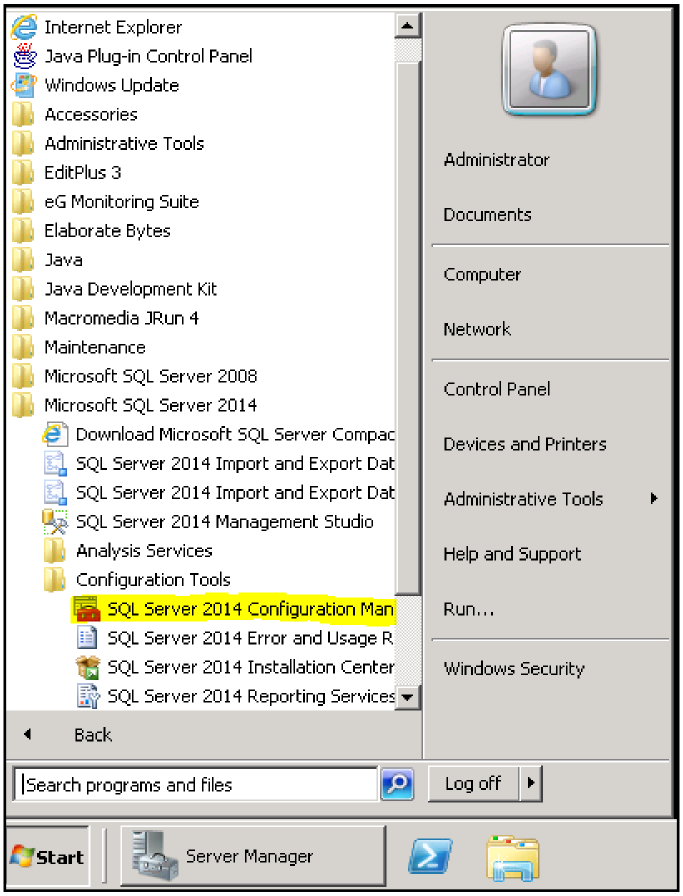
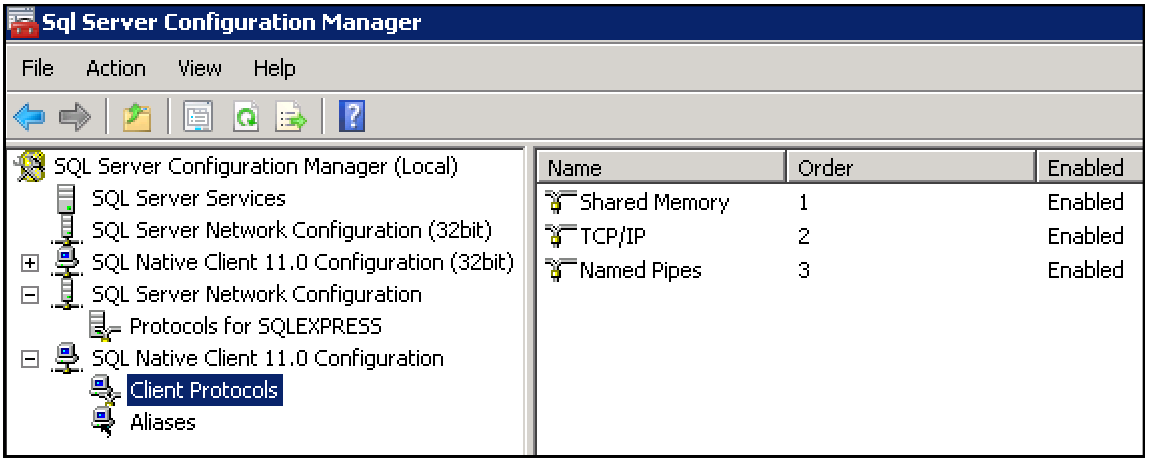

Internet Explorer
Java Plug-in Control Panel
Windows Update
Accessories
Administrative Tools
EditPlus 3
eG Monitoring Suite
Elaborate Bytes
Java
Java Development Kit
Macromedia JRun 4
Maintenance
Microsoft SQL Server 2008
Microsoft SQL Server 2014
Download Microsoft SQL Server Compac
SQL Server 2014 Import and Export Dat
SQL Server 2014 Import and Export Dat
SQL Server 2014 Management Studio
Analysis Services
Configuration Tools
SQL Server 2014 Configuration Man
SQL Server 2014 Error and Usage R
SQL Server 2014 Installation Center
SQL Server 2014 Reporting Services
Back
Search programs and files
Administrator
Documents
Computer
Network
Control Panel
Devices and Printers
Administrative Tools
Help and Support
Run...
Windows Security
Log off
Start
Server Manager

Figure 2.3: Opening the SQL Server Configuration Manager

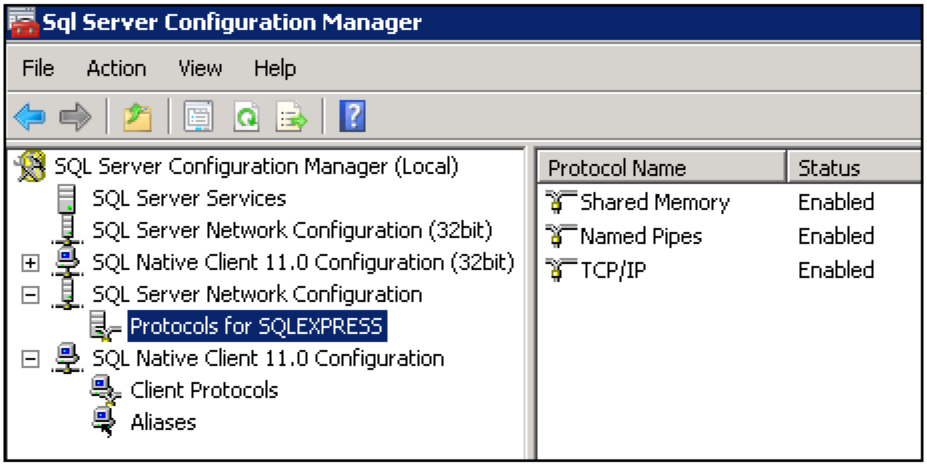
- Figure 2.4 will then appear. Expand the **SQL Native Client 11.0 Configuration** node in the **SQL Server Configuration Manager (Local)** tree structure in the left panel of Figure 2.4. Then, click the **Client Protocols** sub-node within. The right panel will then change to display the client protocols and their current state – i.e., whether enabled/disabled.


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 11.0 Configuration (32bit)
SQL Server Network Configuration
Protocols for SQLEXPRESS
SQL Native Client 11.0 Configuration
Client Protocols
Aliases

Name	Order	Enabled
Shared Memory	1	Enabled
TCP/IP	2	Enabled
Named Pipes	3	Enabled

Figure 2.4: Client protocols and current state

- Make sure that all the three protocols displayed in the right panel of Figure 2.4 are **Enabled**. If any protocol is disabled, then, right-click on that protocol in Figure 2.4 and select the **Enabled** option from the shortcut menu that appears.
- Next, expand the **SQL Server Network Configuration** node and select the **Protocols for <SQL_Server_Name>** sub-node within (see Figure 2.5). The right panel will then change to display the server protocols and their current state – i.e., whether enabled/disabled.
- Make sure that all the three protocols displayed in the right panel of Figure 2.5 are **Enabled**. If any protocol is disabled, then, right-click on that protocol in Figure 2.5 and select the **Enabled** option from the shortcut menu that appears.


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 11.0 Configuration (32bit)
SQL Server Network Configuration
Protocols for SQLEXPRESS
SQL Native Client 11.0 Configuration
Client Protocols
Aliases

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Enabled
TCP/IP	Enabled

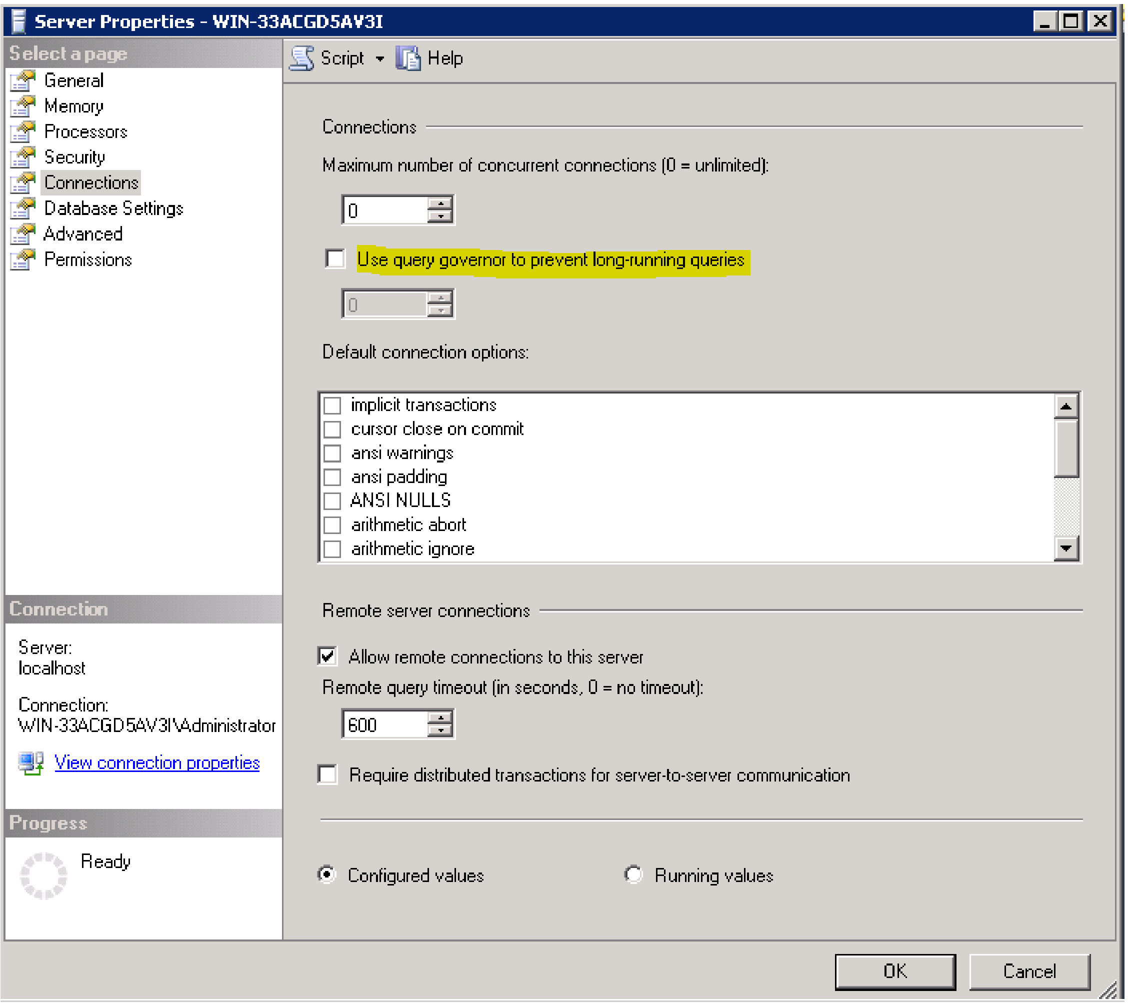
Figure 2.5: Server protocols and their current state

- After you enable any client/server protocol, make sure the Microsoft SQL server is restarted.

3. The SQL Server should be configured to allow long-running queries.

   To ensure this, do the following:

   - Login to the Microsoft SQL server that you want to use as the eG backend, as an *administrator*.
   - Open the **Microsoft SQL Server Management Studio**.
   - In the **Object Explorer** that appears next, right-click on the node that represents the SQL server you are logged into, and then select the **Properties** option from the shortcut menu that appears (see Figure 2.1).
   - The **Server Properties** dialog box will then appear. From the **Select a page** panel in the left, select the **Connections** page, as depicted by Figure 2.6. The right panel will then change to display many options.
   - Make sure that the **Use query governor to prevent long-running queries** option in the right panel is disabled. If not, then uncheck the check box to disable it.



Server:
localhost

Connection:
WIN-33ACGD5AV3I\Administrator

Connections

Maximum number of concurrent connections (0 = unlimited): 0

□ Use query governor to prevent long-running queries

0

Default connection options:

□ implicit transactions
□ cursor close on commit
□ ansi warnings
□ ansi padding
□ ANSI NULLS
□ arithmetic abort
□ arithmetic ignore

Remote server connections

☑ Allow remote connections to this server

Remote query timeout (in seconds, 0 = no timeout): 600

□ Require distributed transactions for server-to-server communication

● Configured values ○ Running values

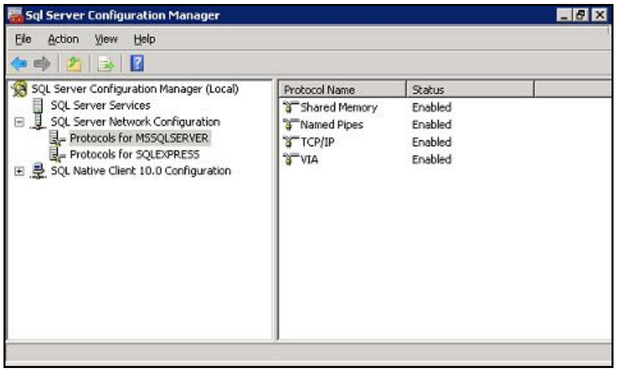
Figure 2.6: Enabling long-running queries to be executed on the Microsoft SQL server

- Finally, click the **OK** button in Figure 2.6.

4. If the Microsoft SQL Server 2008 is used as the eG backend, then ensure that the VIA protocol is disabled on the server

   To achieve this, do the following:

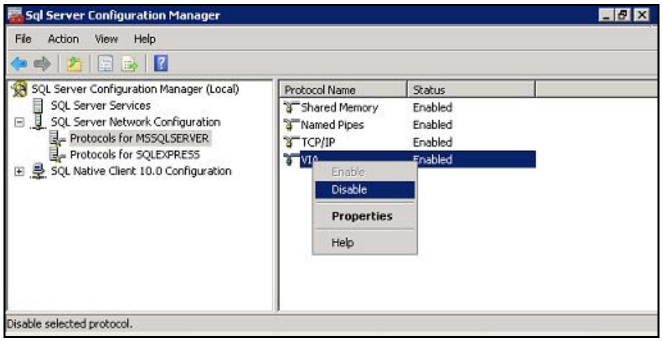
   - On the Microsoft SQL Server 2008 host, open the **SQL Server Configuration Manager**.
   - In the left panel of the configuration manager, click on the **Protocols for <SQLSERVERname>** node as depicted by Figure 2.7. The list of protocols that the SQL server supports will then be displayed in the right panel (see Figure 2.7).


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration
Protocols for MSSQLSERVER
Protocols for SQLEXPRESS
SQL Native Client 10.0 Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Enabled
TCP/IP	Enabled
VIA	Enabled

Figure 2.7: The list of protocols on the SQL Server Configuration Manager

- Check whether the status of the **VIA** protocol in the list is **Enabled**. If so, proceed to disable it by right-clicking on the **VIA** protocol and selecting the **Disable** option (see Figure 2.8).


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration
Protocols for MSSQLSERVER
Protocols for SQLEXPRESS
SQL Native Client 10.0 Configuration
Enable
Disable
Properties
Help

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Enabled
TCP/IP	Enabled
VIA	Enabled

Disable selected protocol.

Figure 2.8: Disabling the VIA protocol

- Next, check whether the other protocols listed in the right panel of Figure 2.7 are **Enabled**. If not, then enable those protocols.

5. Ensure that the 'SQL Server' service is running on the SQL Server host.

6. If the Microsoft SQL Server uses named instances (instead of port number), then, before configuring that server to function as the eG backend, make sure that the 'SQL Browser service' is up and running on the SQL Server host.

2.0.4 Recommended Browser Settings

To connect to the web-based eG management console, you can use any of the following browsers:

- Internet Explorer 11, or Edge
- Mozilla Firefox v18 or above
- Chrome v28 or above

No additional plug-ins need to be installed on any browser for the purpose of accessing or working with the eG manager.

However, before attempting to use any of the browsers for accessing the eG manager, make sure that the settings described in the topicssub-sections below are in place.

- Section **2.0.4.1**
- Section **2.0.4.2**
- Section **2.0.4.3**

2.0.4.1 Internet Explorer Settings

To be able to use Internet Explorer as the browser for the eG manager, the following pre-requisites should be fulfilled:

- The **Document mode** should be *Edge (Default)*.
- If the eG manager has already been added to the compatibility view, remove it, and disable the compatibility mode.
- The security settings should be set to Medium or Medium-High.
- Allow pop-ups from the eG manager alone.
- Configure the browser to use TLS and not SSL.

Each of these requirements have been detailed in the sub-sections that follow.

2.0.4.1.1 Changing the Document Mode

To achieve this, follow the steps below:

1. Open the Internet Explorer browser.
2. Click on the **Tools** icon in the IE tool bar, and select the **F12 Developer Tools** option from the menu that pops up (see Figure 2.9).

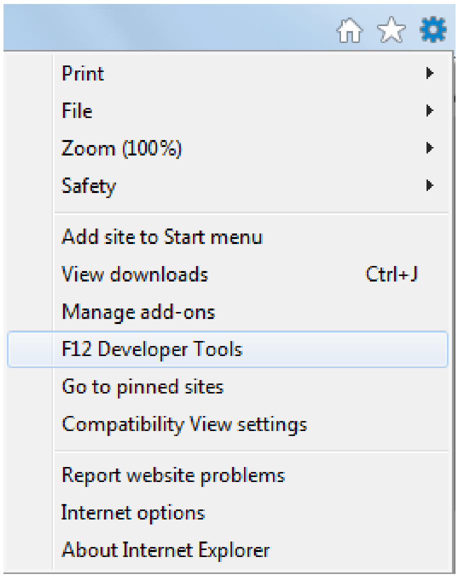
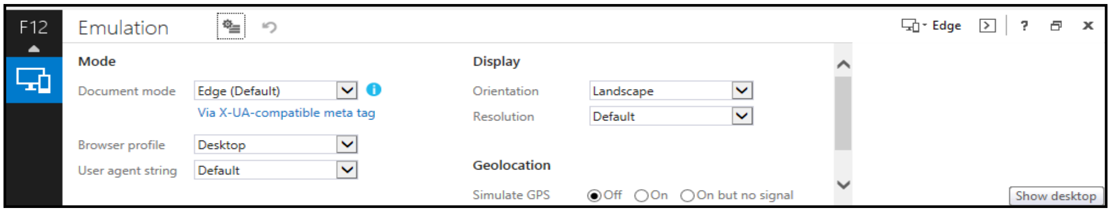


Figure 2.9: Launching the Developer Tools

3. When Figure 2.10 appears, check to see if the selection against **Document mode** is *Edge (Default)*. If not, change it to *Edge (Default)*.



Mode

Document mode: Edge (Default)
Via X-UA-compatible meta tag

Browser profile: Desktop

User agent string: Default

Display

Orientation: Landscape

Resolution: Default

Geolocation

Simulate GPS ● Off ○ On ○ On but no signal

Figure 2.10: Changing the Document mode

2.0.4.1.2 Disabling the Compatibility Mode

For this, follow the steps detailed below:

1. Click on the **Tools** icon in the IE tool bar, and select the **Compatibility View Settings** option from the menu that pops up (see Figure 2.11).

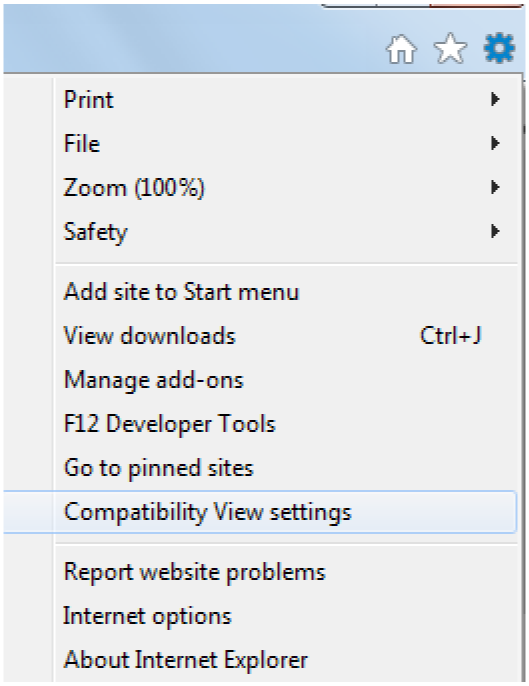
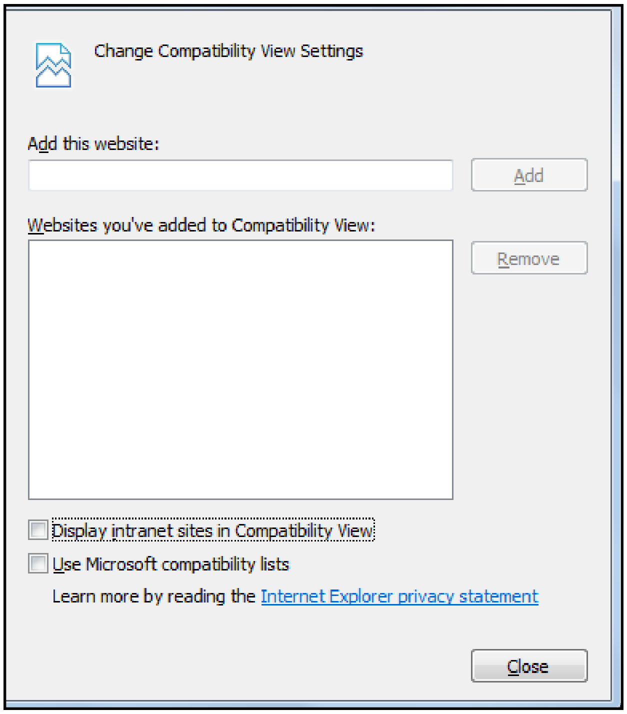


Figure 2.11: Accessing the Compatibility View Settings dialog

2. In Figure 2.12 that then appears, check whether the eG manager's URL is listed in the **Websites you've added to Compatibility View** list. If it is, then, select the eG manager's URL from that list, and click the **Remove** button alongside, to remove it.


Change Compatibility View Settings
Add this website:
Add
Websites you've added to Compatibility View:
Remove
Learn more by reading the Internet Explorer privacy statement
Close

□ Display intranet sites in Compatibility View

□ Use Microsoft compatibility lists

Figure 2.12: Removing the eG manager's URL from the Compatibility View list

3. Also, make sure that **Display intranet sites in Compatibility View** and the **Use Microsoft compatibility lists** check boxes are deselected.
4. Finally, click the **Close** button in Figure 2.12.

2.0.4.1.3 Changing Security Settings

To make these changes, follow the steps below:

1. Click on the **Tools** icon in the IE tool bar, and select **Internet Options** from the menu that pops up (see Figure 2.13).

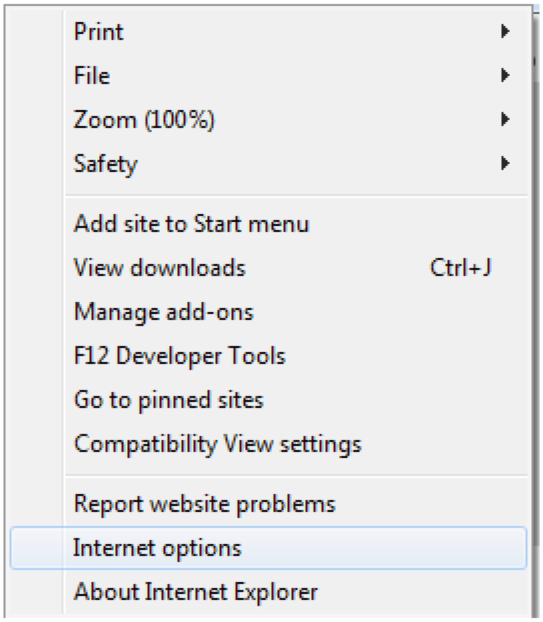
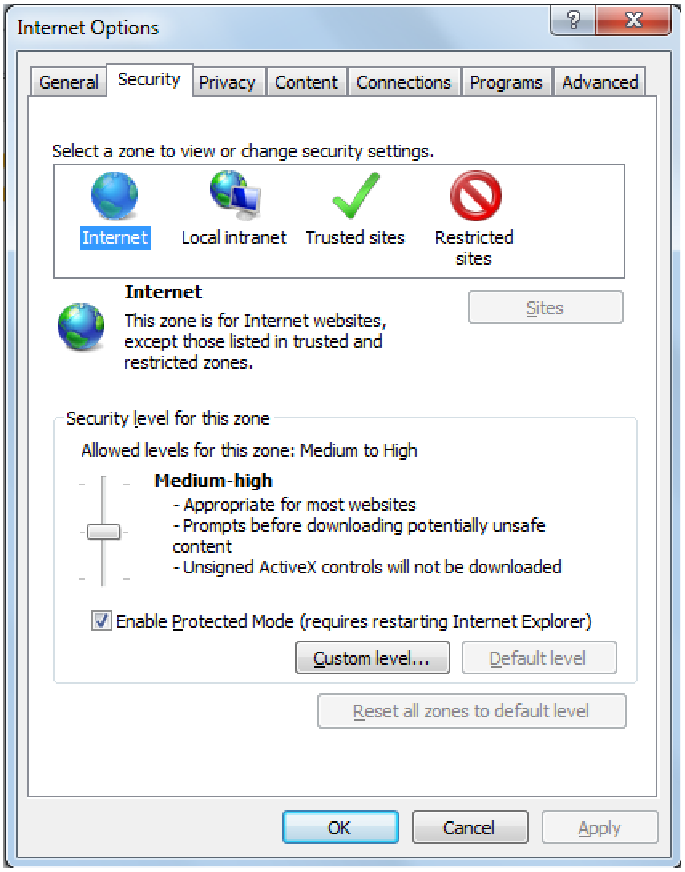


Figure 2.13: Selecting the Internet Options option from the Tools menu

2. Figure 2.14 will then appear. If your eG manager will be accessed by internet users only, then security settings should be configured for the **Internet** and the **Trusted Sites** zones. For this, follow the steps detailed below:

   - Select the **Security** tab page in Figure 2.14 and then pick **Internet** from the **Select a zone…** section.



Select a zone to view or change security settings.

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

Allowed levels for this zone: Medium to High

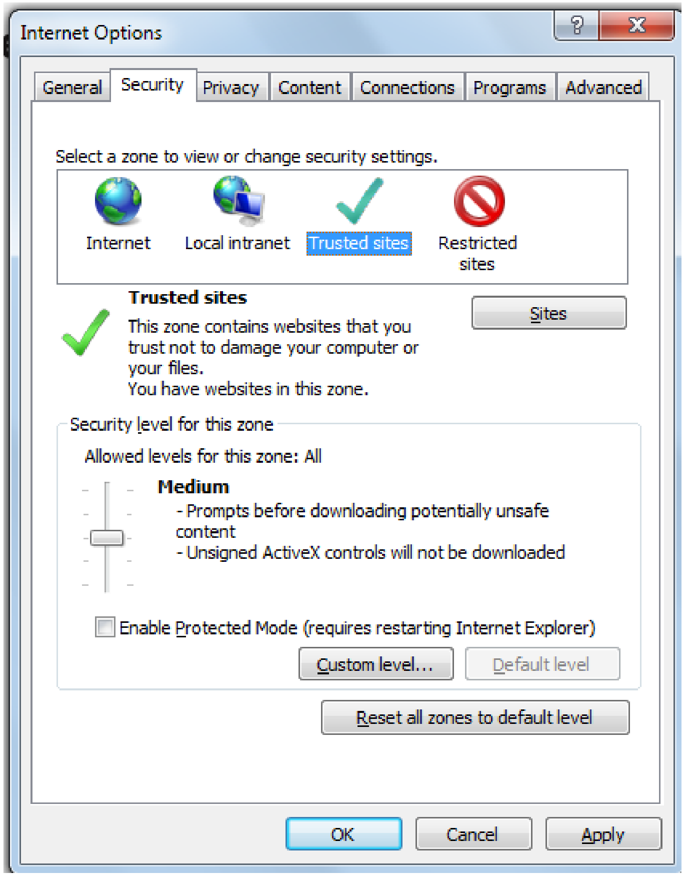
Medium-high

- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☑ Enable Protected Mode (requires restarting Internet Explorer)

Figure 2.14: Changing the security settings for the Internet zone

- Use the slider in the **Security level for this zone** section to set the security level at *Medium* or *Medium-high*.
- Then, select the **Trusted sites** zone and set *Medium* or *Medium-high* as its security level (see Figure 2.15).



Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

Security level for this zone

Allowed levels for this zone: All

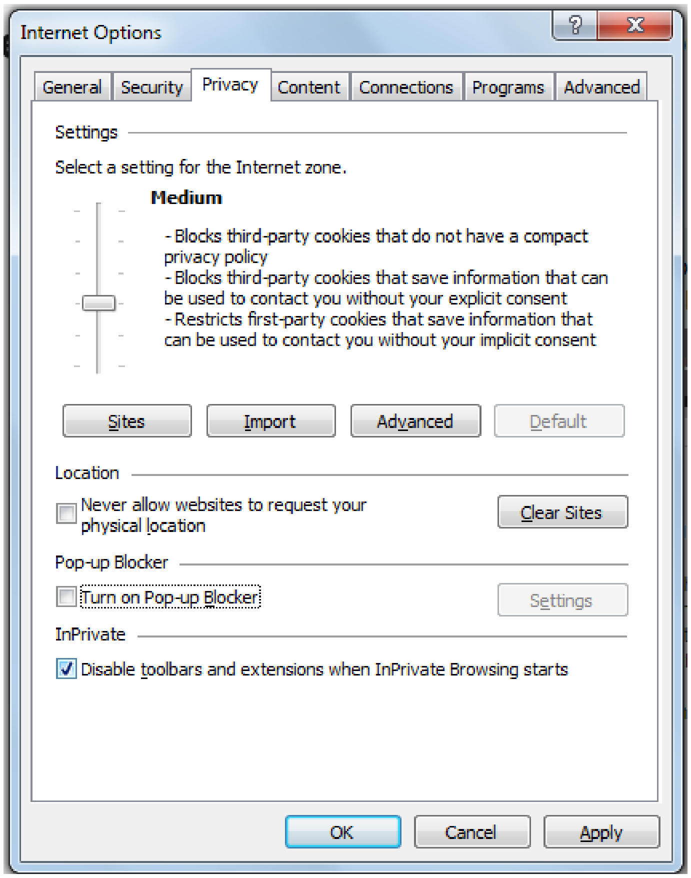
Medium

- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

□ Enable Protected Mode (requires restarting Internet Explorer)

Figure 2.15: Changing the security settings of the Trusted sites zone

- Next, select the **Privacy** tab page. Use the slider in the **Settings** section of the tab page to set the privacy level at *Medium* or *Medium-high* (see Figure 2.16).



Settings

Select a setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that save information that can be used to contact you without your explicit consent
- Restricts first-party cookies that save information that can be used to contact you without your implicit consent

Location

□ Never allow websites to request your physical location

Pop-up Blocker

□ Turn on Pop-up Blocker

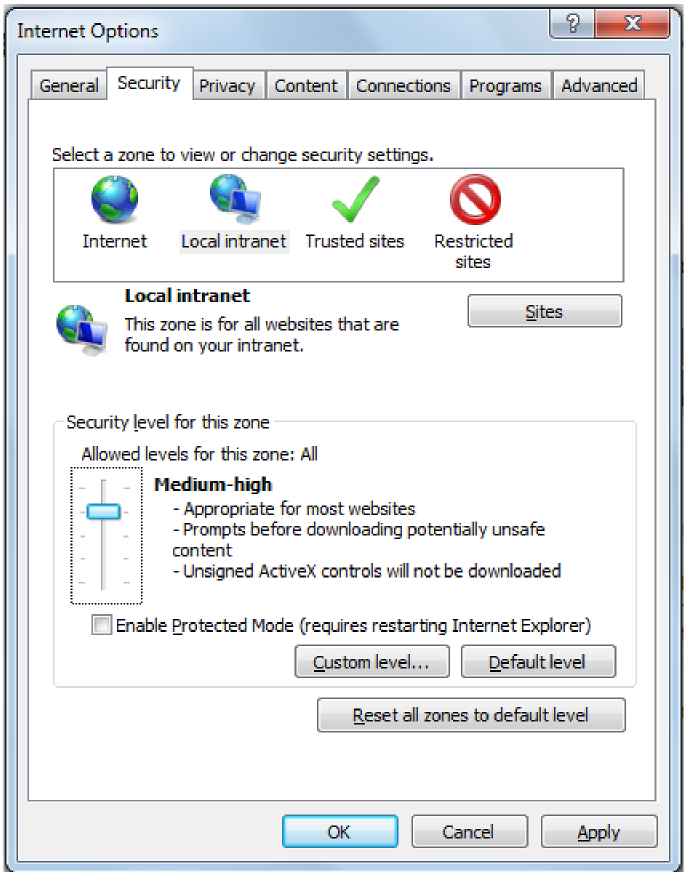
InPrivate

☑ Disable toolbars and extensions when InPrivate Browsing starts

Figure 2.16: Changing privacy settings

3. On the other hand, if your eG manager will be accessed by intranet users only, then, security settings should be configured for the **Local Intranet** and **Trusted Sites** zones. For this, follow the steps detailed below:

   - Pick the **Local intranet** zone and set *Medium* or *Medium-high* as its security level (see Figure 2.17).



Select a zone to view or change security settings.

Local intranet

This zone is for all websites that are found on your intranet.

Security level for this zone

Allowed levels for this zone: All

Medium-high

- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

□ Enable Protected Mode (requires restarting Internet Explorer)

Figure 2.17: Changing the security level of the Local intranet zone

- Then, select the **Trusted sites** zone and set *Medium* or *Medium-high* as its security level (see Figure 2.15).

4. You can allow pop-ups for all sites accessed using the IE browser, by deselecting the **Turn on Pop-up Blocker** check box in Figure 2.16. If you want pop-ups to be allowed for the eG manager alone, then follow the steps detailed in Section **2.0.4.1.4**

5. Finally, click the **Apply** and **OK** buttons in Figure 2.16 to save the changes.

2.0.4.1.4 Allowing Pop-ups from the eG Manager

For this, do the following:

1. Move your mouse pointer over the **Pop-up Blocker** sub-menu of the **Tools** menu in the IE menu bar (see Figure 2.18), and select the **Pop-up Blocker settings** option therein.

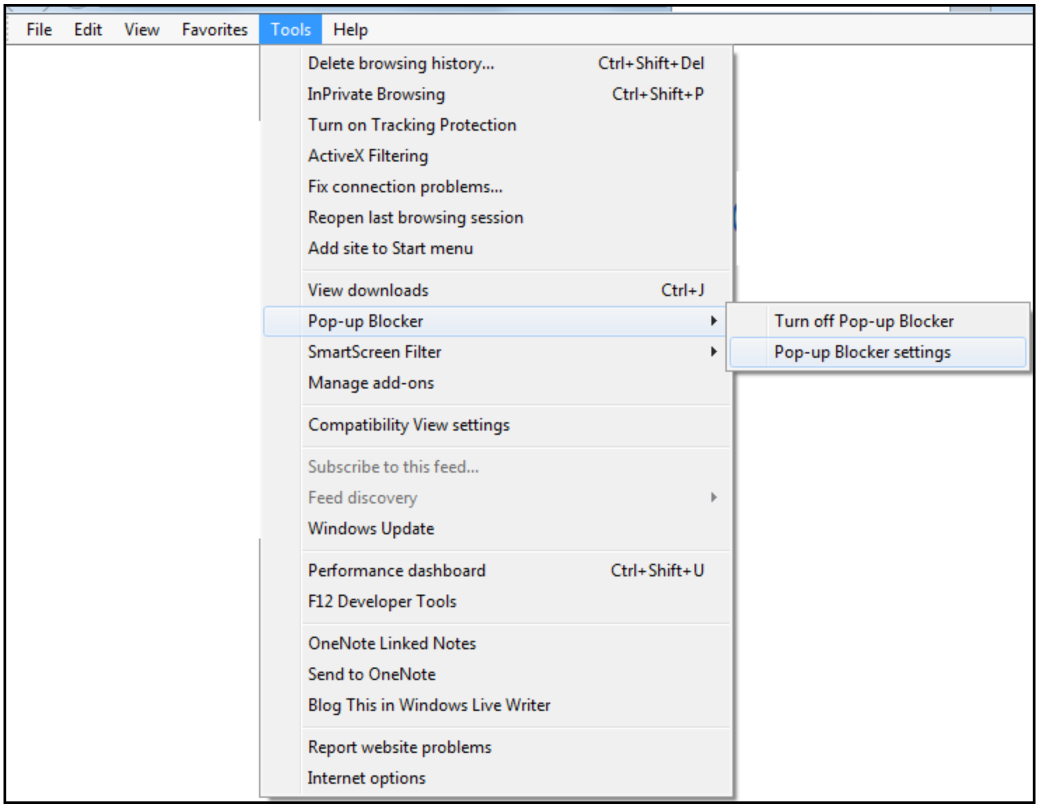
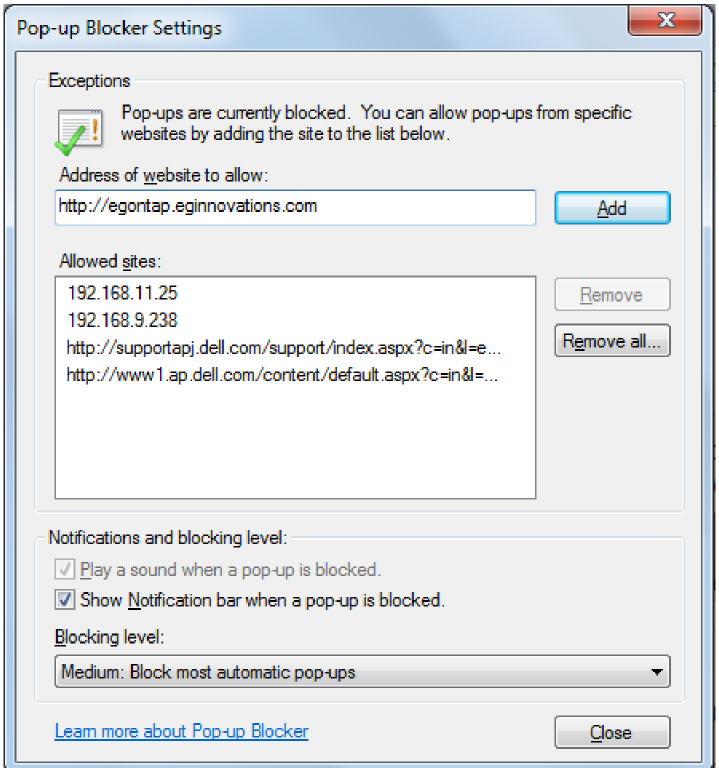


Figure 2.18: Selecting the Pop-up Blocker menu

2. Figure 2.19 will then appear. In the **Address of website to allow** text box, enter the URL of the eG manager for which you want to enable pop-ups. Then, click the **Add** button in Figure 2.19 to add that URL to the **Allowed sites** list.



Exceptions

Pop-ups are currently blocked. You can allow pop-ups from specific websites by adding the site to the list below.

Address of website to allow: http://egontap.eginnovations.com

Allowed sites:

192.168.11.25
192.168.9.238
http://supportapj.dell.com/support/index.aspx?c=in&l=e...
http://www1.ap.dell.com/content/default.aspx?c=in&l=...

Notifications and blocking level:

☑ Play a sound when a pop-up is blocked.
☑ Show Notification bar when a pop-up is blocked.

Blocking level: Medium: Block most automatic pop-ups

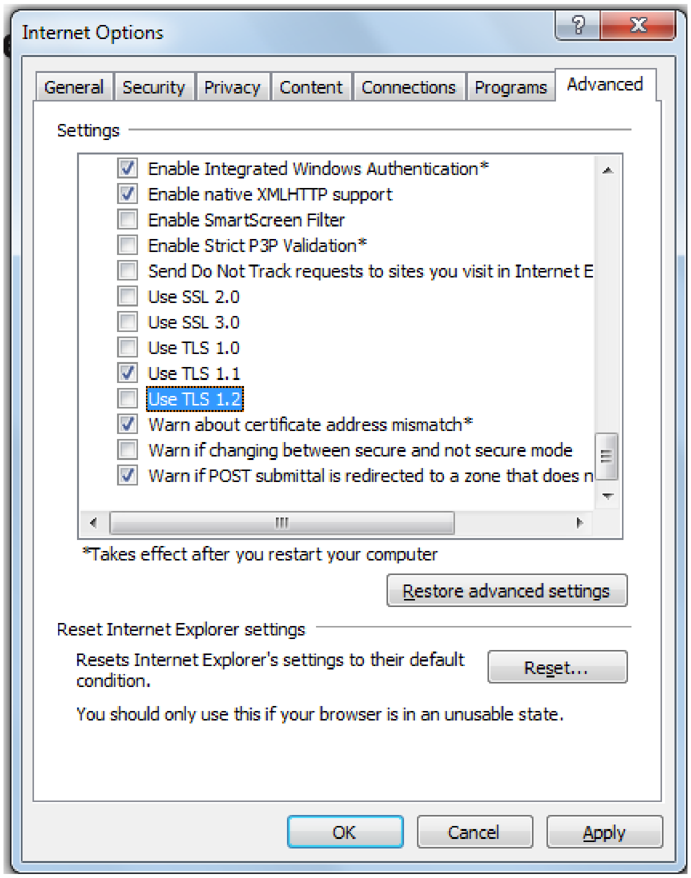
Figure 2.19: Allowing pop-up for the eG manager

3. Finally, click the **Close** button to save the changes.

2.0.4.1.5 Configuring the Browser to Use TLS and not SSL

For this, follow the steps below:

1. Click on the **Tools** icon in the IE tool bar, and select **Internet Options** from the menu that pops up (see Figure 2.9).
2. When Figure 2.10 appears, select the **Advanced** tab page therein. Scroll down the **Settings** list in the **Advanced** tab page until you view the **Use TLS** and **Use SSL** options.



☑ Enable Integrated Windows Authentication*
☑ Enable native XMLHTTP support
□ Enable SmartScreen Filter
□ Enable Strict P3P Validation*
□ Send Do Not Track requests to sites you visit in Internet E
□ Use SSL 2.0
□ Use SSL 3.0
□ Use TLS 1.0
☑ Use TLS 1.1
□ Use TLS 1.2
☑ Warn about certificate address mismatch*
□ Warn if changing between secure and not secure mode
☑ Warn if POST submittal is redirected to a zone that does n

*Takes effect after you restart your computer

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

Figure 2.20: Enabling TLS and disabling SSL

3. Then, deselect the **Use SSL 2.0** and **Use SSL 3.0** check boxes. Instead, select either the **Use TLS 1.1** or the **Use TLS 1.2** check box.
4. Finally, click the **Apply** and **OK** buttons in Figure 2.20 to save the changes.

2.0.4.2 Chrome Settings

To be able to use Chrome as the browser for the eG manager, the following pre-requisites should be fulfilled:

- The security settings should be set to Medium or Medium-High.
- Configure the browser to use TLS and not SSL.

Each of these requirements have been detailed in the sub-sections that follow.

2.0.4.2.1 Changing Security Settings

To make these changes, follow the steps below:

1. Click on the ≡ icon in the Chrome tool bar, and select **Settings** from the menu that pops up (see Figure 2.21).

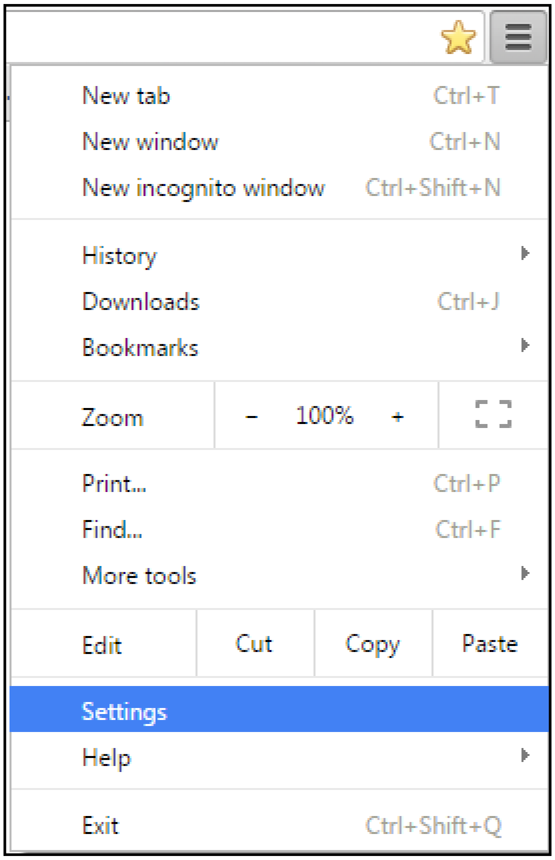
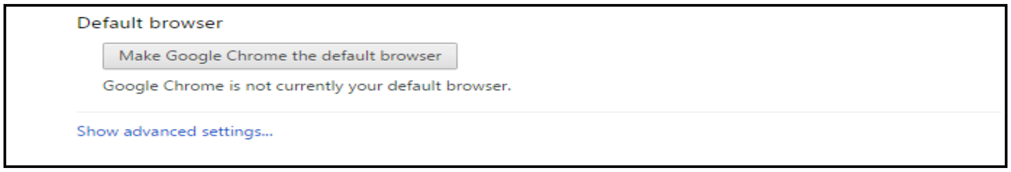


Figure 2.21: Selecting the Settings option from the Chrome menu

2. Scroll down the **Settings** page that then appears until you find the **Show advanced settings** link (see Figure 2.22). Then, click on the link.


Default browser

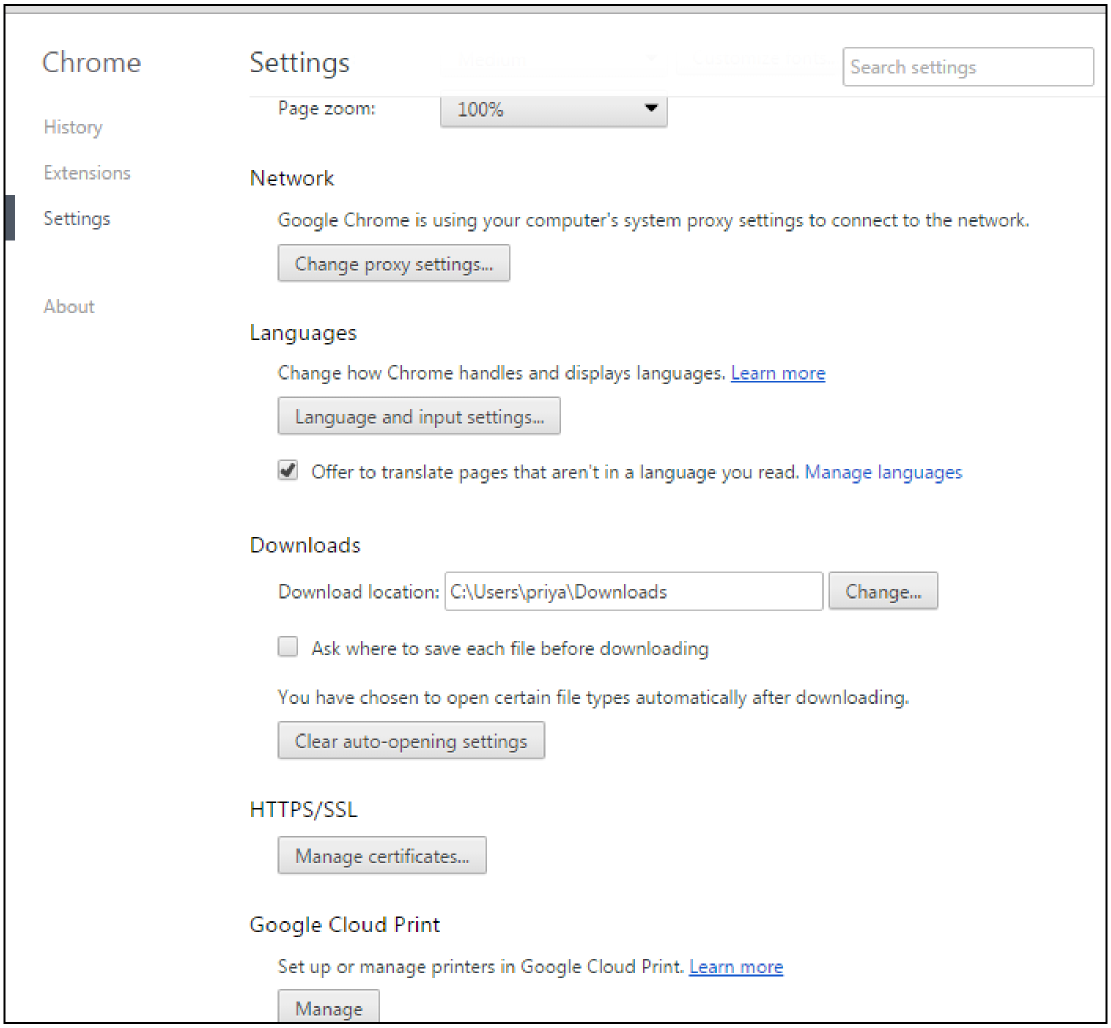
Make Google Chrome the default browser

Google Chrome is not currently your default browser.

Show advanced settings...

Figure 2.22: Clicking the show advanced settings list

3. This will display more settings in the **Settings** page. Scroll down further until you reach the **Network** section. Click the **Change proxy settings** button in that section.



Chrome

History

Extensions

Settings

About

Settings

Search settings

Page zoom: 100%

Network

Google Chrome is using your computer's system proxy settings to connect to the network.

Change proxy settings...

Languages

Change how Chrome handles and displays languages. Learn more

Language and input settings...

☑ Offer to translate pages that aren't in a language you read. Manage languages

Downloads

Download location: C:\Users\priya\Downloads Change...

☐ Ask where to save each file before downloading

You have chosen to open certain file types automatically after downloading.

Clear auto-opening settings

HTTPS/SSL

Manage certificates...

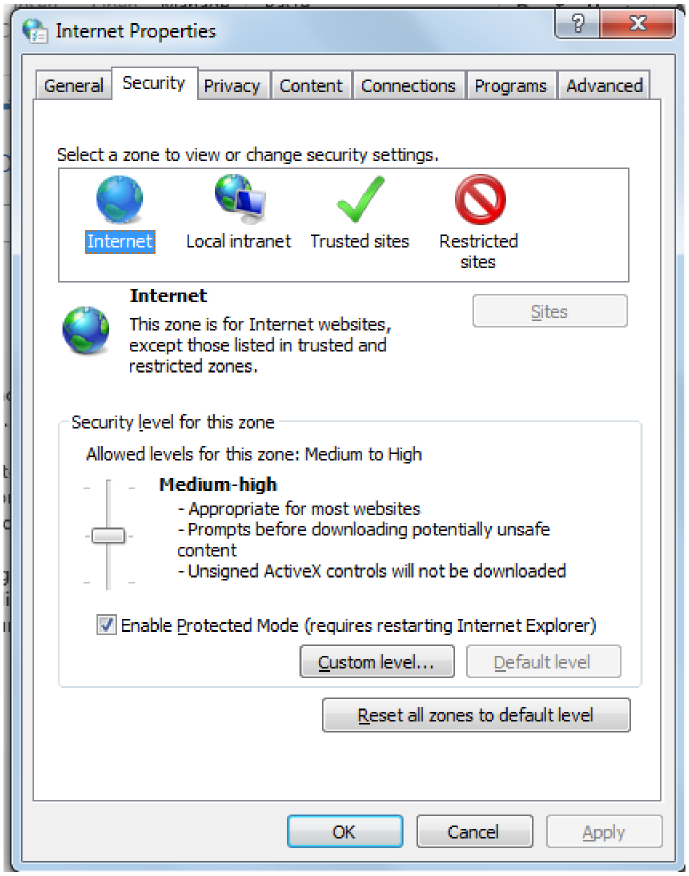
Google Cloud Print

Set up or manage printers in Google Cloud Print. Learn more

Manage

Figure 2.23: Clicking the Change proxy settings button

4. When the **Internet Properties** dialog appears, select the **Security** tab page therein. Next, pick **Internet** from the **Select a zone…** section (see Figure 2.24).



Select a zone to view or change security settings.

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

Allowed levels for this zone: Medium to High

Medium-high

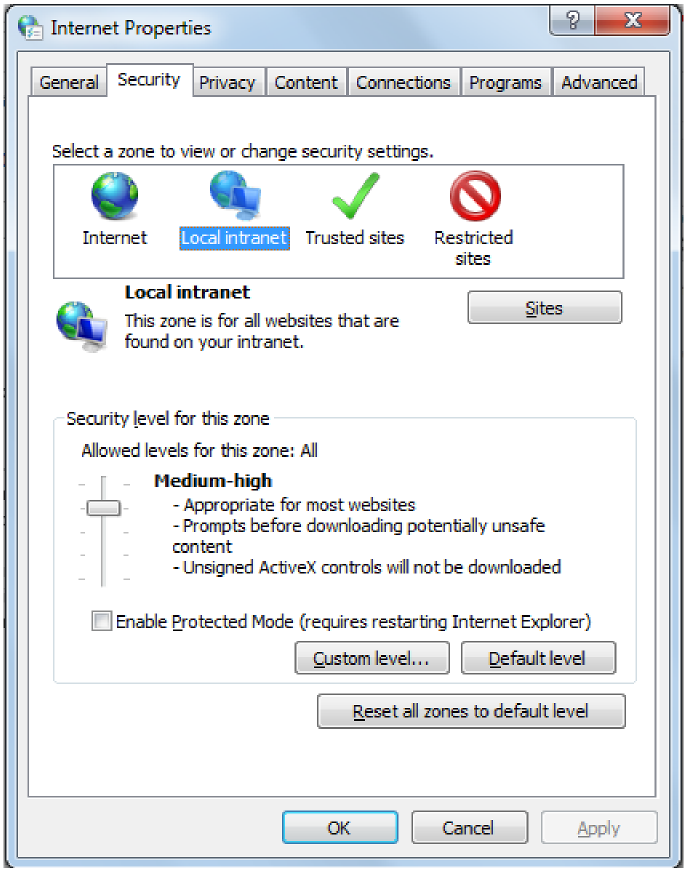
- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☑ Enable Protected Mode (requires restarting Internet Explorer)

Figure 2.24: Changing the security level of the Internet zone

5. Use the slider in the **Security level for this zone** section to set the security level at *Medium* or *Medium-high*.

6. Then, pick the **Local intranet** zone and set *Medium* or *Medium-high* as its security level (see Figure 2.25).



Select a zone to view or change security settings.

Local intranet

This zone is for all websites that are found on your intranet.

Security level for this zone

Allowed levels for this zone: All

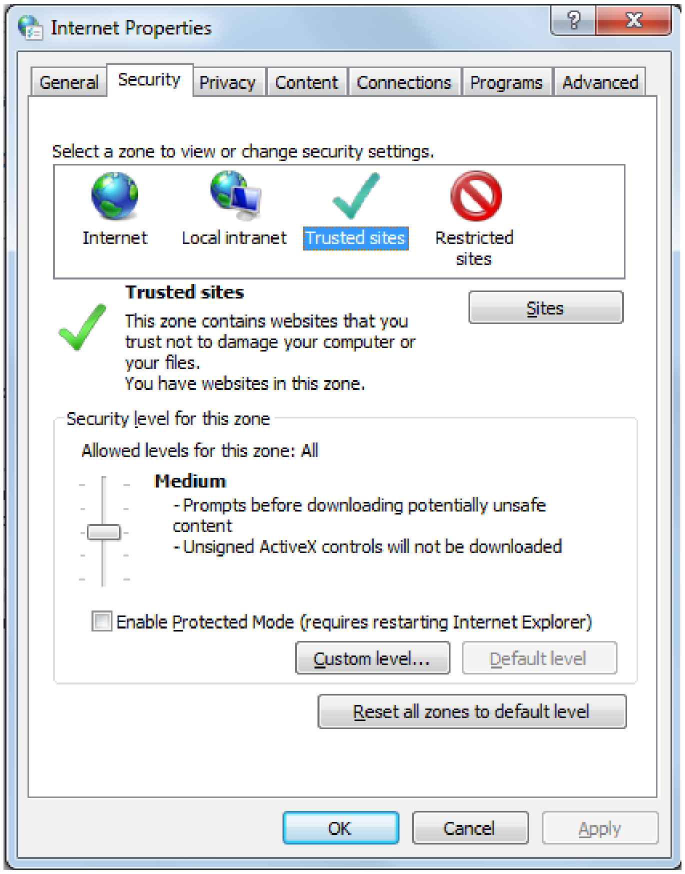
Medium-high

- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

□ Enable Protected Mode (requires restarting Internet Explorer)

Figure 2.25: Changing the security level of the Local intranet zone

7. Then, select the **Trusted sites** zone and set *Medium* or *Medium-high* as its security level (see Figure 2.26).



Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

Security level for this zone

Allowed levels for this zone: All

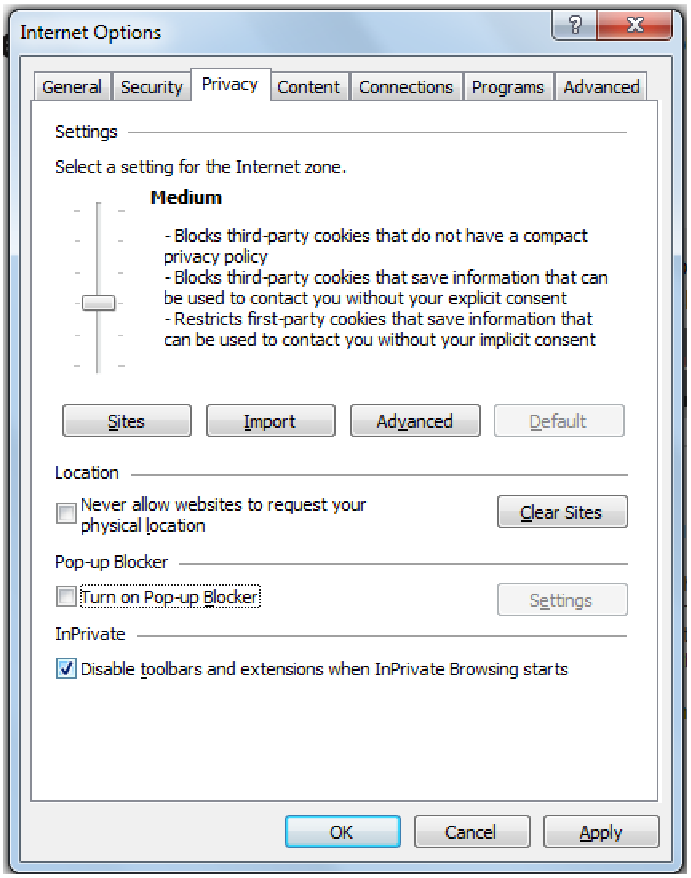
Medium

- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

□ Enable Protected Mode (requires restarting Internet Explorer)

Figure 2.26: Changing the security settings of the Trusted sites zone

8. Then, select the **Privacy** tab page. Use the slider in the **Settings** section of the tab page to set the privacy level at *Medium* or Medium-high (see Figure 2.27).



Settings

Select a setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that save information that can be used to contact you without your explicit consent
- Restricts first-party cookies that save information that can be used to contact you without your implicit consent

Location

□ Never allow websites to request your physical location

Pop-up Blocker

□ Turn on Pop-up Blocker

InPrivate

☑ Disable toolbars and extensions when InPrivate Browsing starts

Figure 2.27: Changing privacy settings

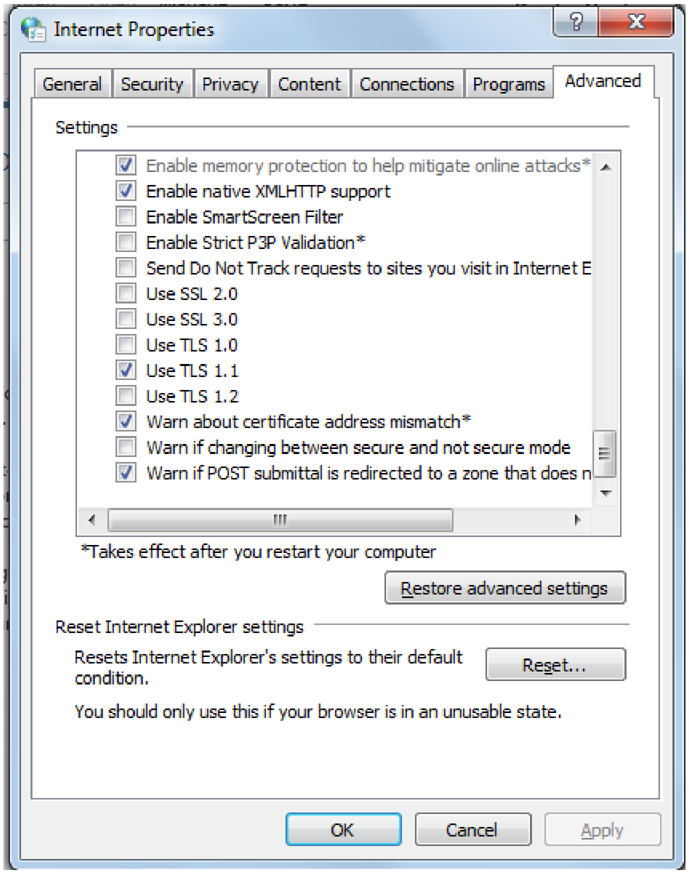
9. Finally, click the **Apply** and **OK** buttons in Figure 2.27 to save the changes.

2.0.4.2.2 Configuring the Browser to Use TLS and not SSL

For this, follow the steps below:

1. Click on the ☰ icon in the Chrome tool bar, and select **Settings** from the menu that pops up (see Figure 2.21).
2. Scroll down the **Settings** page that then appears until you find the **Show advanced settings** link (see Figure 2.22). Then, click on the link.
3. This will display more settings in the **Settings** page. Scroll down further until you reach the **Network** section. Click the **Change proxy settings** button in that section.
4. When the **Internet Properties** dialog appears, select the **Advanced** tab page therein. Scroll down the **Settings** list in the **Advanced** tab page until you view the **Use TLS** and **Use SSL**

options.



- ☑ Enable memory protection to help mitigate online attacks*
- ☑ Enable native XMLHTTP support
- □ Enable SmartScreen Filter
- □ Enable Strict P3P Validation*
- □ Send Do Not Track requests to sites you visit in Internet E
- □ Use SSL 2.0
- □ Use SSL 3.0
- □ Use TLS 1.0
- ☑ Use TLS 1.1
- □ Use TLS 1.2
- ☑ Warn about certificate address mismatch*
- □ Warn if changing between secure and not secure mode
- ☑ Warn if POST submittal is redirected to a zone that does n

*Takes effect after you restart your computer

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

Figure 2.28: Enabling TLS and disabling SSL

5. Then, deselect the **Use SSL 2.0** and **Use SSL 3.0** check boxes. Instead, select either the **Use TLS 1.1** or the **Use TLS 1.2** check box.

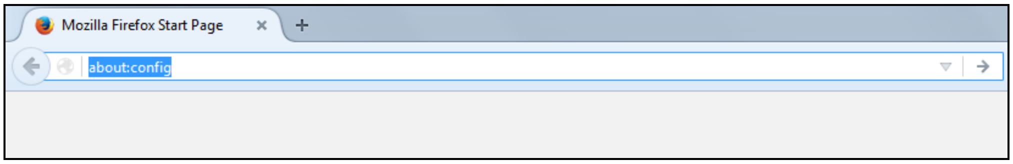
6. Finally, click the **Apply** and **OK** buttons in Figure 2.28 to save the changes.

2.0.4.3 Mozilla Firefox Settings

In Mozilla Firefox, SSL v3 is disabled by default. Therefore, all you need to do before engaging Firefox as your browser for the eG manager is to enable TLS 1.1 or TLS 1.2. For this, follow the steps below:

1. Launch the Mozilla Firefox browser.

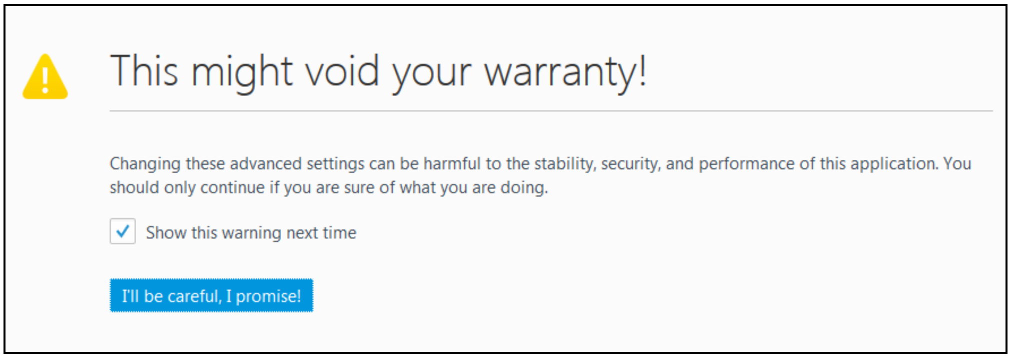
2. In the **Search** bar of the browser, type *about:config*.



about:config

Figure 2.29: Typing about:config in the Search bar

3. The warning message depicted by Figure 2.29 will then appear.



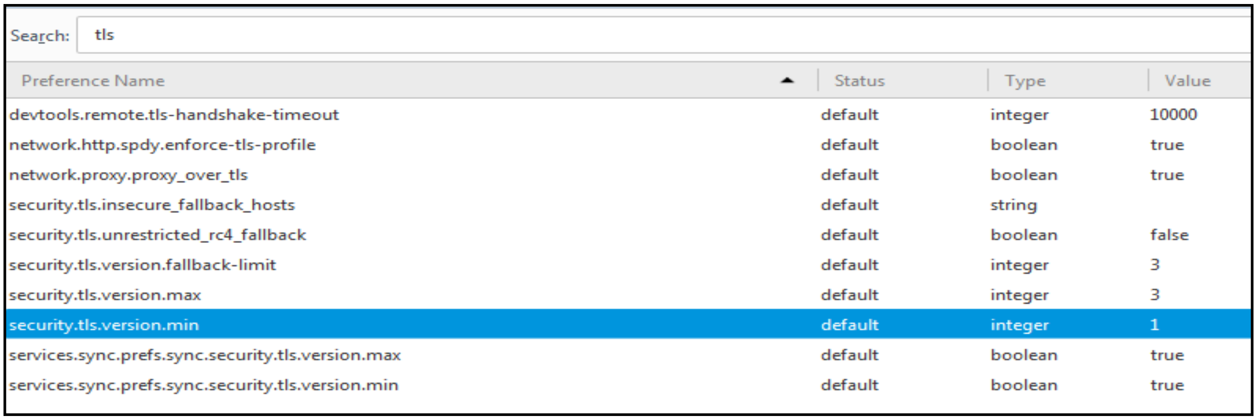
This might void your warranty!

Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.

☑ Show this warning next time

Figure 2.30: The warning message that appears in the Firefox browser

4. Click the **I'll be careful, I promise!** button in Figure 2.30. Figure 2.31 will appear. Here, select the **security.tls.version.min** preference.

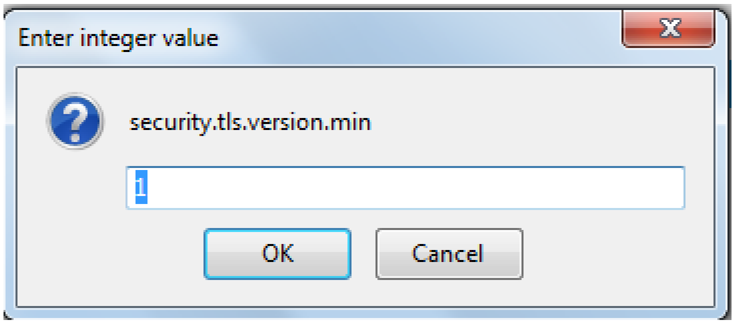


Search: tls

Preference Name	Status	Type	Value
devtools.remote.tls-handshake-timeout	default	integer	10000
network.http.spdy.enforce-tls-profile	default	boolean	true
network.proxy.proxy_over_tls	default	boolean	true
security.tls.insecure_fallback_hosts	default	string	
security.tls.unrestricted_rc4_fallback	default	boolean	false
security.tls.version.fallback-limit	default	integer	3
security.tls.version.max	default	integer	3
security.tls.version.min	default	integer	1
services.sync.prefs.sync.security.tls.version.max	default	boolean	true
services.sync.prefs.sync.security.tls.version.min	default	boolean	true

Figure 2.31: Locating the security.tls.version.min option

5. Check whether the value of this preference is 1. If not, double-click on the preference. Figure 2.32 will appear. Type **1** in the text box that appears next, and click the **OK** button therein (see Figure 2.32).


Enter integer value

security.tls.version.min

1

Figure 2.32: Setting the value of the security.tls.version.min preference

2.1 eG Manager on Windows

This section describes the steps involved in installing and configuring eG Enterprise on Windows operating systems. Installing and configuring the eG manager can be achieved in a single stage in Windows environments. The various factors that need to be considered while installing the eG manager as well as the components that make up the manager have been described in Where to locate the eG Manager?.

Note:

- Administrator privileges are required to perform this installation.
- Before proceeding with the installation process, please go to "*Control Panel-> Display->Settings*" and set the number of colors to **65536** at least. This is the optimal DISPLAY setting in the computer to view the eG user interface well.

The steps for deploying installing and configuring the eG manager on Windows platforms are discussed in the following topics:

- Section **Chapter 2**
- Section **2.1.1**

2.1.1 Installing and Configuring the eG Manager on Windows

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

1. Section **2.1.1.1**
2. Section **2.1.1.2**
3. Section **2.1.1.3**

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:

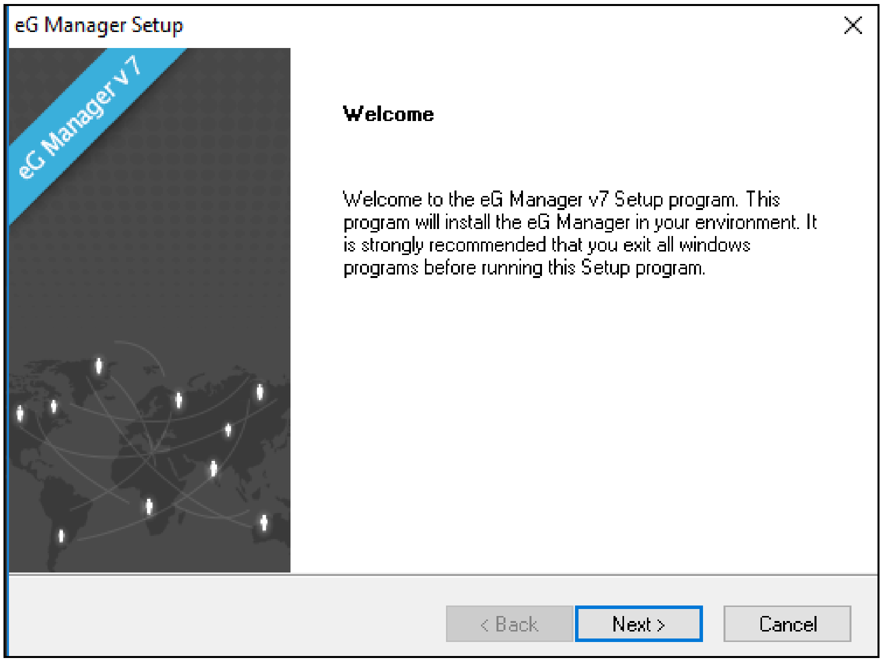
- The **eGManager_win2008_x64.exe**, if you are installing the eG manager on a 64-bit Windows 2008/Windows 7 host;
- The **eGManager_win2012_x64.exe**, if you are installing the eG manager on a 64-bit Windows 8/Windows 2012 host;
- The **eGManager_win2016_x64.exe**, if you are installing the eG manager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

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

2.1.1.1 Installing the eG Manager

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.

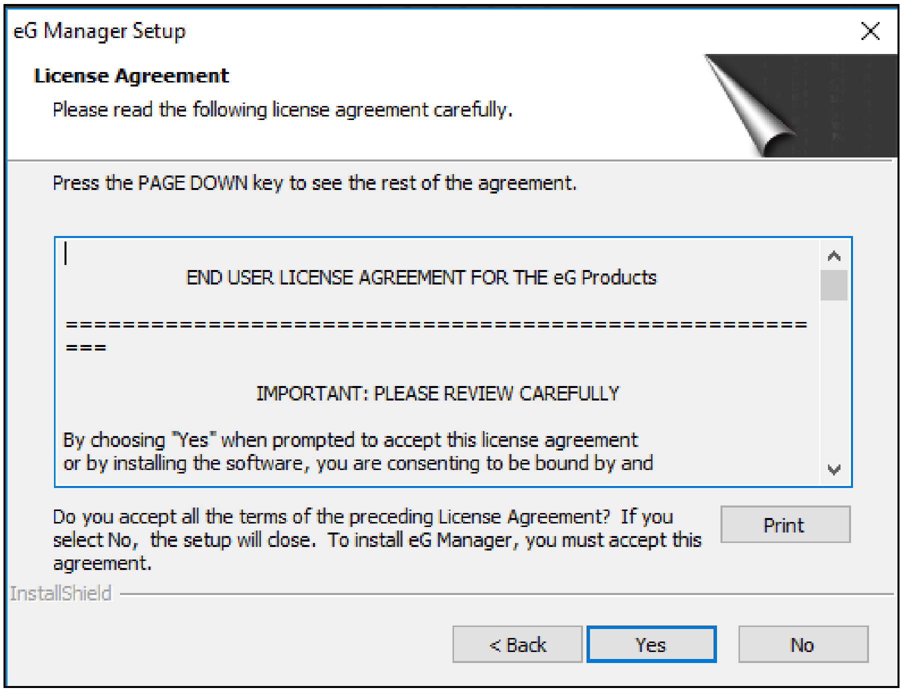


Welcome

Welcome to the eG Manager v7 Setup program. This program will install the eG Manager in your environment. It is strongly recommended that you exit all windows programs before running this Setup program.

Figure 2.33: The Welcome screen of the installation wizard

2. Accept the license agreement that follows by clicking the **Yes** button therein (see Figure 2.34).



eG Manager Setup

License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

END USER LICENSE AGREEMENT FOR THE eG Products

===
===

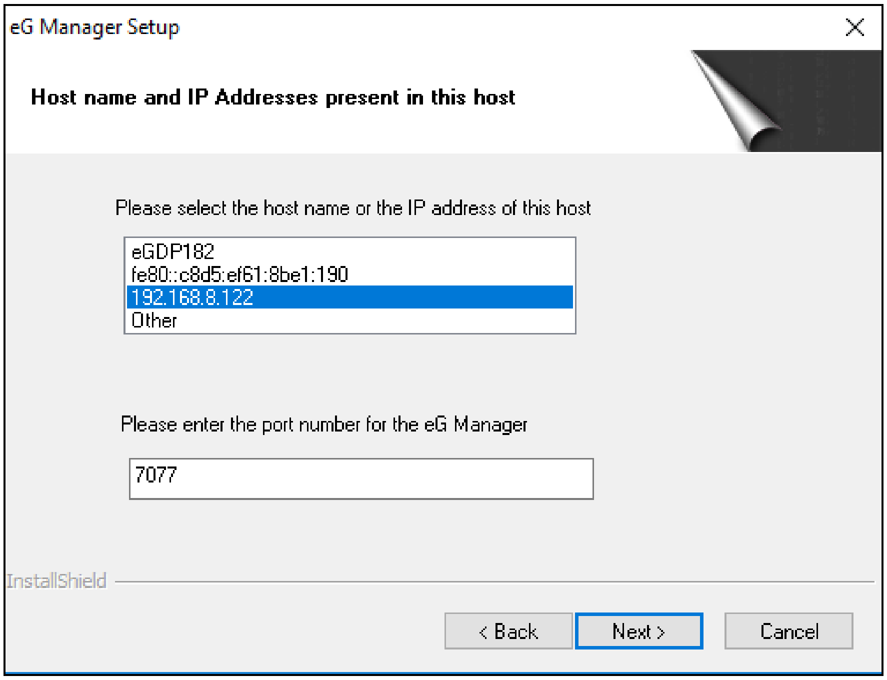
IMPORTANT: PLEASE REVIEW CAREFULLY

By choosing "Yes" when prompted to accept this license agreement
or by installing the software, you are consenting to be bound by and

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install eG Manager, you must accept this agreement.

Figure 2.34: Accepting the license agreement for installing the eG manager

3. The setup process now requires the hostname and port number of the host on which the eG manager is being configured (see 2.1.1). By default, setup auto-discovers the host name and the IP address(es) of the eG manager host, and makes it available for selection in 2.1.1. You can pick the host name or any of the IP addresses listed therein to take the eG manager installation forward. If the IP address/host name that you want to use for your eG manager is not discovered for some reason, then, you can choose the **Other** option in 2.1.1. This will invoke Figure 2.36 where you can manually specifiy the IP address/host name of the eG manager. 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.



Host name and IP Addresses present in this host

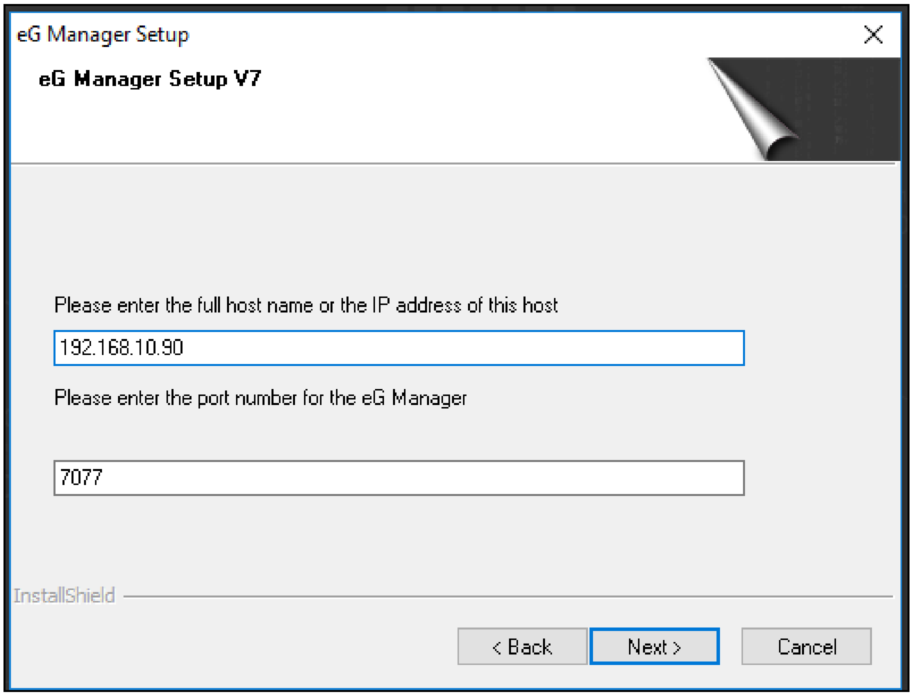
Please select the host name or the IP address of this host

eGDP182
fe80::c8d5:ef61:8be1:190
192.168.8.122
Other

Please enter the port number for the eG Manager

7077

Figure 2.35: Selecting the IP address/host name to use for the eG manager



eG Manager Setup V7

Please enter the full host name or the IP address of this host

192.168.10.90

Please enter the port number for the eG Manager

7077

Figure 2.36: Hostname and port number of the system on which the eG manager will execute

Note:

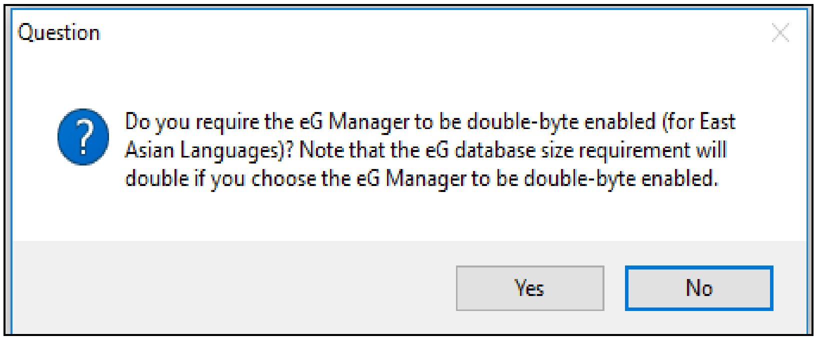
- While specifying the host name/IP address of the manager, please take care of the following aspects:

   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 manager, note that only an IPv4 address can be provided. To configure the eG manager 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 2.36.

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 manager should be explicitly configured to display and process double-byte characters. In such a case, enable double-byte support for the eG manager 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 manager need not be double-byte enabled. At such times, click the **No** button to disable double-byte support for the eG manager.


Question

Do you require the eG Manager to be double-byte enabled (for East Asian Languages)? Note that the eG database size requirement will double if you choose the eG Manager to be double-byte enabled.

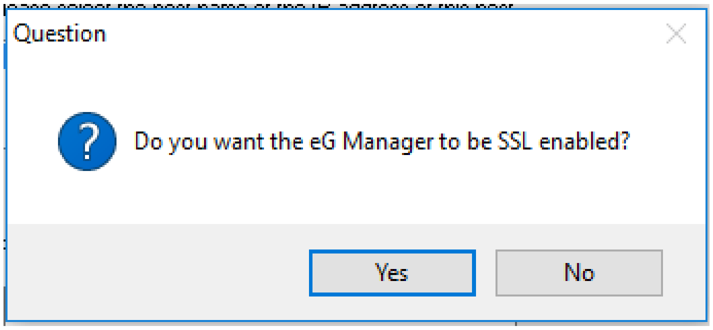
Figure 2.37: Enabling double-byte support for the eG manager

Note:

For a detailed discussion on how to enable double-byte support for eG Enterprise, refer to Section **2.9**.

5. Setup then prompts you to indicate if the eG manager is to be SSL-enabled. If so, click **Yes**. If not,

click **No**.

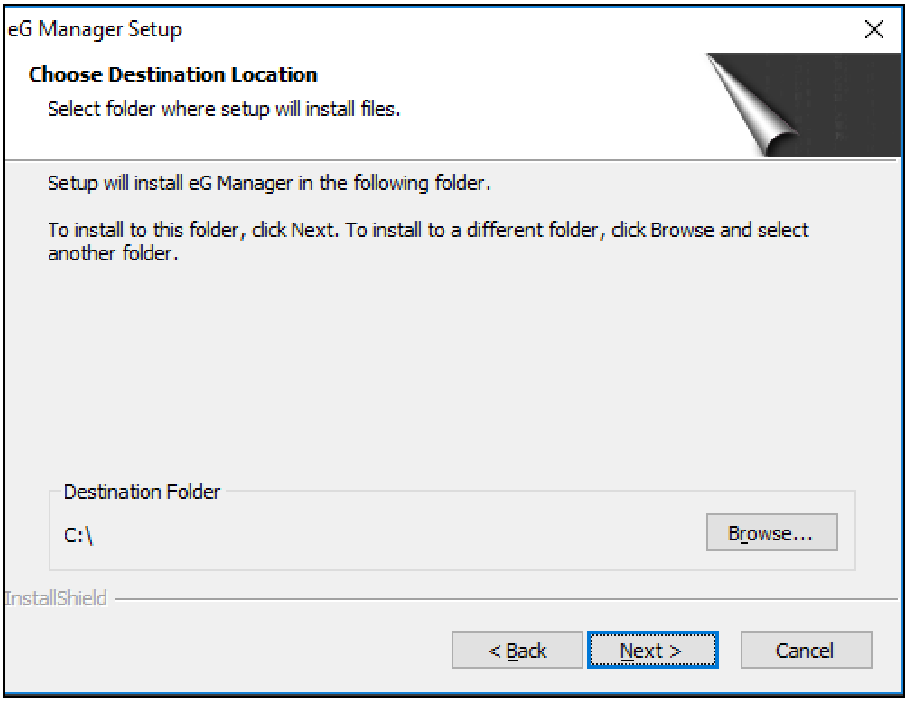


Question

Do you want the eG Manager to be SSL enabled?

Figure 2.38: Indicating whether/not to SSL-enable the eG manager

6. Next, indicate where the eG manager is to be installed. By default, setup installs the eG manager in the C drive. If you want the eG manager installed in a different directory, use the **Browse** button in Figure 2.39. Then, click the **Next** button in Figure 2.39 to move to the next step.



eG Manager Setup

Choose Destination Location

Select folder where setup will install files.

Setup will install eG Manager in the following folder.

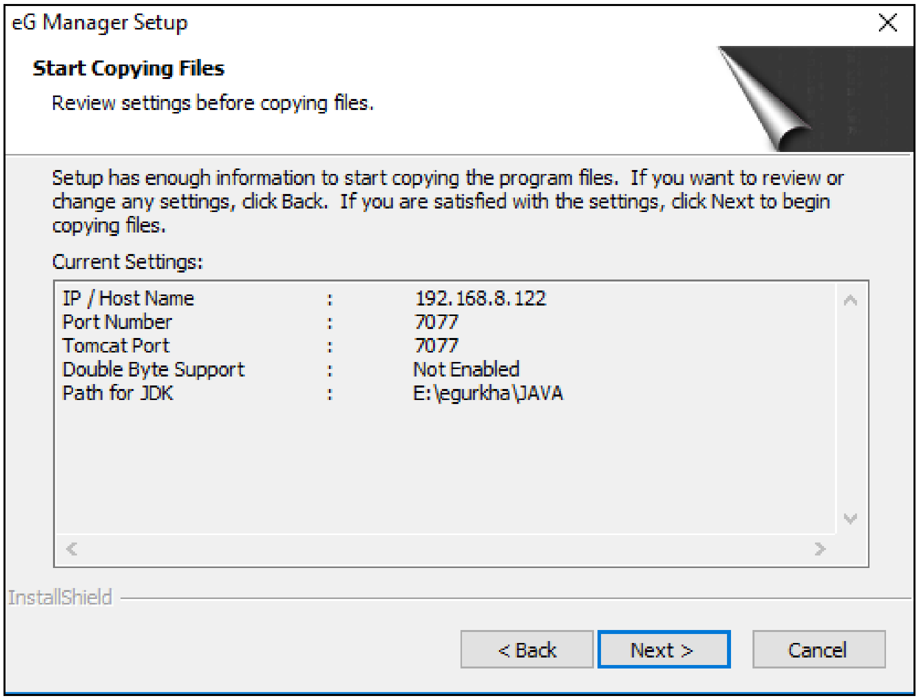
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\

Figure 2.39: Specifying the location of the eG manager

7. Figure 2.40 then appears, using which you can quickly review your install specifications. To proceed, click the Next button in Figure 2.40.



Start Copying Files

Review settings before copying files.

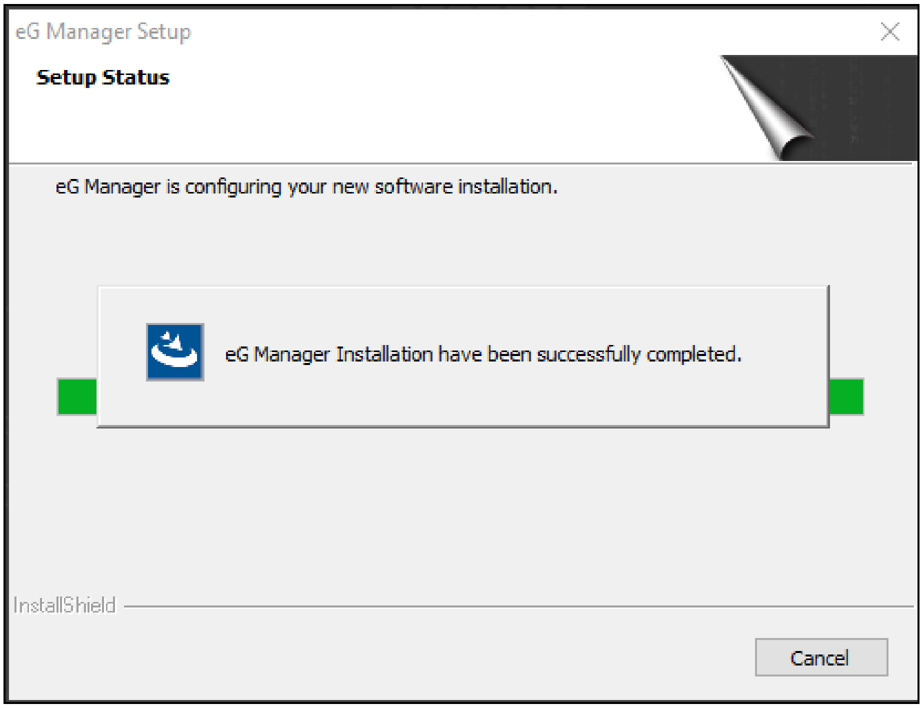
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
IP / Host Name          :        192.168.8.122
Port Number             :        7077
Tomcat Port             :        7077
Double Byte Support     :        Not Enabled
Path for JDK            :        E:\egurkha\JAVA
```

Figure 2.40: Reviewing the install settings

8. This will begin the eG manager installation. During this process, setup automatically extracts and deploys the built-in JDK - OpenJDK 12 - for the eG manager's use. Additionally, setup also automatically configures and readies the built-in Apache Tomcat server, so that the eG manager can service web requests to it efficiently. Once the installation completes successfully, the message depicted by Figure 2.41 will appear.



eG Manager is configuring your new software installation.

eG Manager Installation have been successfully completed.

Figure 2.41: The message confirming the successful eG manager installation

2.1.1.2 Configuring the eG Database

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

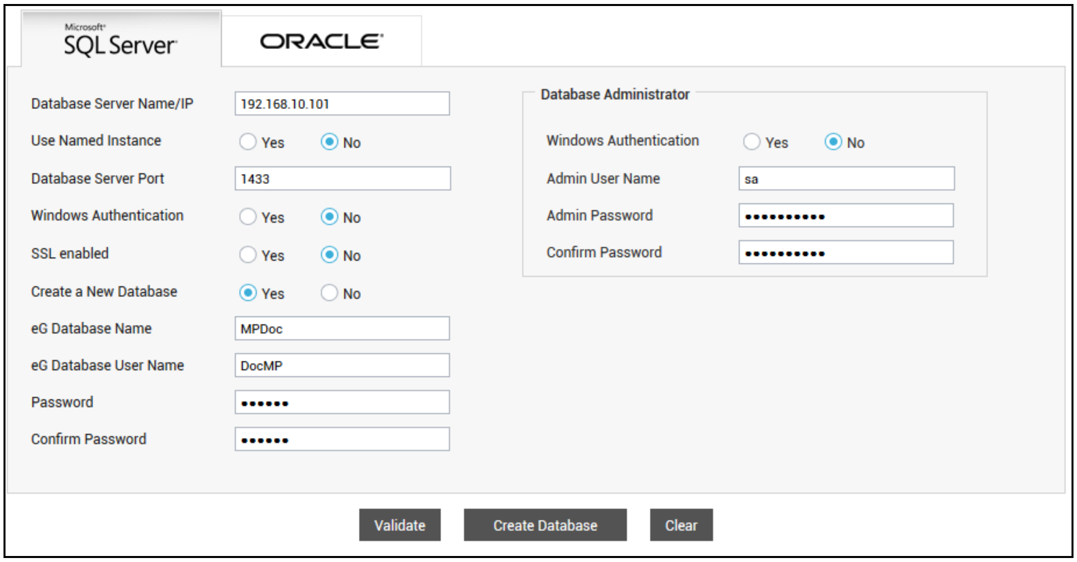
If a SQL database pre-exists on Microsoft Azure, you can configure such a database as the eG database. On the other hand, if a Microsoft Azure SQL database is not in use in your environment, then it is essential to ensure that an Oracle / Microsoft SQL server is available to host the eG database. Such a database server can either reside on the eG manager 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 manager. Using this web page, you can pick a backend for the eG manager, 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 2.42).



Database Server Name/IP	192.168.10.101
Use Named Instance	○ Yes ● No
Database Server Port	1433
Windows Authentication	○ Yes ● No
SSL enabled	○ Yes ● No
Create a New Database	● Yes ○ No
eG Database Name	MPDoc
eG Database User Name	DocMP
Password	••••••
Confirm Password	••••••

Database Administrator

Windows Authentication	○ Yes ● No
Admin User Name	sa
Admin Password	•••••••••••
Confirm Password	•••••••••••

Figure 2.42: 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 2.42:

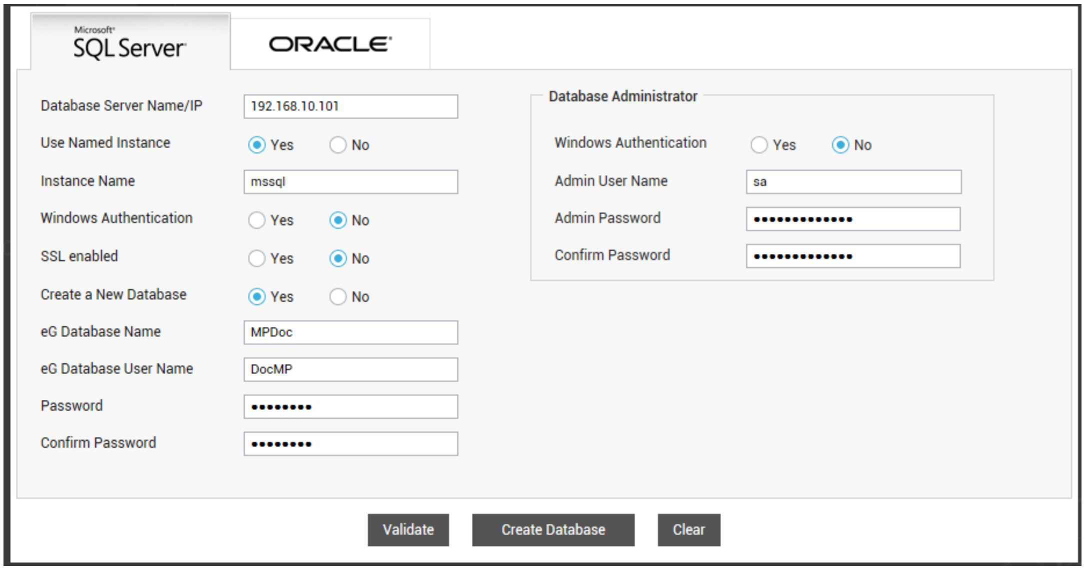
1. First, enter the location of the Microsoft SQL server by specifying the hostname and port on which the server is hosted against **Database Server Name/IP**. If you have already configured a SQL database on Microsoft Azure and want to use this database as the eG database, then, against **Database Server 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 2.43.



Database Server Name/IP	192.168.10.101	
Use Named Instance	● Yes	○ No
Instance Name	mssql	
Windows Authentication	○ Yes	● No
SSL enabled	○ Yes	● No
Create a New Database	● Yes	○ No
eG Database Name	MPDoc	
eG Database User Name	DocMP	
Password	••••••••	
Confirm Password	••••••••	

Database Administrator

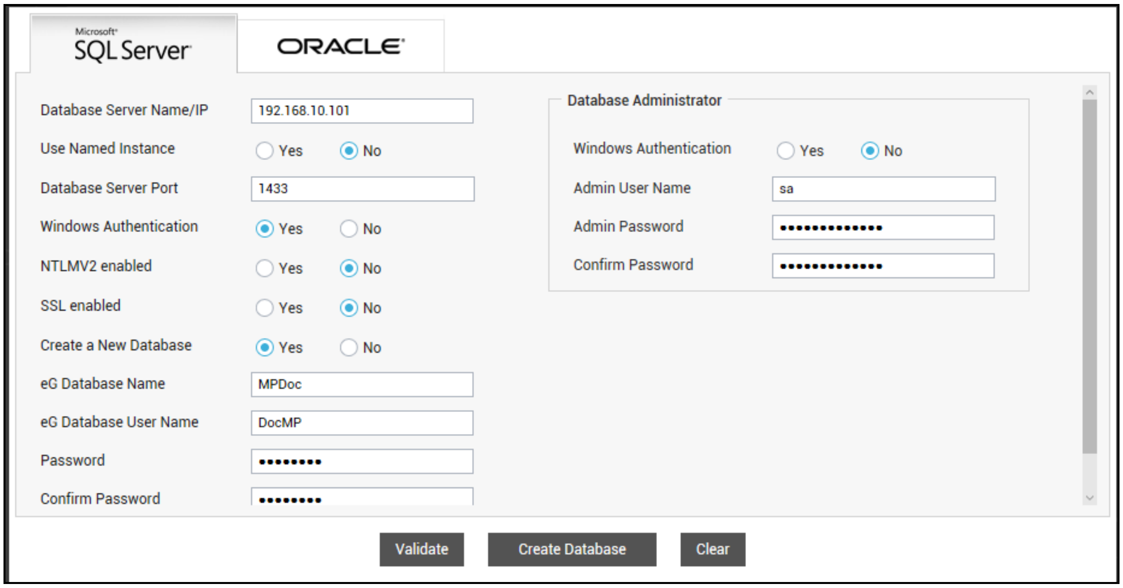
Windows Authentication	○ Yes	● No
Admin User Name	sa	
Admin Password	•••••••••••••	
Confirm Password	•••••••••••••	

Figure 2.43: 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 2.42).

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 2.1.1). 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**.



Database Server Name/IP	192.168.10.101	
Use Named Instance	○ Yes	● No
Database Server Port	1433	
Windows Authentication	● Yes	○ No
NTLMV2 enabled	○ Yes	● No
SSL enabled	○ Yes	● No
Create a New Database	● Yes	○ No
eG Database Name	MPDoc	
eG Database User Name	DocMP	
Password	••••••••	
Confirm Password	••••••••	

Database Administrator

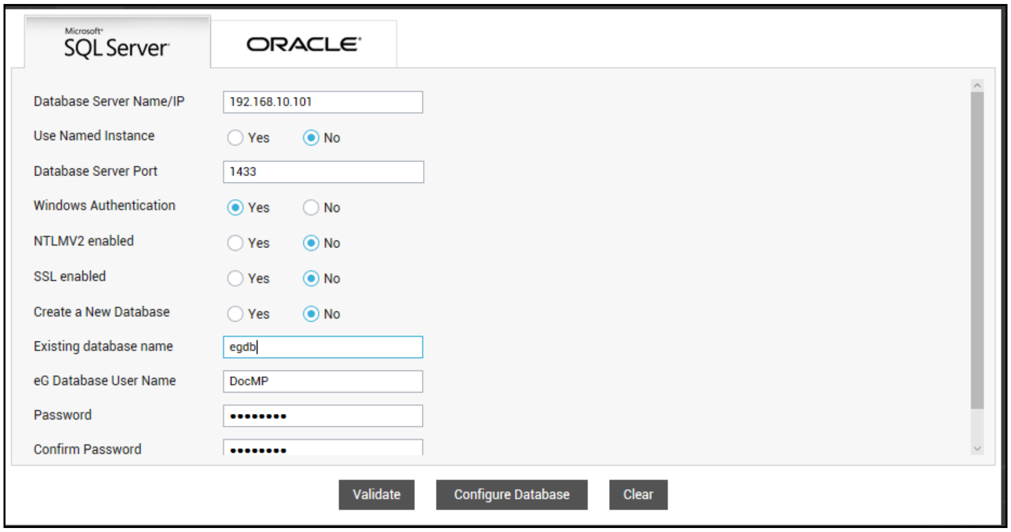
Windows Authentication	○ Yes	● No
Admin User Name	sa	
Admin Password	•••••••••••••	
Confirm Password	•••••••••••••	

Figure 2.44: 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 2.1.1). On the other hand, if the **Create a New Database** flag is set to **No**, then, in the **Existing database name** text box, mention the name of the existing database in which the eG manager will be storing metrics (see 2.1.1). 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**.



Database Server Name/IP	192.168.10.101
Use Named Instance	○ Yes ● No
Database Server Port	1433
Windows Authentication	● Yes ○ No
NTLMV2 enabled	○ Yes ● No
SSL enabled	○ Yes ● No
Create a New Database	○ Yes ● No
Existing database name	egdb
eG Database User Name	DocMP
Password	••••••••
Confirm Password	••••••••

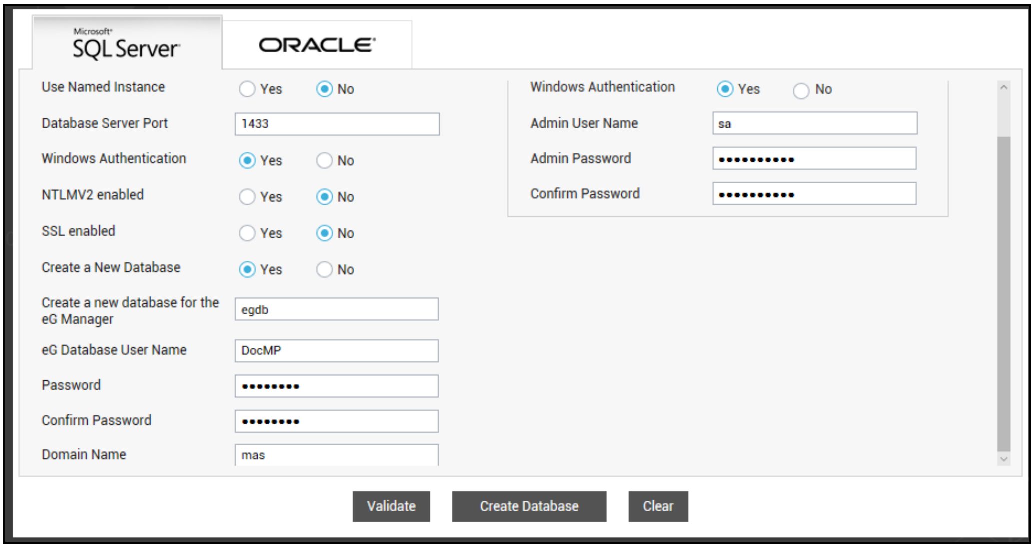
Figure 2.45: Using an existing database on the Microsoft SQL server as the eG database

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 manager - i.e., if you have set the **Create a New Database** flag to **Yes** and have specified a new **eG Database Name** (see 2.1.1) - 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 2.1.1) - 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 2.46).



Use Named Instance ○ Yes ● No

Database Server Port 1433

Windows Authentication ● Yes ○ No

NTLMV2 enabled ○ Yes ● No

SSL enabled ○ Yes ● No

Create a New Database ● Yes ○ No

Create a new database for the eG Manager egdb

eG Database User Name DocMP

Password ••••••••

Confirm Password ••••••••

Domain Name mas

Windows Authentication ● Yes ○ No

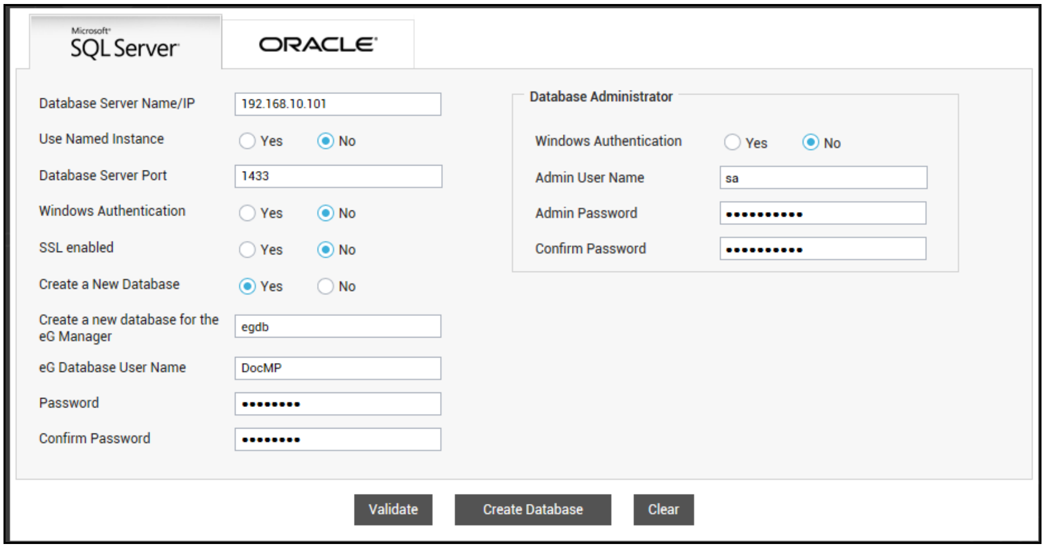
Admin User Name sa

Admin Password ••••••••••

Confirm Password ••••••••••

Figure 2.46: 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 2.47).



Database Server Name/IP 192.168.10.101

Use Named Instance ○ Yes ● No

Database Server Port 1433

Windows Authentication ○ Yes ● No

SSL enabled ○ Yes ● No

Create a New Database ● Yes ○ No

Create a new database for the eG Manager egdb

eG Database User Name DocMP

Password ••••••••

Confirm Password ••••••••

Database Administrator

Windows Authentication ○ Yes ● No

Admin User Name sa

Admin Password ••••••••••

Confirm Password ••••••••••

Figure 2.47: 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

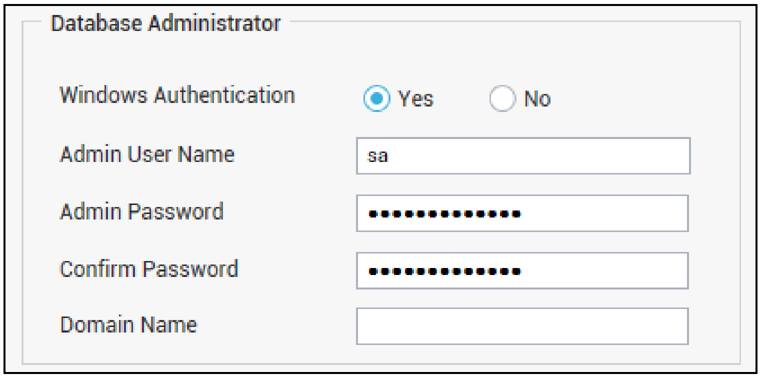
    For instance, if the name of the special database user is **egdb**, then the password that you set for this user should be a **strong password** such as, **db123$%#@**.

    Note that without a ‘strong password’, the eG manager 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 manager in step 7 above , then make sure you configure the **Database Administrator** section in Figure 2.47 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 2.1.1).



Database Administrator

Windows Authentication ● Yes ○ No

Admin User Name: sa

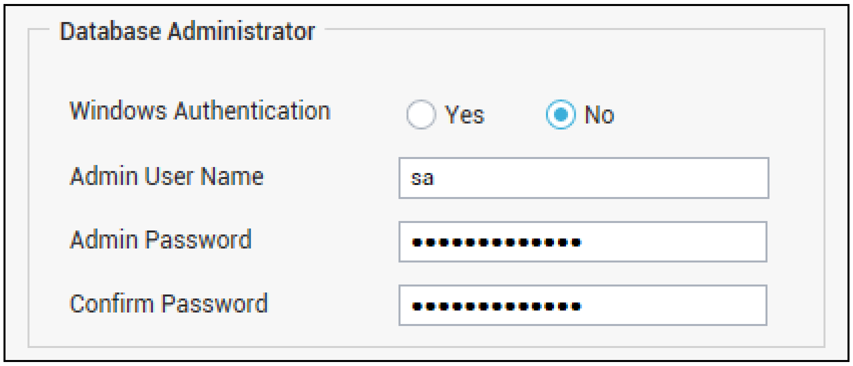
Admin Password: •••••••••••••

Confirm Password: •••••••••••••

Domain Name:

Figure 2.48: 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 2.1.1).



Database Administrator

Windows Authentication ○ Yes ● No

Admin User Name: sa

Admin Password: •••••••••••••

Confirm Password: •••••••••••••

Figure 2.49: 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 2.1.1. Figure 2.50, Figure 2.51, and Figure 2.52 depict how to create a new user with the aforesaid privileges using the **Microsoft SQL Server Management Studio**.

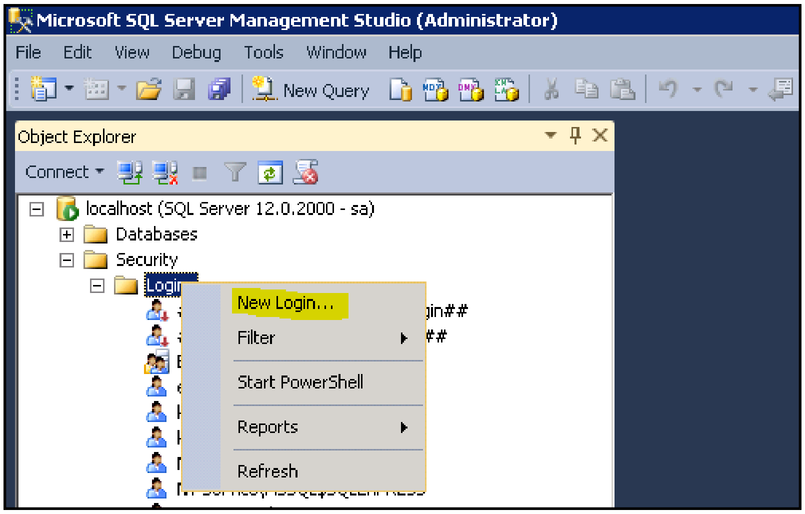
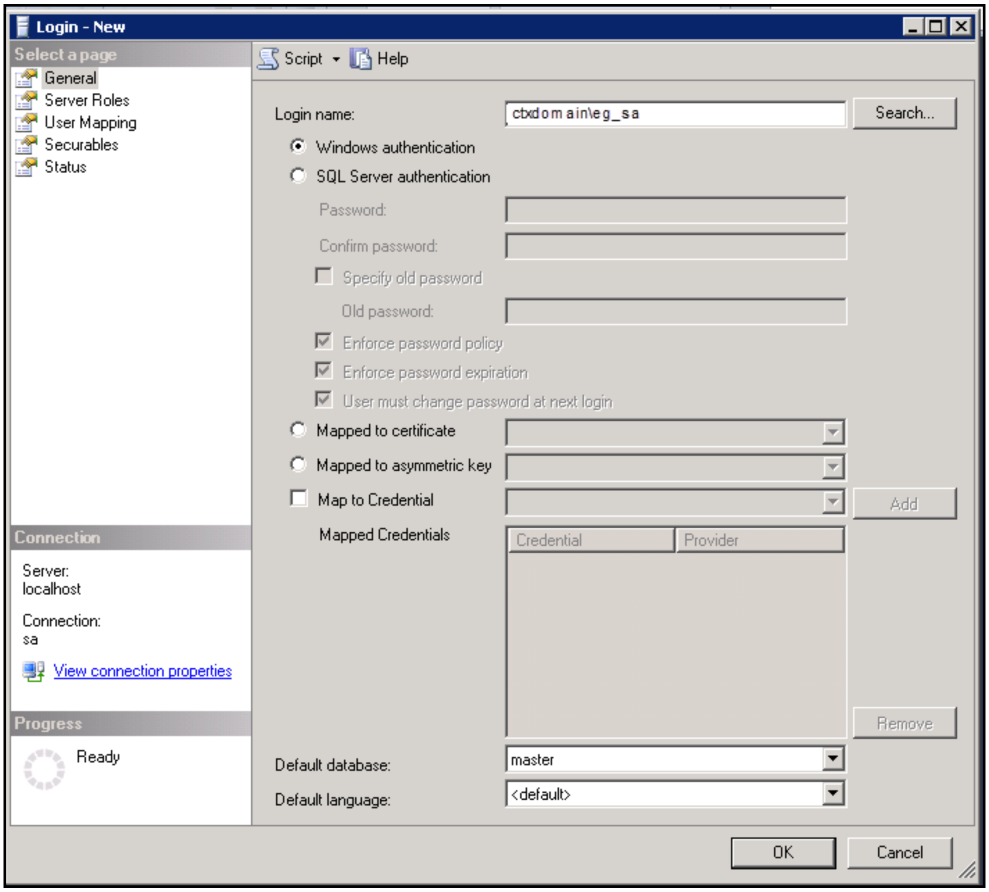

Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Object Explorer
Connect
localhost (SQL Server 12.0.2000 - sa)
Databases
Security
Logins
New Login...
Filter
Start PowerShell
Reports
Refresh

Figure 2.50: Choosing to create a new login



Login name: ctxdomain\eg_sa

● Windows authentication

○ SQL Server authentication

Password:

Confirm password:

□ Specify old password

Old password:

☑ Enforce password policy

☑ Enforce password expiration

☑ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

Mapped Credentials

Credential	Provider

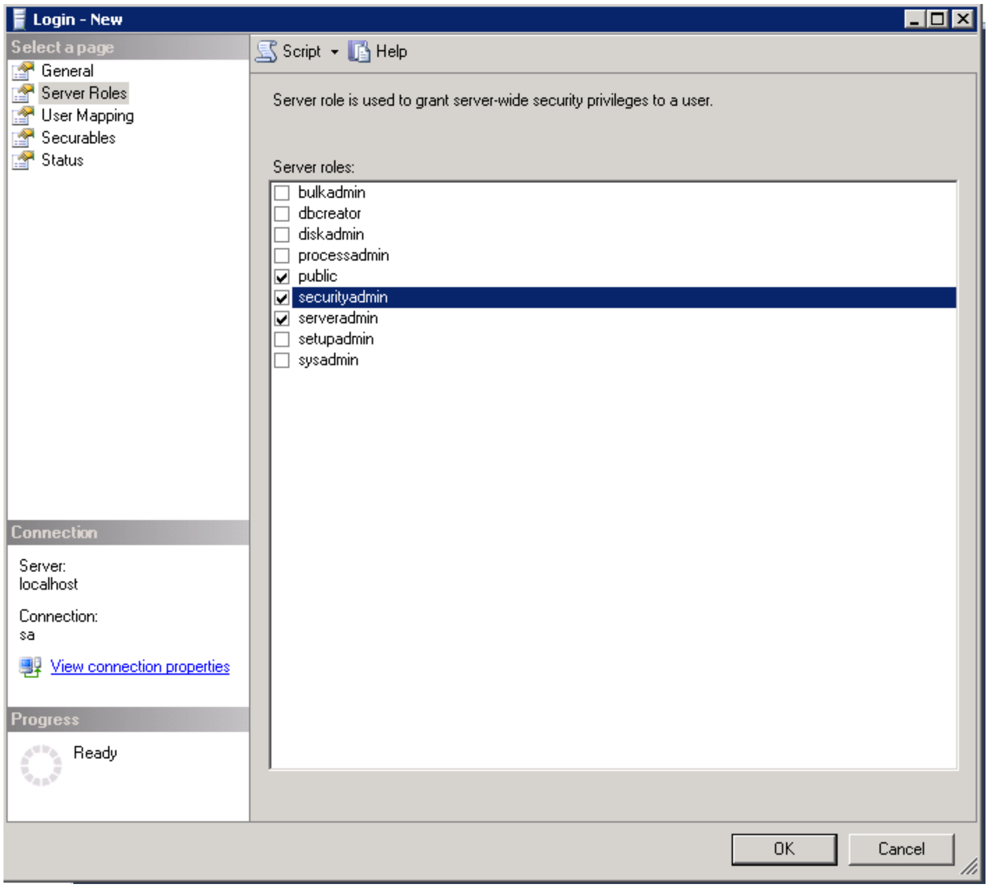
Default database: master

Default language: <default>

Server:
localhost

Connection:
sa

Figure 2.51: Creating a new user



Server role is used to grant server-wide security privileges to a user.

Server roles:

- □ bulkadmin
- □ dbcreator
- □ diskadmin
- □ processadmin
- ☑ public
- ☑ securityadmin
- ☑ serveradmin
- □ setupadmin
- □ sysadmin

Server:
localhost

Connection:
sa

Figure 2.52: 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 manager 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 2.47. 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 manager, 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 2.47. 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 2.47 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 2.47, 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 manager 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:

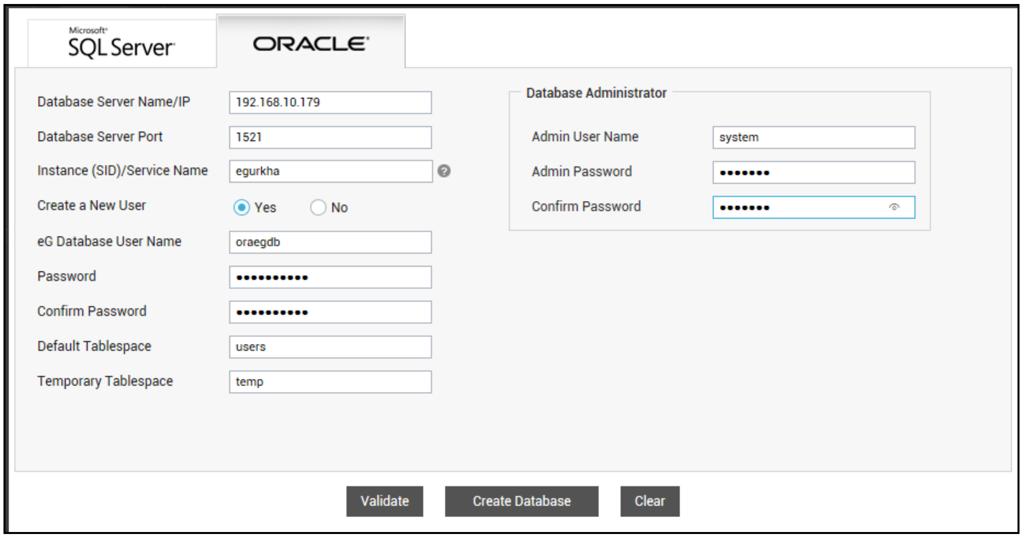
By default, the eG manager is configured for agent-based monitoring - i.e., when a server is auto-discovered and then managed, it is monitored in an agent-based manner. Administrators have an option to set agentless monitoring as the default for the eG manager.

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 manager. 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 2.53 will then appear.



Database Server Name/IP: 192.168.10.179
Database Server Port: 1521
Instance (SID)/Service Name: egurkha
Create a New User: ● Yes ○ No
eG Database User Name: oraegdb
Password: ••••••••••
Confirm Password: ••••••••••
Default Tablespace: users
Temporary Tablespace: temp

Database Administrator
Admin User Name: system
Admin Password: •••••••
Confirm Password: •••••••

Figure 2.53: Configuring the eG database on an Oracle database server

To configure the eG database on Oracle, do the following using Figure 2.53:

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 manager should use. A Service Name is mandatory if a pluggable database is being used.
4. The eG manager 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 manager to use, first set the

Create a New User flag in Figure 2.53 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:

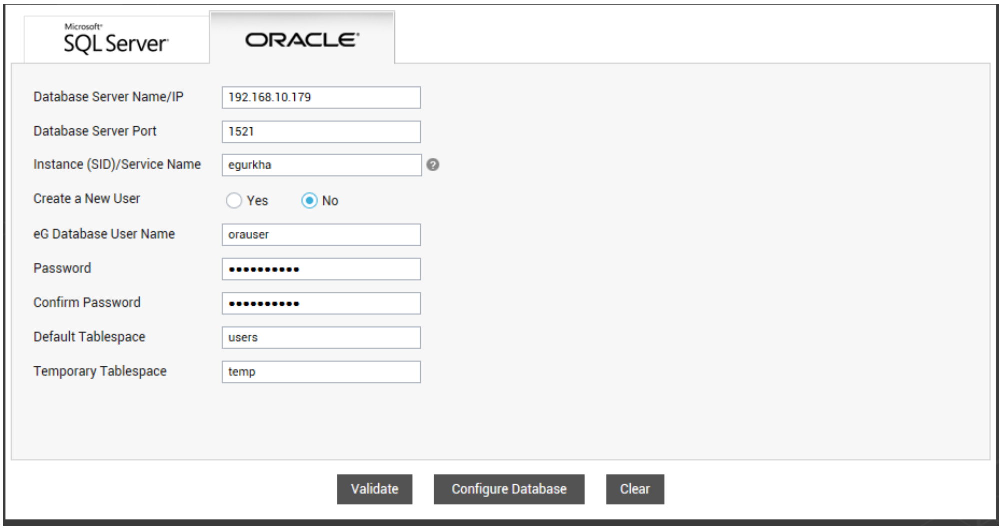
If the user chooses not to have the user account created by the configuration process, the user account has to be created manually on the Oracle database server with *connect, resource, and select_catalog* privileges. To know how to create such a user, refer to the table below, which describes the complete 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 manager's use.

5. If you want to use an existing database user account for the eG manager, first set the **Create a New User** flag to **No** (see Figure 2.54). 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.



Database Server Name/IP	192.168.10.179
Database Server Port	1521
Instance (SID)/Service Name	egurkha
Create a New User	○ Yes ● No
eG Database User Name	orauser
Password	••••••••••
Confirm Password	••••••••••
Default Tablespace	users
Temporary Tablespace	temp

Figure 2.54: Configuring an existing database user account for the eG manager

Note:

If you set an existing database user as the eG database user at step 5, then before configuring the eG manager 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 2.53). 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 manager 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 manager 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.

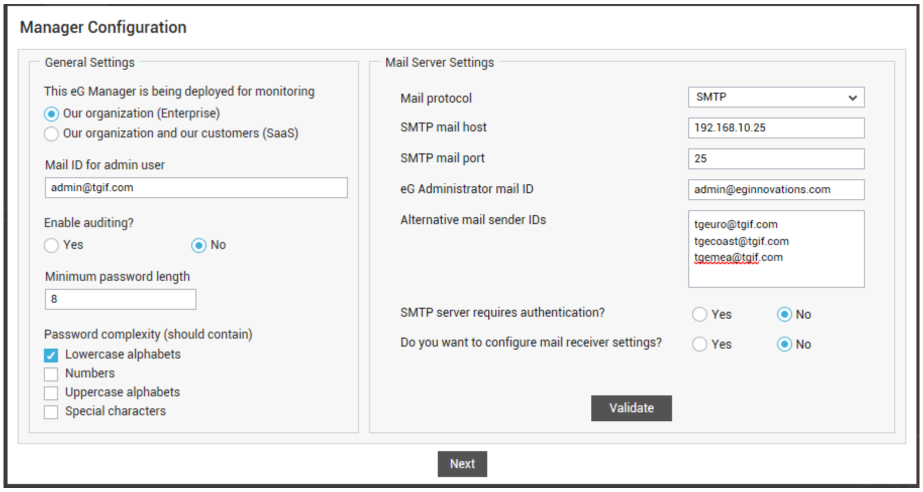
These parameters might have to be tuned further based on an increase in server load.

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 2.53 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 manager, then you will not have to provide database administrator credentials. In this case therefore, the **Database Administrator** section will not appear (see Figure 2.54).
8. To check the veracity of your configuration, click the Validate button in Figure 2.54. 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 manager, 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 2.53. 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 2.54) to configure the specified database user account for use by the eG manager.
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 2.53 or Figure 2.54 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 2.53, 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 manager 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 2.55). This page enables you to indicate what type of environment your eG manager deployment needs to monitor. Depending upon the type of environment, you can even turn on/off certain key capabilities of the eG manager 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 manager operations, without even logging into the eG management console!



Manager Configuration

General Settings

This eG Manager is being deployed for monitoring

● Our organization (Enterprise)

○ Our organization and our customers (SaaS)

Mail ID for admin user: admin@tgif.com

Enable auditing? ○ Yes ● No

Minimum password length: 8

Password complexity (should contain)

☑ Lowercase alphabets
□ Numbers
□ Uppercase alphabets
□ Special characters

Mail Server Settings

Mail protocol: SMTP

SMTP mail host: 192.168.10.25

SMTP mail port: 25

eG Administrator mail ID: admin@eginnovations.com

Alternative mail sender IDs: tgeuro@tgif.com
tgecoast@tgif.com
tgemea@tgif.com

SMTP server requires authentication? ○ Yes ● No

Do you want to configure mail receiver settings? ○ Yes ● No

Figure 2.55: Configuring the basic manager settings

Using Figure 2.55, do the following:

1. First, choose the deployment model for the eG manager - Enterprise or SaaS. These models are briefly discussed below:

   - Enterprise: This model is ideal if your eG manager 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 manager - 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.

If you want to deploy the eG manager for Enterprise, then select the **Our Organization (Enterprise)** option in Figure 2.55.

- SaaS: This model is ideal if you are a Managed Service Provider (MSP), providing infrastructure hosting and management services to multiple customers. Monitoring is quiet often a cloud-based service that an MSP offers to each of their customers. If you are an MSP, you will want the eG manager to not just monitor your infrastructure, but also that of your customers. This means that an eG manager centrally deployed in the MSP infrastructure will be managing agents deployed in the customer infrastructure as well.

  The SaaS model also helps where a single eG manager manages agents used by different departments (eg., Development, Testing, Support etc.) / support groups (Europe Support, EMEA Support, USA Support etc.) / IT domains (Network administration, Database administration, Windows administration etc.).

  With the SaaS model, eG Enterprise fully supports mult-tenancy. Unlike the Enterprise model, in SaaS, the administrator will not be the sole custodian of administrative rights. Instead, these rights will be delegated to the individual tenants - say, MSP customers, department heads/workers, support personnel who are part of different support groups, or IT domain experts. The tenants are thus empowered to deploy the agents they want, manage the components they wish to monitor, and customize accesses, monitoring, and alerting based on the requirements of their infrastructure. The central administrator will continue to hold unrestricted administrative rights, which will enable him/her to manage monitoring licenses of the tenants, oversee performance and problems across tenant infrastructures, and even override a tenant's monitoring configuration if required.

  If you want to deploy the eG manager for SaaS, then select the **Our Organization and our customers (SaaS)** option in Figure 2.55.

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 manager 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 manager 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 2.55, you can also enable/disable audit logging for your eG manager. An audit log can be best described as a simple log of changes, typically used for tracking temporal information. The eG manager 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 2.55).

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 2.55, 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 2.55.

   Note:

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

5. Then, proceed to configure **Mail Server Settings**. Here, you provide details of the mail server that eG should use for sending emails. This specification is optional for an Enterprise deployment, but is mandatory for a SaaS deployment.

   In case of an Enterprise deployment, you need to configure a mail server only if you want to enable email alerting - i.e., only if you want your users to receive problem alerts by email. If you do not want to enable email alerting, then the mail server settings need not be defined.

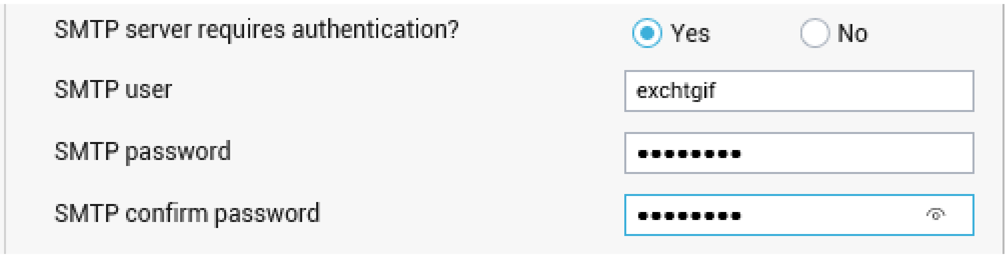
   In case of a SaaS deployment on the other hand, it is mandatory to configure a mail server. This is because, without a mail server, verification codes cannot be emailed to tenants who attempt to register with the eG manager. In the absence of a verification code, the registration will fail. As a result, eG Enterprise will be unable to monitor tenant environments - eg., environments of MSP customers.

   To configure a mail server, specify the following:

   - The protocol through which you wish to transmit or send the outgoing mail messages across the Internet Protocol (IP) networks has to be selected from the **Mail protocol** list box. The **SMTP** option would be selected by default in this list box. If the mail server through which you wish to send the mail messages is **SSL-enabled**, then select, **SMTP-SSL** from the **Mail protocol** list box. If your mail server offers enhanced security and provides certificate based authentication, select the **SMTP-TLS** option from the **Mail protocol** list.
   - The identity (IP address or host name) of the mail server to be used by the eG manager for generating alarms has to be entered in the **SMTPmail host** text box. The port at which the mail host listens has to be provided in the **SMTP mail port** text box.
   - In MSP environments typically, different support groups are created to address performance issues relating to different customers. These support groups might prefer to receive problem intimation from customer-specific mail IDs instead of the global admin mail ID, so that they can instantly identify the customer environment that is experiencing problems currently. Moreover, this way, every support group will be enabled to send status updates on reported issues directly to the concerned customer, instead of overloading the admin mailbox. To facilitate this, Figure 2.55 allows the administrator to configure multiple **Alternative Mail sender IDs** - normally, one each for every customer in case of an MSP environment. While configuring multiple sender IDs in the space provided, ensure that you press the **Enter** key on your keyboard after every mail ID. This way, every ID will occupy one row of the text area. Later, while creating a new user using the eG administrative interface, the administrator can select

one of these configured sender IDs from the **Mail sender** list and assign it to the new user. This ensures that all email alerts received by the user are generated by the chosen ID only.

- If the mail server requires users to login before sending mails, then select the **Yes** option against the **SMTP server requires authentication?** field. By default, authentication is set to **No**. Upon selecting **Yes**, you will be required to provide a valid **SMTP user** name and **SMTP password** for logging into the mail server. Confirm the password by retyping it in the **SMTP confirm password** text box.



SMTP server requires authentication? ● Yes ○ No

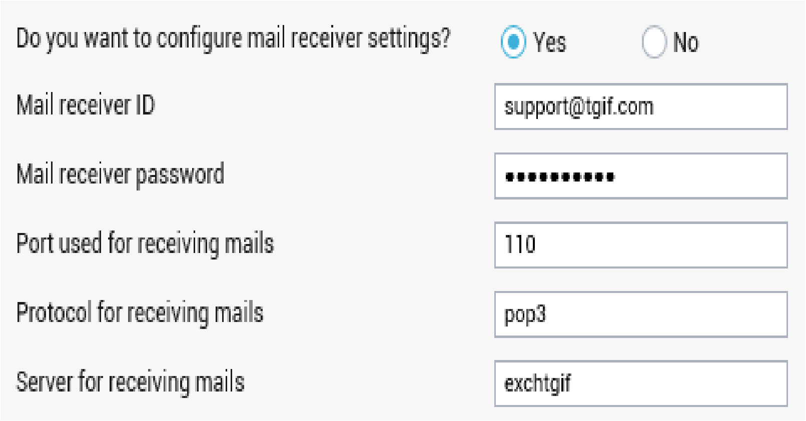
SMTP user: exchtgif

SMTP password: •••••••••

SMTP confirm password: •••••••••

Figure 2.56: Configuring the SMTP login credentials, if SMTP server requires authentication

- To safeguard from spam, some mail servers are configured so that they will allow mails to be sent from a system only if that system is also used to receive mails. To allow the eG manager to use such mail servers to send email alerts, additional configuration is needed. In such a case, select the **Yes** option against the **Do you want to configure mail receiver settings?** field.



Do you want to configure mail receiver settings? ● Yes ○ No

Mail receiver ID: support@tgif.com

Mail receiver password: •••••••••••

Port used for receiving mails: 110

Protocol for receiving mails: pop3

Server for receiving mails: exchtgif

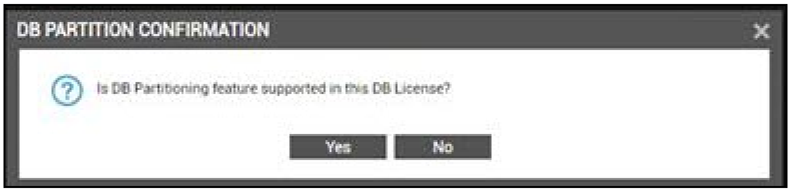
Figure 2.57: Configuring mail receiver settings

By default this field is set to **No**. When you enable this authentication to **Yes**, you need to specify the following details in the corresponding text boxes (see Figure 2.57):

- **Mail receiver ID:** Specify the login name to be used for receiving mails.
- **Mail receiver password:** The password of the mail receiver needs to be specified here.

- ○ **Port used for receiving mails:** The port number on the mail server to which the mail manager connects needs to be provided here.
- ○ **Protocol for receiving mails:** Mention the protocol used for receiving mails. The protocol can be either POP3 or IMAP
- ○ **Server for receiving mails**: Specify the server to which the mail manager will connect to receive mails.

- To verify whether/not your mail server settings are correct, click the **Validate** button in Figure 2.55. This brings incorrect/invalid specifications to your notice, so you can amend them. Once validation is successful, click the **Next** button in Figure 2.55 to proceed.
- If you have configured an Oracle database backend for the eG manager, then Figure 2.58 will appear.



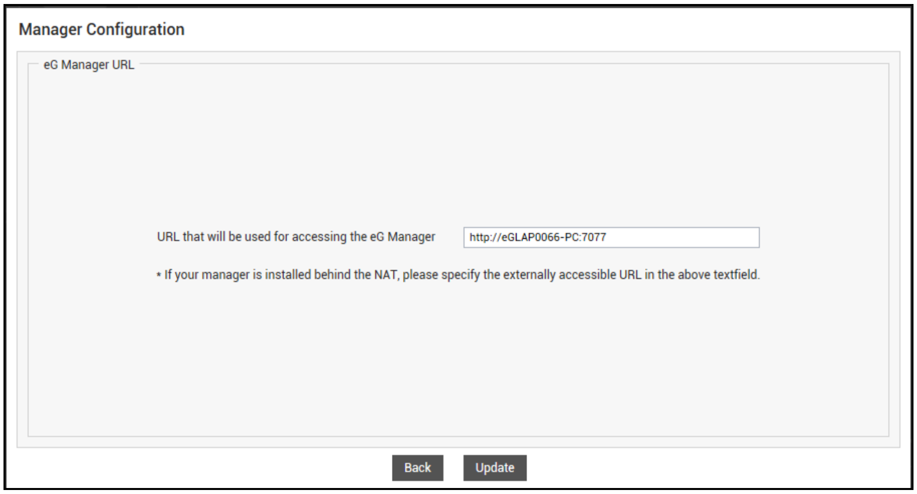
DB PARTITION CONFIRMATION

Is DB Partitioning feature supported in this DB License?

Figure 2.58: 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 manager 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 2.58 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 manager 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 2.58. 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 2.59 will then appear, displaying the URL using which the eG manager should be accessed. The default URL will be of the format http://<eGManagerIPorHostName>:<eGManagerPort> or https://<eGManagerIPorHostName>:<eGManagerPort>, depending upon whether/not the manager is SSL-enabled. If your eG manager is behind the NAT, then you may want to replace the default URL with the externally accessible URL. Then, click the **Update** button.



Manager Configuration

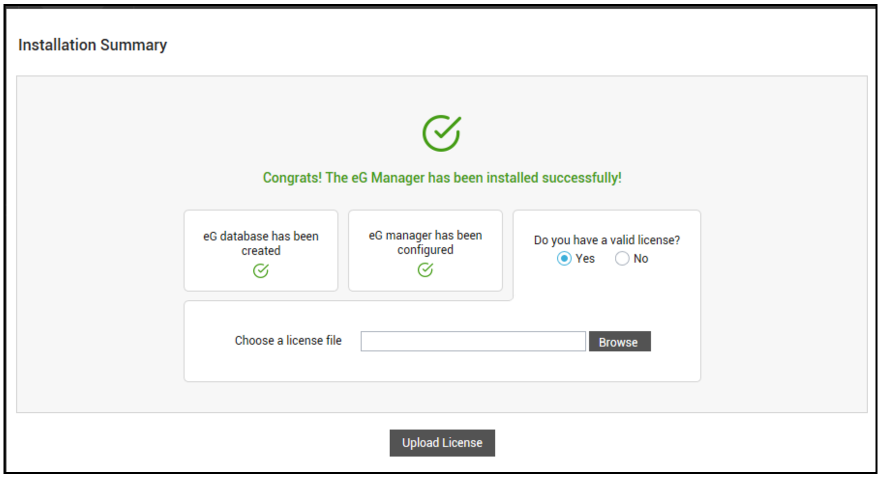
eG Manager URL

URL that will be used for accessing the eG Manager: http://eGLAP0066-PC:7077

* If your manager is installed behind the NAT, please specify the externally accessible URL in the above textfield.

Figure 2.59: The URL that will be used for accessing the eG manager

- Figure 2.60 will then appear informing you of the successful installation of the eG manager. 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.



Installation Summary

✓

Congrats! The eG Manager has been installed successfully!

eG database has been created ✓

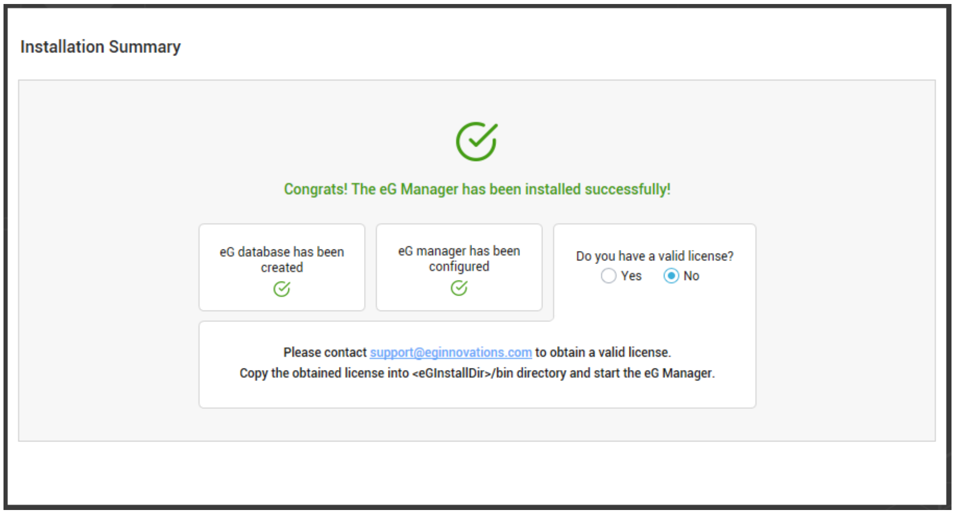
eG manager has been configured ✓

Do you have a valid license? ● Yes ○ No

Choose a license file

Figure 2.60: 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 2.61). 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.


Installation Summary

Congrats! The eG Manager has been installed successfully!

eG database has been created ✓

eG manager has been configured ✓

Do you have a valid license? ○ Yes ● No

Please contact support@eginnovations.com to obtain a valid license.
Copy the obtained license into <eGInstallDir>/bin directory and start the eG Manager.

Figure 2.61: Requesting a valid license

2.1.2 Silent Mode Installation of the eG Manager

The first step towards installing the eG manager in the silent mode is to create the silent mode script for a manager installation. The script file will carry the extension **.iss**, and will contain the inputs provided by the administrator while installing the eG manager in the normal mode. Before attempting script creation, ensure that the **eGManager_<OS>.exe** is available on the local host. Then, to create the script, do the following:

1. From the command prompt, switch to the directory in which the **eGManager_<OS>.exe** resides.
2. Next, issue the following command: **eGManager_<OS>.exe -a -r /f1"<Full path to the script file >"**. For example, to create a script file named **eGManager.iss** in the **c:\script** directory, the command should be: **eGManager_<OS>.exe -a -r /f1"c:\script\eGManager.iss"**.
3. The *Normal mode* manager installation will then begin. The inputs supplied during the normal mode will automatically be saved in the **iss** file that was created in step 2. Refer to the Section **2.1.1** topic for the detailed procedure for installing an eG manager on Windows in the normal mode.

The next time you wish to install the eG manager on the same host, you can do so in the *Silent mode*, following the steps given below:

1. Uninstall the eG manager on the host (if it already exists).
2. Ensure that the **eGManager_<OS>.exe** is present on the host, go to the command prompt, and then switch to the directory containing the manager executable.

3. From that directory, execute the following command to install the eG manager in the silent mode: **eGManager_<OS>.exe -a -s /f1"<Full path to the script file containing the inputs for the installation>"**. In other words, to extract installation inputs from the **eGManager.iss** file that was created in our example above, the command will be: **eGManager_<OS>.exe -a -s /f1"c:\script\eGManager.iss"**.

4. The eG manager installation will then begin and proceed in the silent mode. Setup will extract the required inputs from the **iss** file specified in step 3 above and perform the installation automatically, requiring no user intervention of any kind.

Note:

- If the silent mode installation is to be carried out on a different host, then inputs such as manager IP/hostname will undergo a change. To ensure that such changes are effected during the silent mode install, edit the inputs registered with the **.iss** file using an Editor.

- The silent mode installation procedure applies only to the eG manager on Windows with Oracle/MS SQL backend. If the backend is MSDE, then the eG manager cannot be reinstalled in the silent mode.

2.1.2.1 Configuring Redundancy for the eG Manager on Windows

To enable redundancy for a manager on Windows, a special batch file needs to be executed. This batch file, named **setup_cluster.bat**, resides in the <EG_INSTALL_DIR>\lib directory, and when executed, requests the following inputs.

The **setup_cluster** batch file will first request your confirmation to proceed with enabling manager redundancy.

```
Would you like to enable eG Manager redundancy y/n [n]? y
```

Specifying **n** here will terminate the script execution. If you enter **y**, then the following steps will apply:

1. Provide the IP (or hostname) and port number of the manager being configured.

   ```
   Please enter the hostname (or IP address) of this host: 192.168.10.87
   Please enter the port at which this eG Manager listens: 7077
   ```

   Note:

   - If an eG manager (primary/secondary) in a cluster supports only an IPv6 address, then its best that you configure redundancy for that manager using its hostname and not its IP address.

- If the eG manager is configured using the hostname, then ensure that cluster setup is also performed using the hostname only. Likewise, if the eG manager is configured using the IP address, then ensure that cluster setup is also performed using the IP address alone.

2. Next, you will be required to indicate whether SSL has been enabled for the manager being configured.

   ```
   Please indicate if your eG Manager uses SSL y/n :[n] n
   ```

   Press **y** to confirm SSL-enabling and **n** to deny it.

3. Next, indicate whether Network Address Translation (NAT) is used.

   ```
   Please specify if you use Network Address Translation(NAT) y/n :[n] y
   ```

   NAT facilitates multiple managers spanning geographies to communicate with one another. In such a case, specify **y** here. If not, enter **n**.

4. If NAT is used (i.e., if **y** is specified at step 3), provide the NAT IP (or hostname), using which the managers interact with each other.

   ```
   Please enter the NAT IP/hostname:
   ```

5. Similarly, also indicate whether Port Address Translation (PAT) is used. PAT again comes into play only when the managers span geographies. In such a case, enter **y**. If not, press **n**.

   ```
   Please specify if you use Port Address Translation(PAT) y/n :[n]y
   ```

6. If **y** is specified against PAT usage, then specify the PAT port number.

   ```
   Please enter the PAT port: 8088
   ```

7. Then, specify **y** if the manager uses a proxy server for communicating with the other managers in the redundant cluster.

   ```
   Please indicate if you would use proxy server for communications y/n :[n] y
   ```

8. If a proxy server is indeed used, you will then have to provide the IP address (or hostname) and port number of the proxy server.

   ```
   Please enter the hostname of the proxy: 192.168.10.60
   ```

   ```
   Please enter the port of the proxy: 80
   ```

9. Indicate whether further authentications for the proxy server are required, and if so, proceed to provide the user name and password to be used for the proxy.

```
Do you need authentication for the proxy? y/n [n]: y
Please enter the username to be used for the proxy: user
Please enter the password for user :
Please re-enter the password for user :
```

10. Next, state whether the manager being configured is to be set as the **primary manager**.

    ```
    Is this a primary eG Manager y/n [n]? n
    ```

11. If the current manager is not a primary manager (i.e., if **n** is specified at step 10), then it means it is a secondary manager. Therefore, proceed to provide the IP address and port number of the primary manager with which this secondary manager communicates.

    ```
    Please enter the hostname of the primary eG Manager: 192.168.10.59
    Please enter the port of the primary eG Manager: 7077
    ```

    Note:

    - A target environment can have only one primary manager and one secondary manager.
    - An admin user can login to the primary manager only.
    - When running **setup_cluster** on a secondary manager, make sure that you specify the IP/hostname of the primary manager depending upon how you have configured the cluster in the primary manager. In other words, if when running **setup_cluster** on the primary manager, you have provided the IP address of the primary manager, then make sure that you provide the IP address only when **setup_cluster** prompts you for the details of the primary manager on the secondary manager.

12. Finally, indicate whether the primary manager uses SSL or not by specifying **y** or **n**.

    ```
    Please indicate if your primary eG Manager uses SSL y/n [n]: n
    ```

    Note:

    Ensure that primary and secondary managers in a cluster use a separate database.

2.1.3 Starting the eG Manager

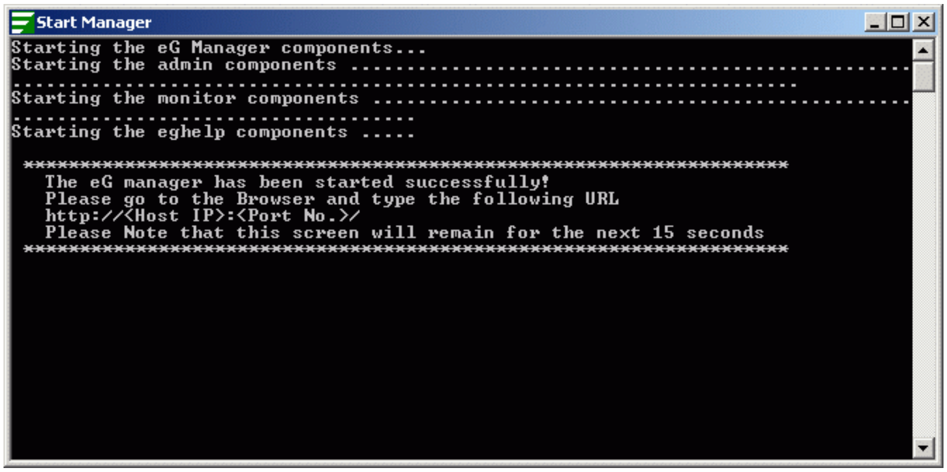
The following sections provide you the steps for starting the eG manager with/without SSL support:

- Section **2.1.3.1**
- Section **2.1.3.2**

2.1.3.1 Starting the eG Manager Without SSL Support

To start an eG manager on a Windows 2008 / Windows 7 server, ‘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.

If the manager starts successfully, the following message appears:



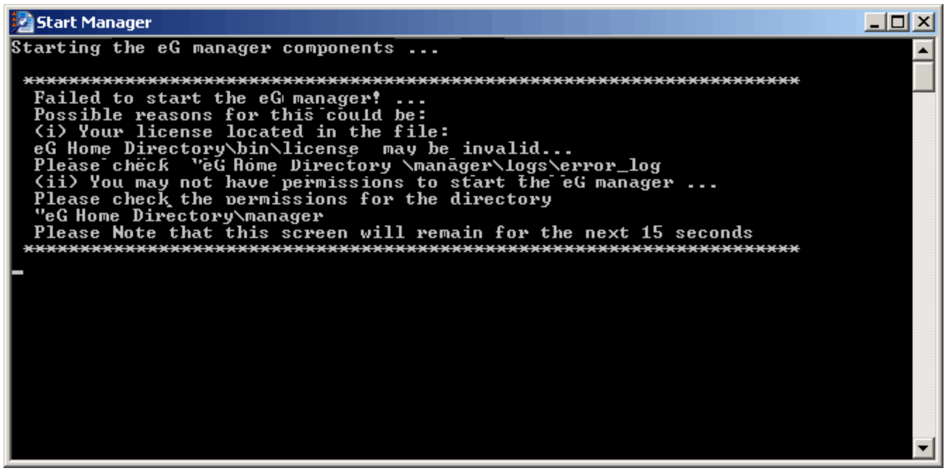
```
Starting the eG Manager components...
Starting the admin components ..................................................
......................................................................
Starting the monitor components ................................................
....................................
Starting the eghelp components .....

 ********************************************************************
   The eG manager has been started successfully!
   Please go to the Browser and type the following URL
   http://<Host IP>:<Port No.>/
   Please Note that this screen will remain for the next 15 seconds
 ********************************************************************
```

Figure 2.62: Message indicating that the manager has been started successfully

Upon starting the eG manager, 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 manager has been started successfully. If the manager fails to start, the following message appears.



```
Starting the eG manager components ...

 *********************************************************************
  Failed to start the eG manager! ...
  Possible reasons for this could be:
  (i) Your license located in the file:
  eG Home Directory\bin\license  may be invalid...
  Please check  "eG Home Directory \manager\logs\error_log
  (ii) You may not have permissions to start the eG manager ...
  Please check the permissions for the directory
  "eG Home Directory\manager
  Please Note that this screen will remain for the next 15 seconds
 *********************************************************************

_
```

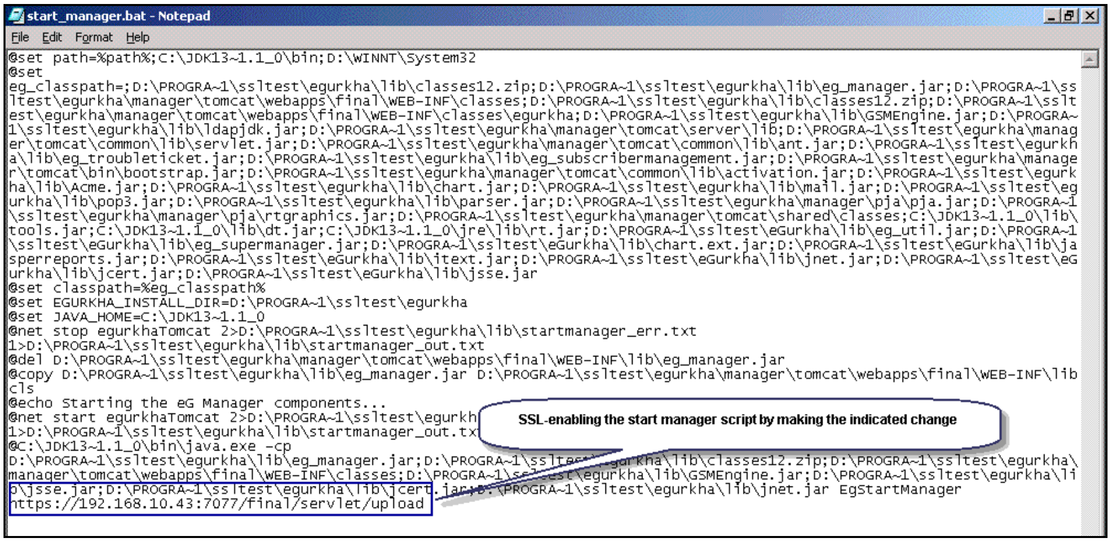
Figure 2.63: Message indicating that the manager has not been started successfully

Please check the <EG_HOME_DIR>\manager\logs\error_log file to find out the reasons due which the manager failed to start.

2.1.3.2 Starting the eG Manager with SSL Support

The first step towards starting the manager with SSL support is to SSL- enable the **startmanager.bat** script by following the steps below:

1. Open the **start_manager.bat** file (see Figure 2.64) residing in the <EG_INSTALL_DIR>/lib directory. Change the URL *http://<eGmanagerIp>:<eGmanagerdefaultTCPPort>/final/servlet/upload* present in the last line of the batch file to *https://<eGmanagerIp>:<eGmanagerPort>/final/servlet/upload* (see Figure 2.64).



```
@set path=%path%;C:\JDK13~1.1_0\bin;D:\WINNT\System32
@set
eg_classpath=;D:\PROGRA~1\ssltest\egurkha\lib\classes12.zip;D:\PROGRA~1\ssltest\egurkha\lib\eg_manager.jar;D:\PROGRA~1\ss
ltest\egurkha\manager\tomcat\webapps\final\WEB-INF\classes;D:\PROGRA~1\ssltest\egurkha\lib\classes12.zip;D:\PROGRA~1\sslt
est\egurkha\manager\tomcat\webapps\final\WEB-INF\classes\egurkha;D:\PROGRA~1\ssltest\egurkha\lib\GSMEngine.jar;D:\PROGRA~
1\ssltest\egurkha\lib\ldapjdk.jar;D:\PROGRA~1\ssltest\egurkha\manager\tomcat\server\lib;D:\PROGRA~1\ssltest\egurkha\manag
er\tomcat\common\lib\servlet.jar;D:\PROGRA~1\ssltest\egurkha\manager\tomcat\common\lib\ant.jar;D:\PROGRA~1\ssltest\egurkh
a\lib\eg_troubleticket.jar;D:\PROGRA~1\ssltest\egurkha\lib\eg_subscribermanagement.jar;D:\PROGRA~1\ssltest\egurkha\manage
r\tomcat\bin\bootstrap.jar;D:\PROGRA~1\ssltest\egurkha\manager\tomcat\common\lib\activation.jar;D:\PROGRA~1\ssltest\egurk
ha\lib\Acme.jar;D:\PROGRA~1\ssltest\egurkha\lib\chart.jar;D:\PROGRA~1\ssltest\egurkha\lib\mail.jar;D:\PROGRA~1\ssltest\eg
urkha\lib\pop3.jar;D:\PROGRA~1\ssltest\egurkha\lib\parser.jar;D:\PROGRA~1\ssltest\egurkha\manager\pja\pja.jar;D:\PROGRA~1
\ssltest\egurkha\manager\pja\rtgraphics.jar;D:\PROGRA~1\ssltest\egurkha\manager\tomcat\shared\classes;C:\JDK13~1.1_0\lib\
tools.jar;C:\JDK13~1.1_0\lib\dt.jar;C:\JDK13~1.1_0\jre\lib\rt.jar;D:\PROGRA~1\ssltest\eGurkha\lib\eg_util.jar;D:\PROGRA~1
\ssltest\eGurkha\lib\eg_supermanager.jar;D:\PROGRA~1\ssltest\eGurkha\lib\chart.ext.jar;D:\PROGRA~1\ssltest\eGurkha\lib\ja
sperreports.jar;D:\PROGRA~1\ssltest\eGurkha\lib\itext.jar;D:\PROGRA~1\ssltest\eGurkha\lib\jnet.jar;D:\PROGRA~1\ssltest\eG
urkha\lib\jcert.jar;D:\PROGRA~1\ssltest\eGurkha\lib\jsse.jar
@set classpath=%eg_classpath%
@set EGURKHA_INSTALL_DIR=D:\PROGRA~1\ssltest\egurkha
@set JAVA_HOME=C:\JDK13~1.1_0
@net stop egurkhaTomcat 2>D:\PROGRA~1\ssltest\egurkha\lib\startmanager_err.txt
1>D:\PROGRA~1\ssltest\egurkha\lib\startmanager_out.txt
@del D:\PROGRA~1\ssltest\egurkha\manager\tomcat\webapps\final\WEB-INF\lib\eg_manager.jar
@copy D:\PROGRA~1\ssltest\egurkha\lib\eg_manager.jar D:\PROGRA~1\ssltest\egurkha\manager\tomcat\webapps\final\WEB-INF\lib
cls
@echo Starting the eG Manager components...
@net start egurkhaTomcat 2>D:\PROGRA~1\ssltest\egurkh
1>D:\PROGRA~1\ssltest\egurkha\lib\startmanager_out.tx
@C:\JDK13~1.1_0\bin\java.exe -cp
D:\PROGRA~1\ssltest\egurkha\lib\eg_manager.jar;D:\PROGRA~1\ssltest\egurkha\lib\classes12.zip;D:\PROGRA~1\ssltest\egurkha\
manager\tomcat\webapps\final\WEB-INF\classes;D:\PROGRA~1\ssltest\egurkha\lib\GSMEngine.jar;D:\PROGRA~1\ssltest\egurkha\li
b\jsse.jar;D:\PROGRA~1\ssltest\egurkha\lib\jcert.jar;D:\PROGRA~1\ssltest\egurkha\lib\jnet.jar EgStartManager
https://192.168.10.43:7077/final/servlet/upload
```

SSL-enabling the start manager script by making the indicated change

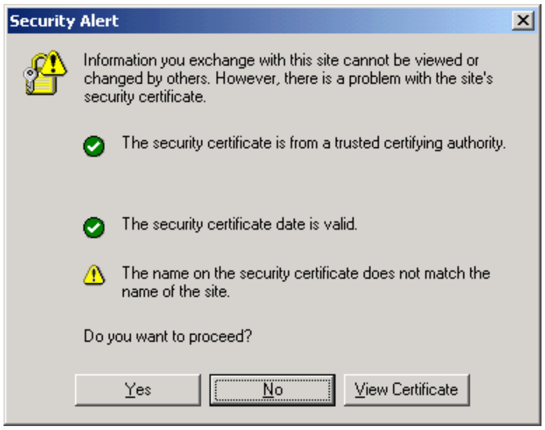
Figure 2.64: SSL-enabling the startmanager script

2. Finally, start the eG manager as discussed in SSL-Enabling the eG Manager.

2.1.4 Testing the SSL Installation

To test whether the eG Manager is SSL-enabled or not, do the following:

1. Try to access the eG manager with a secured connection (https) by typing *https://<eGmanagerIP>:<eGmanagerPort/* in the browser. If you receive a security message that states that the certificate is not from a trusted root certification authority, click **Yes** to continue to the web page (see Figure 2.65). This page will appear every time you try to access the web page using https, until you receive a certificate signed by a proper CA such as Verisign or Thawte.



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

✓ The security certificate is from a trusted certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate does not match the name of the site.

Do you want to proceed?

Figure 2.65: A security message

2. You can view the **eG Manager Login** page, which indicates that enabling SSL support for the eG installation has been successful.

2.1.5 Increasing the Memory of the eG Manager

The eG manager runs as a Java process. Typically, 1/3rdof the total system memory is the maximum heap memory that can be allocated to the eG manager process.

Where a large number of components are to be monitored, you may want to allocate more memory heap to the eG manager process. In such a case, follow the steps discussed below on an eG manager on Windows:

1. Login to the eG manager host.
2. Edit the <EG_INSTALL_DIR>\lib\setEnv.bat file.
3. Search for the following entries:

```
@set XMX=
@set XMS=
```

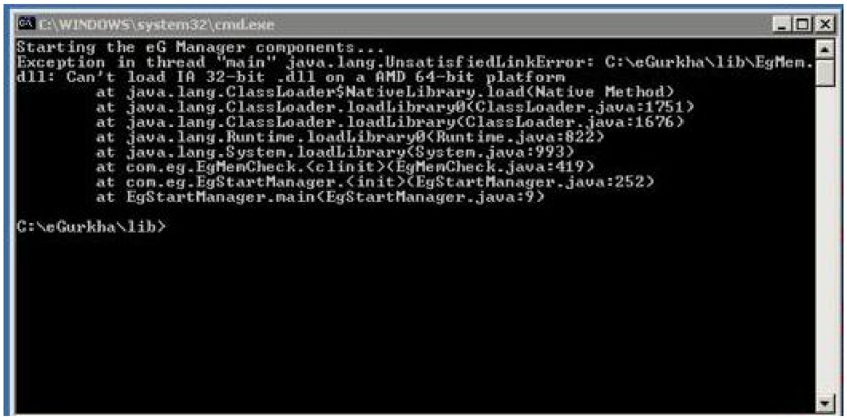
4. The *XMX* and *XMS* specifications govern the heap memory allocations to the eG manager. If you want to increase it to say, 8 GB (i.e., 8192 MB), change these specifications as indicated below:

```
@set XMX=8192
@set XMS=8192
```

5. Finally, save the file.

2.1.6 Dealing with Operating System Variations

The eG manager is a 32-bit application, which can be deployed on a 64-bit Windows operating system, provided the Windows host uses a 32-bit JDK. If a 32-bit JDK is not available on the Windows host, then the following error message appears upon attempting to start the eG manager:



```
Starting the eG Manager components...
Exception in thread "main" java.lang.UnsatisfiedLinkError: C:\eGurkha\lib\EgMem.
dll: Can't load IA 32-bit .dll on a AMD 64-bit platform
        at java.lang.ClassLoader$NativeLibrary.load(Native Method)
        at java.lang.ClassLoader.loadLibrary0(ClassLoader.java:1751)
        at java.lang.ClassLoader.loadLibrary(ClassLoader.java:1676)
        at java.lang.Runtime.loadLibrary0(Runtime.java:822)
        at java.lang.System.loadLibrary(System.java:993)
        at com.eg.EgMemCheck.<clinit>(EgMemCheck.java:419)
        at com.eg.EgStartManager.<init>(EgStartManager.java:252)
        at EgStartManager.main(EgStartManager.java:9)

C:\eGurkha\lib>
```

Figure 2.66: The error message that appears upon starting the eG manager on a 64-bit Windows host

In such a case, you have the following options:

- You use the JDK that is bundled with the eG manager, (OR)
- Download and install a 32-bit JDK on the Windows host and configure the eG manager to use the 32-bit JDK instead of the 64-bit one.

2.1.7 Stopping the eG Manager

To stop the manager, click the **Start** button on the task bar. From thereon, select Programs > eG Monitoring Suite > eG Manager > Stop Manager (see Figure 2.67).

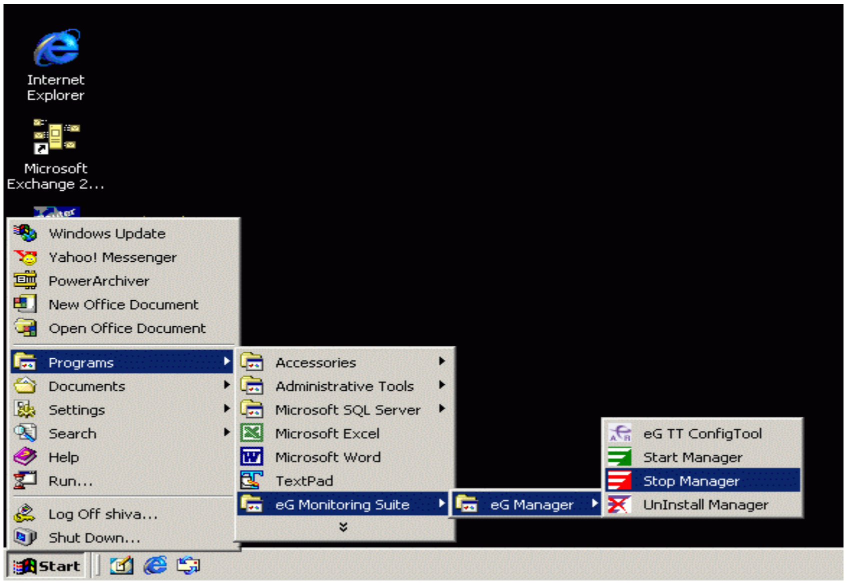
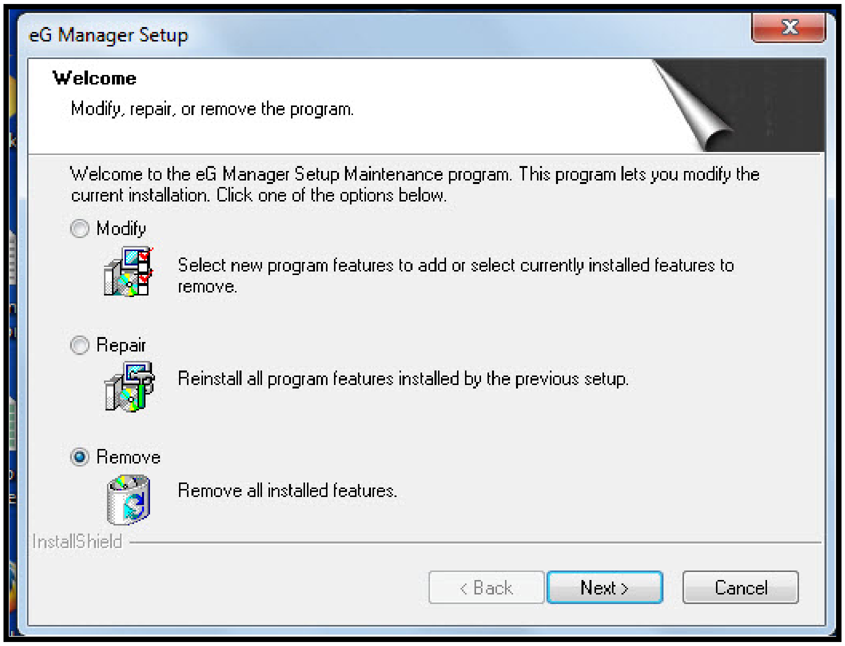


Figure 2.67: Stopping the eG manager

2.1.8 Uninstalling the eG Manager

1. It is essential to stop the manager (Section **2.1.7**) before uninstalling it. To stop it, first choose the eG Monitoring Suite option of the Windows Programs menu. Next, choose eG Manager. Finally, select **Stop Manager** from the options available.

2. To uninstall the eG manager, select **Uninstall Manager** from the options available under the eG Manager menu. The screen depicted by Figure 2.68 will appear. Here, select the **Remove** option and click the **Next >** button.



eG Manager Setup

Welcome

Modify, repair, or remove the program.

Welcome to the eG Manager Setup Maintenance program. This program lets you modify the current installation. Click one of the options below.

○ Modify

Select new program features to add or select currently installed features to remove.

○ Repair

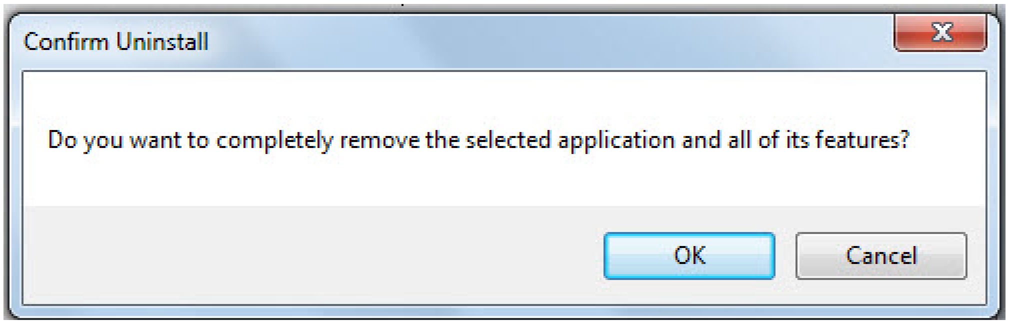
Reinstall all program features installed by the previous setup.

● Remove

Remove all installed features.

Figure 2.68: Uninstalling the eG manager

3. This process requires the confirmation of the user to remove the package and its related components as in Figure 2.69. Click the **OK** button.



Confirm Uninstall

Do you want to completely remove the selected application and all of its features?

Figure 2.69: Uninstall process seeking the confirmation of the user to delete the eG manager

2.1.9 Manually Uninstalling the eG Manager

To manually uninstall the eG manager, do the following:

1. Stop the eG manager if it is running.
2. Delete the following registry keys to remove Win32 Services of the eG Manager.

   - **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\eGurkhaTomcat**
   - **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\eGMon**
   - **HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\eGurkhaTomcat**
   - **HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\eGMon**
   - **HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\eGurkhaTomcat**
   - **HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\eGMon**

3. Delete the following registry keys to remove eG Manager software from Add/Remove Programs.

   - **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{12ECDC9D-2DEE-4550-BEF0-C5FAAA070D7A}**

     Note:

     Ensure that the **DisplayName** for the above-mentioned key is eG Manager.

   - **HKEY_LOCAL_MACHINE\SOFTWARE\eG Innovations, Inc.\eG Manager**

4. Delete the following shortcut: *Start->Programs->eG Monitoring Suite->eG Manager*

   Note:

   If the eG agent is not installed on the manager box, you can directly delete the *Start->Programs->eG Monitoring Suite shorcut*.

5. Delete the <EG_INSTALL_DIR>\manager directory.

   Note:

   If the agent is not installed on the manager box, then you can remove the entire <EG_INSTALL_DIR>.

2.2 eG Manager on Unix

The procedure for installing the eG manager differs depending on the operating system environment being used on the server on which the manager is to be installed. The eG manager is available for Solaris, Linux, and Windows operating system environments. The following steps are involved in installing and configuring eG Enterprise on Solaris and Linux operating systems. For detailed instructions of installing and configuring the manager on Windows operating systems, refer to Section **2.1**.

Before you start installing the eG manager on Unix systems, make sure that the pre-requisites discussed in **Pre-requisites for Installing eG Manager** topic are set in place.

2.2.1 Installing the eG Manager on Linux/CentOS

For installation on Linux/CentOS systems, the eG manager is provided as a tar file (named **eGmanager_linux.tar**). The installation process is driven by a shell script named **iManager_linux**.

Note:

The eG manager software has to be installed from a super-user account.

The steps involved in installing the eG manager are as follows:

1. To start the installation process, locate the **eGmanager_linux.tar** and **iManager_linux** files in the same directory and execute the **iManager_linux** command.
2. We recommend that eG Enterprise be executed by a special user account that is exclusively created for this purpose. Next, the installation process attempts to create the eG user account. For this process to continue, specify the user account to be used for executing eG Enterprise. The default value is **“egurkha”**.

   ```
   This script will install the eG manager. The eG manager must be executed by a separate
   user. If you have already installed the eG agent, both the manager and agent must use
   the same user accounts and must be installed in the same directory.
   ```

   ```
   Enter the name of the eG user [egurkha]:
   ```

3. Next, the installation process prompts the user to choose the path of the directory in which the eG manager is to reside. If possible the eG manager should be installed in the /opt directory. If space considerations preclude this, the eG manager can be installed in any other directory on the system. At the end of the installation process, a symbolic link is created to link the installation directory (eg., /usr/egurkha) to the /opt/egurkha directory.

   ```
   Enter the directory in which the eG manager should be installed [/opt] :
   ```

Also, specify the group to which this user account should be associated. The default value taken is **“egurkha”**.

```
Enter the group to which the eG user is to be associated [egurkha]:
```

Note:

- An existing user and/or group can be specified during this step.
- The installation process checks for the existence of the user and/or group, and creates a new user or group only if necessary.
- If the eG agent has been installed on the same system, use the same user and installation directory for both the manager and the agent.

4. The install process will now request the user to confirm installation of the auto-restart feature. This feature will enable the manager to start automatically every time the system hosting the manager reboots. Now, press **y** to install the auto-restart feature, or **n** to proceed without installing the same.

```
Would you like the eG manager to auto-restart on system boot-up? y/n [n] :
```

5. Upon successful completion of the installation process, the following message will be displayed:

```
********************************************************************
The eG manager has been successfully installed!
Please login as <user name> and run the script
/opt/egurkha/bin/setup_manager to configure the manager.
The licensing terms for eG products are mentioned in the file
/opt/egurkha/license_agreement.
PLEASE READ THIS FILE BEFORE PROCEEDING FURTHER.
Note that the eG manager requires JDK 1.8 or higher.
********************************************************************
```

2.2.2 Configuring the eG Manager for Linux Systems

After the installation, the eG manager needs to be configured for proper functioning. The eG manager configuration involves:

- Section **2.2.2.1**
- Section **2.2.2.2**

- Section **2.2.2.3**

The sections that follow discuss each of these steps elaborately.

2.2.2.1 Setting Up the eG Manager

eG manager setup involves configuring the IP address and port number of the eG manager, SSL enabling it, enabling/disabling support for double-byte characters, and configuring manager redundancy if required.

To setup the eG manager, do the following

1. For configuring the eG manager, first login as the eG user.

2. For the eG manager to operate correctly, a valid license must be available at the location **/opt/egurkha/bin**.

3. It is essential to ensure that a database server is available to host the eG database. The database server used for the eG database can either reside on the eG manager itself or it could be hosted on an external server. The installation process will attempt to connect to the database server and install the eG database. The sizing requirements for the eG database depend on the number of servers to be monitored.

4. Next, at the prompt issue the following command:

   ```
   /opt/egurkha/bin/setup_manager
   ```

   The following message will appear.

   ```
   Configuring the eG Manager...
   The licensing terms for eG products are mentioned in the file
   /opt/egurkha/license_agreement.
   PLEASE READ THIS FILE BEFORE PROCEEDING FURTHER.
   ```

5. Press **y** for accepting the terms. Once the licensing terms have been accepted, the configuration process prompts the user to enter the full hostname or the IP address of the host on which the eG manager is being configured. Pressing **n** on the other hand, indicates non-acceptance of the licensing terms and terminates the configuration process.

   ```
   Please indicate if you accept the eG licensing terms y/n [n]
   ```

6. In this stage, enter the full hostname or the IP address of the host on which the eG manager is being configured. If the domain name service is used in the target environment, use the full hostname. Otherwise, specify the IP address. Also, enter the port number on which the eG

manager listens for requests (from the agents and from the users) [default is **7077**]

```
Port configuration for the eG Manager
*********************************************************************
Enter the full hostname (or IP address) of this host:
Enter the port number for the eG Manager [7077]:
```

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 manager, note that only an IPv4 address can be provided. To configure the eG manager 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, at the above prompt.

7. Following this you will be required to indicate if the manager is to be configured to use SSL or not.

    ```
    Do you want the eG Manager to be SSL enabled y/n [n] :
    ```

    Enter **y** to enable SSL, or **n** to disable it.

8. 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 manager should be explicitly configured to display and process double-byte characters. In such a case, enable double-byte support for the eG manager by specifying y. On the other hand, for handling the character sets of other languages (example: French, German, Spanish, Portugese, etc.), the eG manager need not be double-byte enabled. At such times, enter **n** to disable double-byte support for the eG manager.

    ```
    Do you require the eG Manager to be double-byte enabled (for East Asian languages) y/n
    ? n
    ```

Note:

For a detailed discussion on how to enable double-byte support for eG Enterprise, refer to Chapter 4 of this manual.

9. Next, the **setup_manager** script invokes the **setup_cluster** script (from the **/opt/egurkha/bin** directory) to configure the redundant manager capability of eG Enterprise. eG Enterprise offers a redundant manager option wherein a secondary management console can act as an active or passive standby for the primary console. This capability, together with the ability to deploy redundant external agents in multiple locations, ensures that there is no single point of failure for the monitoring solutions. For more details about manager redundancy, refer to the eG User Manual.

   When **setup_ cluster** executes, it first requests your confirmation to enable manager redundancy.

   ```
   Would you like to enable eG manager redundancy y/n [n]? y
   ```

   If **n** is specified, the **setup_cluster** script will automatically terminate, and the **setup_manager** script will continue executing. To configure manager redundancy at any later point in time, execute the **setup_ cluster** script separately, from the **/opt/egurkha/bin** directory. The procedure for this has been provided in the Section **2.2.3** topic.

10. If **y** is specified at step 9, you will be required to indicate whether SSL has been enabled for the manager being configured.

    ```
    Please indicate if your eG Manager uses SSL y/n :[n] n
    ```

    Press **y** to confirm SSL-enabling and **n** to deny it.

11. Next, indicate whether Network Address Translation (NAT) is used.

    ```
    Please specify if you use Network Address Translation(NAT) y/n :[n] y
    ```

    NAT facilitates multiple managers spanning geographies to communicate with one another. In such a case, specify **y** here. If not, enter **n**.

12. If NAT is used (i.e., if **y** is specified at step 13), provide the NAT IP (or hostname), using which the managers interact with each other.

    ```
    Please enter the NAT IP/hostname:
    ```

13. Similarly, also indicate whether Port Address Translation (PAT) is used. PAT again comes into

play only when the managers span geographies. In such a case, enter **y**. If not, press **n**.

```
Please specify if you use Port Address Translation(PAT) y/n :[n]y
```

14. If **y** is specified against PAT usage, then specify the PAT port number.

```
Please enter the PAT port: 8088
```

15. Then, specify **y** if the manager uses a proxy server for communicating with the other managers in the redundant cluster.

```
Please indicate if you would use proxy server for communications y/n :[n] y
```

16. If a proxy server is indeed used, you will then have to provide the IP address (or hostname) and port number of the proxy server.

```
Please enter the hostname of the proxy: 192.168.10.60
```

```
Please enter the port of the proxy: 80
```

17. Indicate whether further authentications for the proxy server are required, and if so, proceed to provide the user name and password to be used for the proxy.

```
Do you need authentication for the proxy? y/n [n]: y
```

```
Please enter the username to be used for the proxy: user
```

```
Please enter the password for user :
```

```
Please re-enter the password for user :
```

18. Next, state whether the manager being configured is to be set as the **primary manager**.

```
Is this a primary eG Manager y/n [n]? n
```

19. If the current manager is not a primary manager (i.e., if **n** is specified at step 21), then it means it is a secondary manager. Therefore, proceed to provide the IP address and port number of the primary manager with which this secondary manager communicates.

```
Please enter the hostname of the primary eG Manager: 192.168.10.59
```

```
Please enter the port of the primary eG Manager: 7077
```

Note:

- A target environment can have only one primary manager and one secondary manager.
- An admin user can login to the primary manager only.
- When running **setup_cluster** on a secondary manager, make sure that you specify the IP/hostname of the primary manager depending upon how you have configured the cluster in

the primary manager. In other words, if when running **setup_cluster** on the primary manager, you have provided the IP address of the primary manager, then make sure that you provide the IP address only when **setup_cluster** prompts you for the details of the primary manager on the secondary manager.

20. Finally, indicate whether the primary manager uses SSL or not by specifying **y** or **n**.

```
Please indicate if your primary eG Manager uses SSL y/n [n]: n
```

Once this is specified, the **setup_cluster** script will exit, and the **setup_manager** script will resume.

Note:

Ensure that primary and secondary managers in a cluster use a separate database.

21. With that, the configuration of the eG manager setup ends. Upon successful configuration, the following messages appear:

```
***********************************************************
If there were no errors, the eG Manager has been installed.

You will now need to create the eG database. To do so, open a browser and
access the URL https://<EG_MANAGER_IPORHOSTNAME>:<EG_MANAGER_PORT>

Once the database is set up, use the commands /opt/egurkha/bin/start_manager
and /opt/egurkha/bin/stop_manager to start and stop the manager.

You will need a valid license to start the eG Manager.
Please contact support@eginnovations.com to request for a license.
***********************************************************
```

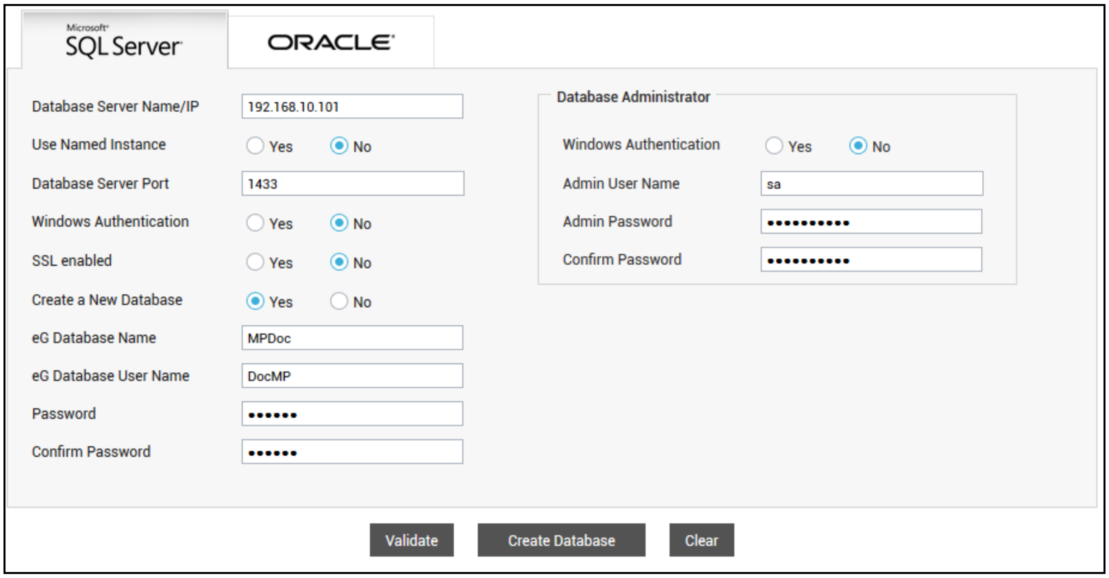
2.2.2.2 Configuring the eG Database

After setting up the eG manager, proceed to configure the eG database. The eG manager 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 manager itself or it could be hosted on an external server.

To enable you to easily configure an eG database, a special web page is provided. To access this web page, do the following:

1. From any supported browser, connect to the URL: http://<eGManagerIPorHostName>:<eGManagerPort> or https://<eGManagerIPorHostName>:<eGManagerPort>, depending upon whether/not the eG manager is SSL-enabled.
2. Figure 2.70 will then appear.



Database Server Name/IP	192.168.10.101
Use Named Instance	○ Yes ● No
Database Server Port	1433
Windows Authentication	○ Yes ● No
SSL enabled	○ Yes ● No
Create a New Database	● Yes ○ No
eG Database Name	MPDoc
eG Database User Name	DocMP
Password	••••••
Confirm Password	••••••

Database Administrator

Windows Authentication	○ Yes ● No
Admin User Name	sa
Admin Password	•••••••••••
Confirm Password	•••••••••••

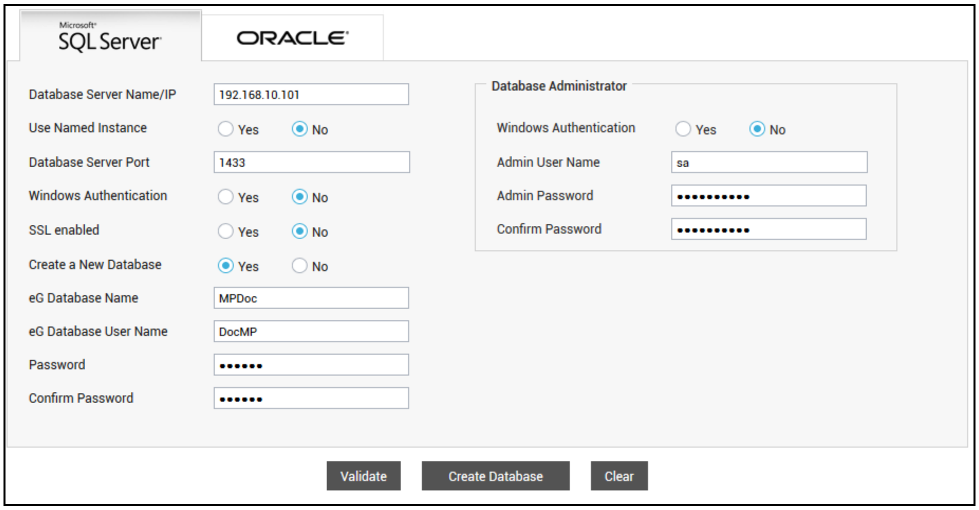
Figure 2.70: Configuring an eG database

3. Using Figure 2.70, you can pick a backend for the eG manager, 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;

2.2.2.2.1 Using Microsoft SQL Database

As soon as the web page opens, the **Microsoft SQL Server** tab page opens in it by default (see Figure 2.71).



Database Server Name/IP	192.168.10.101
Use Named Instance	○ Yes ● No
Database Server Port	1433
Windows Authentication	○ Yes ● No
SSL enabled	○ Yes ● No
Create a New Database	● Yes ○ No
eG Database Name	MPDoc
eG Database User Name	DocMP
Password	••••••
Confirm Password	••••••

Database Administrator

Windows Authentication	○ Yes ● No
Admin User Name	sa
Admin Password	••••••••••
Confirm Password	••••••••••

Figure 2.71: 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 2.71:

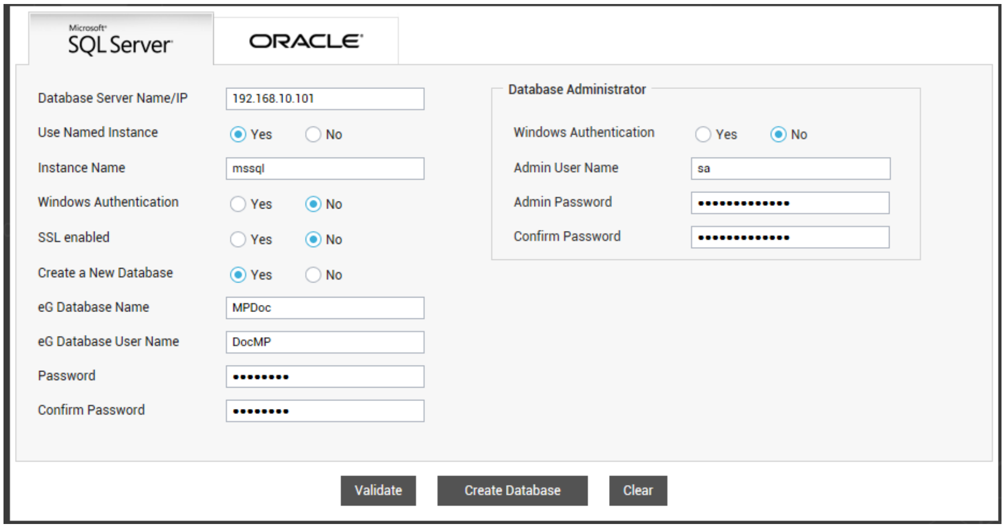
1. First, enter the location of the Microsoft SQL server by specifying the hostname and port on which the server is hosted against **Database Server Name/IP**. If you have already configured a SQL database on Microsoft Azure and want to use this database as the eG database, then, against **Database Server 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 2.72.



Database Server Name/IP: 192.168.10.101

Use Named Instance: ● Yes ○ No

Instance Name: mssql

Windows Authentication: ○ Yes ● No

SSL enabled: ○ Yes ● No

Create a New Database: ● Yes ○ No

eG Database Name: MPDoc

eG Database User Name: DocMP

Password: ••••••••

Confirm Password: ••••••••

Database Administrator

Windows Authentication: ○ Yes ● No

Admin User Name: sa

Admin Password: ••••••••••••••

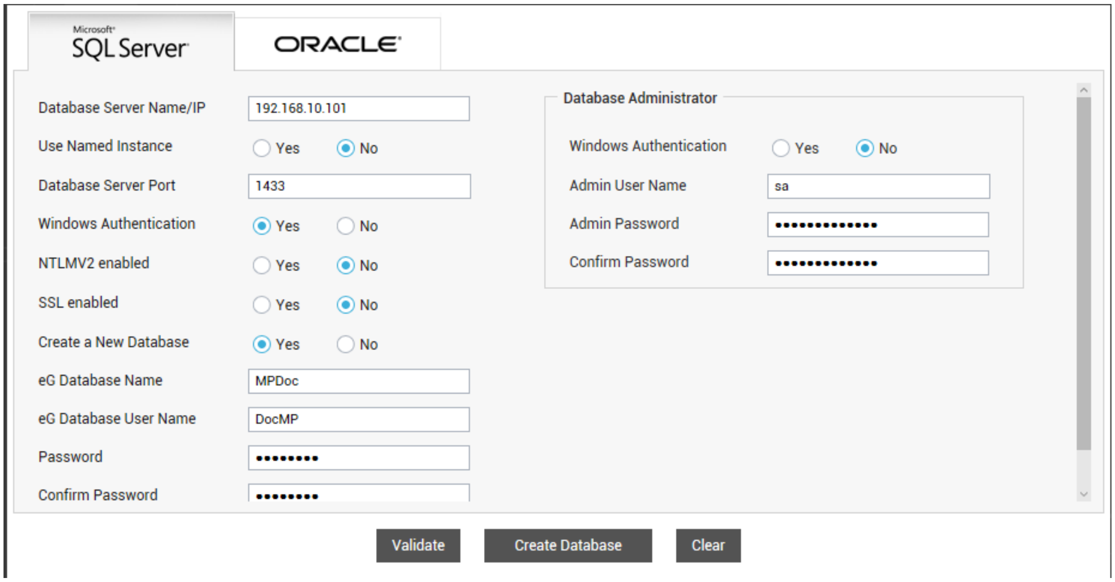
Confirm Password: ••••••••••••••

Figure 2.72: 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 2.71).

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 2.73). 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**.



Database Server Name/IP	192.168.10.101	
Use Named Instance	○ Yes	● No
Database Server Port	1433	
Windows Authentication	● Yes	○ No
NTLMV2 enabled	○ Yes	● No
SSL enabled	○ Yes	● No
Create a New Database	● Yes	○ No
eG Database Name	MPDoc	
eG Database User Name	DocMP	
Password	••••••••	
Confirm Password	••••••••	

Database Administrator

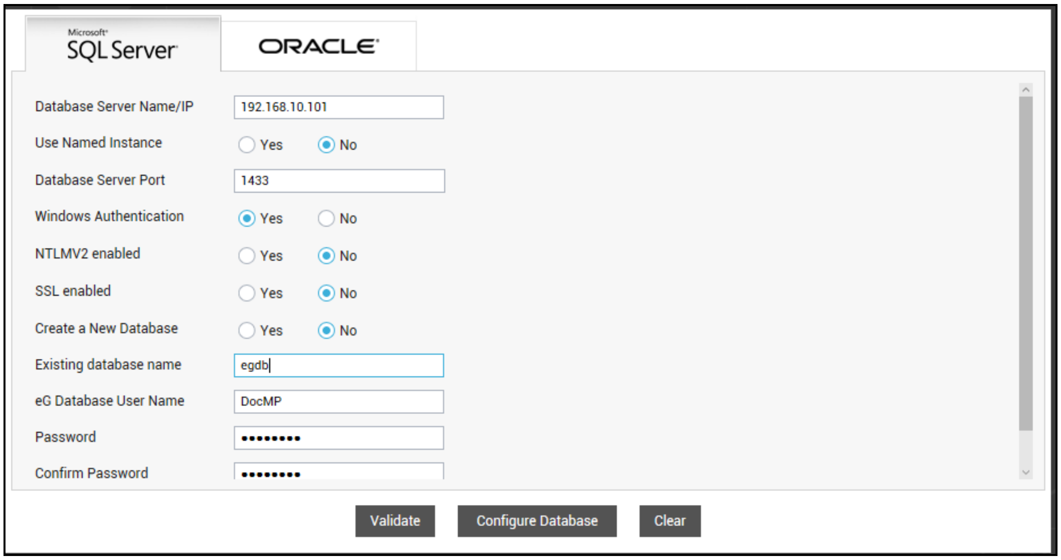
Windows Authentication	○ Yes	● No
Admin User Name	sa	
Admin Password	•••••••••••••	
Confirm Password	•••••••••••••	

Figure 2.73: 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 2.74). On the other hand, if the **Create a New Database** flag is set to **No**, then, in the **Existing database name** text box, mention the name of the existing database in which the eG manager will be storing metrics (see Figure 2.74). 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**.



Database Server Name/IP	192.168.10.101
Use Named Instance	○ Yes ● No
Database Server Port	1433
Windows Authentication	● Yes ○ No
NTLMV2 enabled	○ Yes ● No
SSL enabled	○ Yes ● No
Create a New Database	○ Yes ● No
Existing database name	egdb
eG Database User Name	DocMP
Password	••••••••
Confirm Password	••••••••

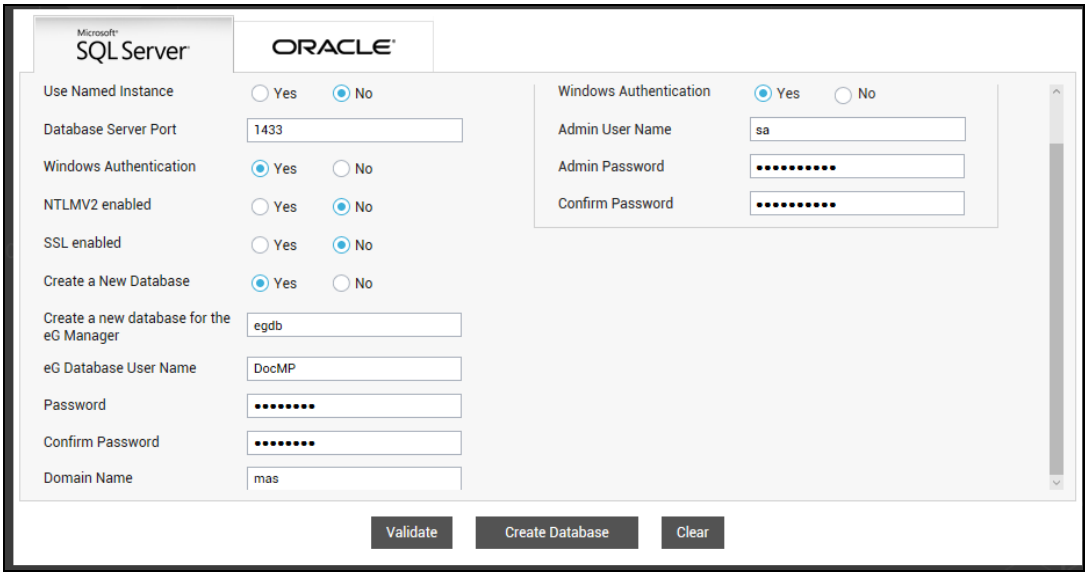
Figure 2.74: Using an existing database on the Microsoft SQL server as the eG database

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 manager - i.e., if you have set the **Create a New Database** flag to **Yes** and have specified a new **eG Database Name** (see Figure 2.75) - 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 2.75) - 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 2.75).

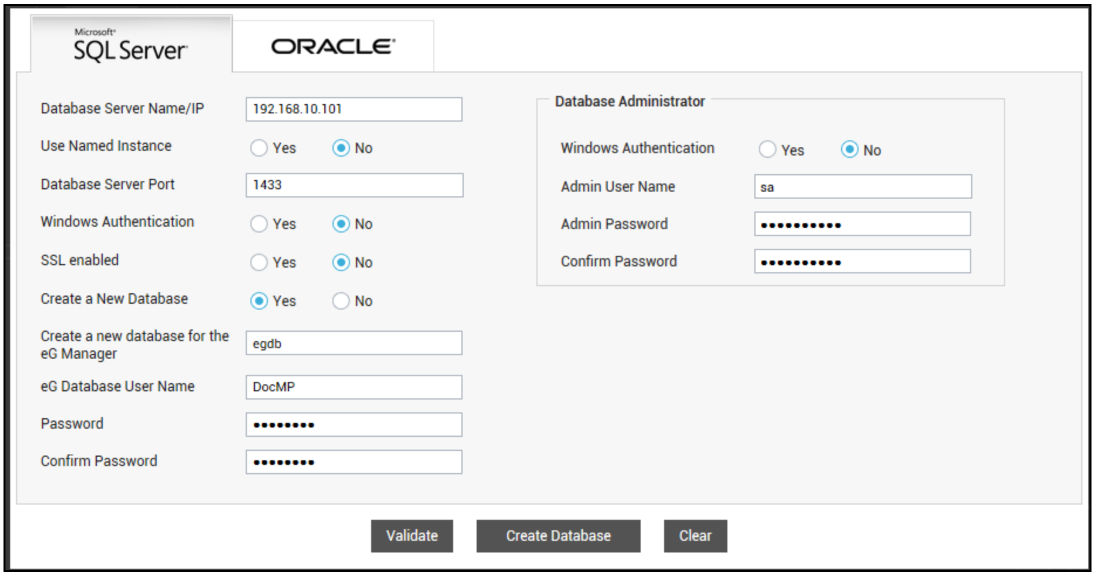


Use Named Instance ○ Yes ● No
Database Server Port: 1433
Windows Authentication ● Yes ○ No
NTLMV2 enabled ○ Yes ● No
SSL enabled ○ Yes ● No
Create a New Database ● Yes ○ No
Create a new database for the eG Manager: egdb
eG Database User Name: DocMP
Password: ••••••••
Confirm Password: ••••••••
Domain Name: mas

Windows Authentication ● Yes ○ No
Admin User Name: sa
Admin Password: ••••••••••
Confirm Password: ••••••••••

Figure 2.75: 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 2.76).



Database Server Name/IP: 192.168.10.101
Use Named Instance ○ Yes ● No
Database Server Port: 1433
Windows Authentication ○ Yes ● No
SSL enabled ○ Yes ● No
Create a New Database ● Yes ○ No
Create a new database for the eG Manager: egdb
eG Database User Name: DocMP
Password: ••••••••
Confirm Password: ••••••••

Database Administrator
Windows Authentication ○ Yes ● No
Admin User Name: sa
Admin Password: ••••••••••
Confirm Password: ••••••••••

Figure 2.76: 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

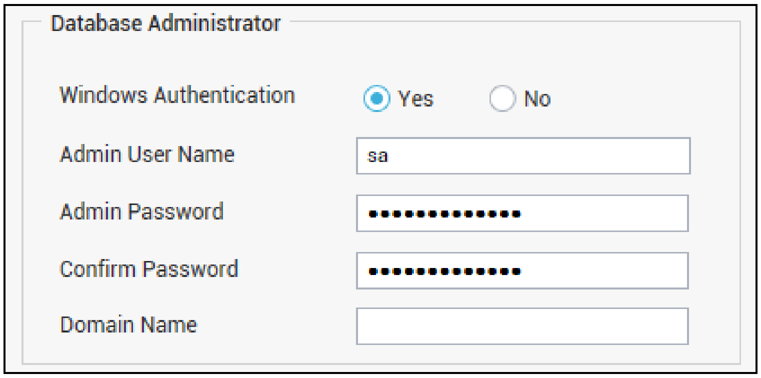
For instance, if the name of the special database user is **egdb**, then the password that you set for this user should be a **strong password** such as, **db123$%#@**.

Note that without a ‘strong password’, the eG manager 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 manager in step 7 above , then make sure you configure the **Database Administrator** section in Figure 2.76 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 2.77).



Database Administrator

Windows Authentication ● Yes ○ No

Admin User Name sa

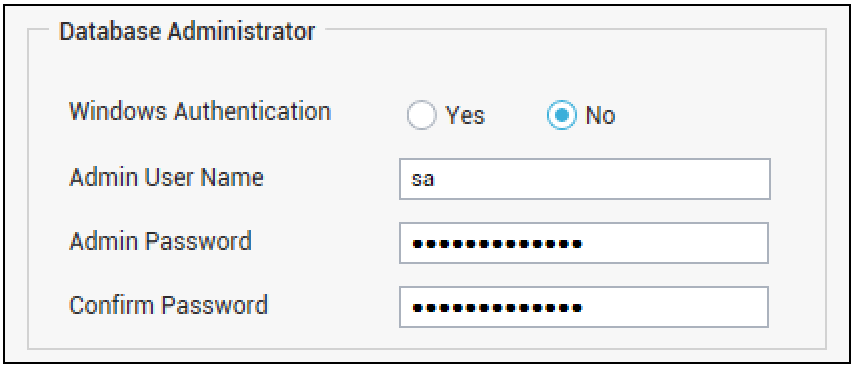
Admin Password •••••••••••••

Confirm Password •••••••••••••

Domain Name

Figure 2.77: 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 2.78).



Database Administrator

Windows Authentication ○ Yes ● No

Admin User Name sa

Admin Password ••••••••••••••

Confirm Password ••••••••••••••

Figure 2.78: 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 2.77. Figure 2.79, Figure 2.80, and Figure 2.81 depict how to create a new user with the aforesaid privileges using the **Microsoft SQL Server Management Studio**.

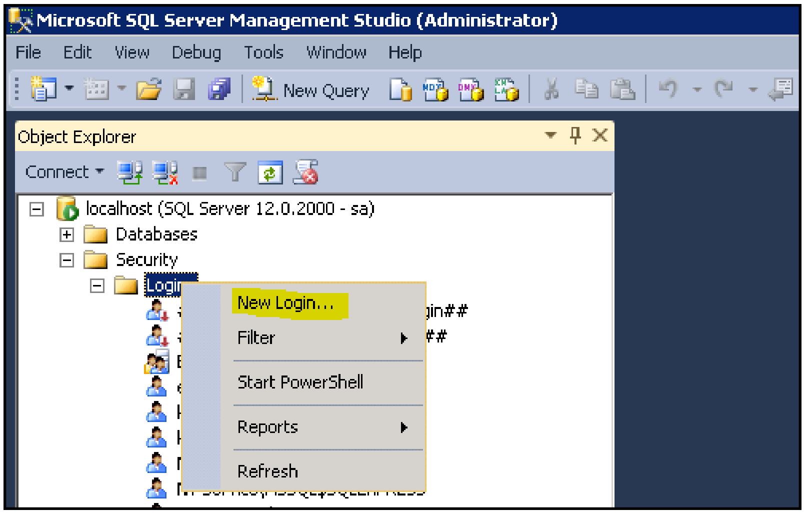
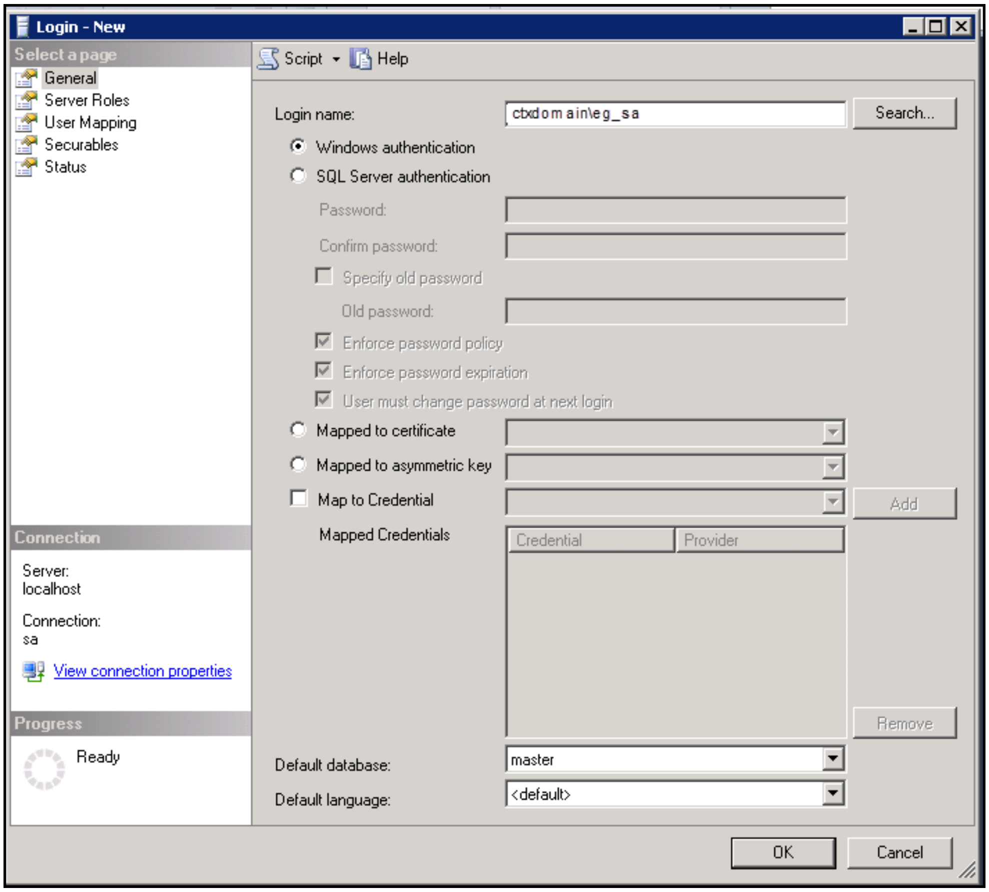

Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Object Explorer
Connect
localhost (SQL Server 12.0.2000 - sa)
Databases
Security
Logins
New Login...
Filter
Start PowerShell
Reports
Refresh

Figure 2.79: Choosing to create a new login



Login - New

Login name: ctxdomain\eg_sa

● Windows authentication

○ SQL Server authentication

Password:

Confirm password:

□ Specify old password

Old password:

☑ Enforce password policy

☑ Enforce password expiration

☑ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

Mapped Credentials

Credential	Provider

Default database: master

Default language: <default>

Connection

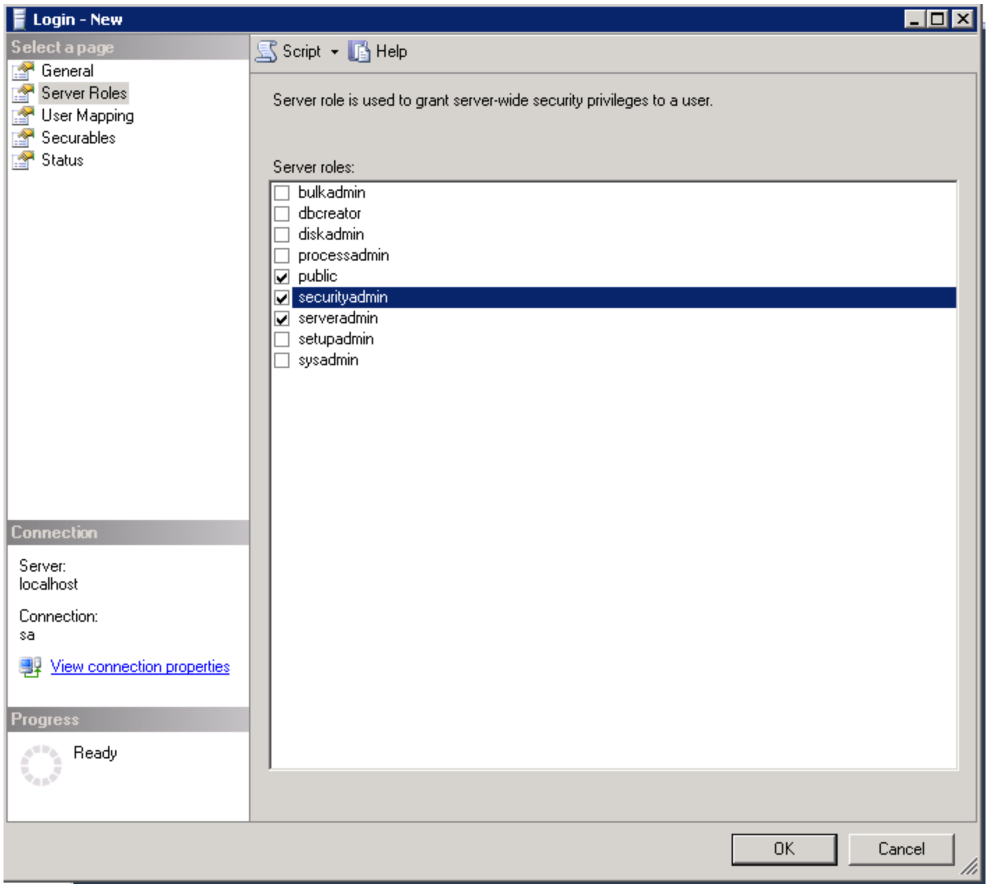
Server: localhost

Connection: sa

Progress

Ready

Figure 2.80: Creating a new user



Server role is used to grant server-wide security privileges to a user.

Server roles:

- ☐ bulkadmin
- ☐ dbcreator
- ☐ diskadmin
- ☐ processadmin
- ☑ public
- ☑ securityadmin
- ☑ serveradmin
- ☐ setupadmin
- ☐ sysadmin

Server:
localhost

Connection:
sa

Ready

Figure 2.81: 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 manager 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 2.76. 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 manager, 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 2.76. 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 2.76 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 2.76, 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 manager begins monitoring and alerting in no time! To know what these settings are and how to configure them, refer to Section **2.2.2.3**.

Note:

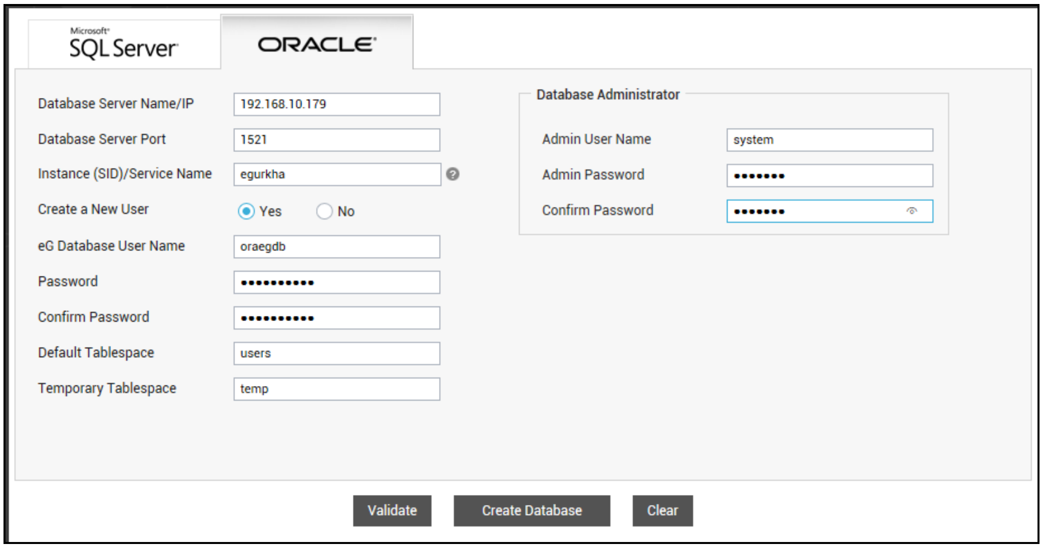
By default, the eG manager is configured for agent-based monitoring - i.e., when a server is auto-discovered and then managed, it is monitored in an agent-based manner. Administrators have an option to set agentless monitoring as the default for the eG manager.

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 manager. 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!
**************************************************************
```

2.2.2.2.2 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 2.82 will then appear.



Database Server Name/IP	192.168.10.179
Database Server Port	1521
Instance (SID)/Service Name	egurkha
Create a New User	● Yes ○ No
eG Database User Name	oraegdb
Password	••••••••••
Confirm Password	••••••••••
Default Tablespace	users
Temporary Tablespace	temp

Database Administrator

Admin User Name	system
Admin Password	•••••••
Confirm Password	•••••••

Figure 2.82: Configuring the eG database on an Oracle database server

To configure the eG database on Oracle, do the following using Figure 2.82:

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 manager should use. A Service Name is mandatory if a pluggable database is being used.

4. The eG manager 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 manager to use, first set the **Create a New User** flag in Figure 2.82 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:

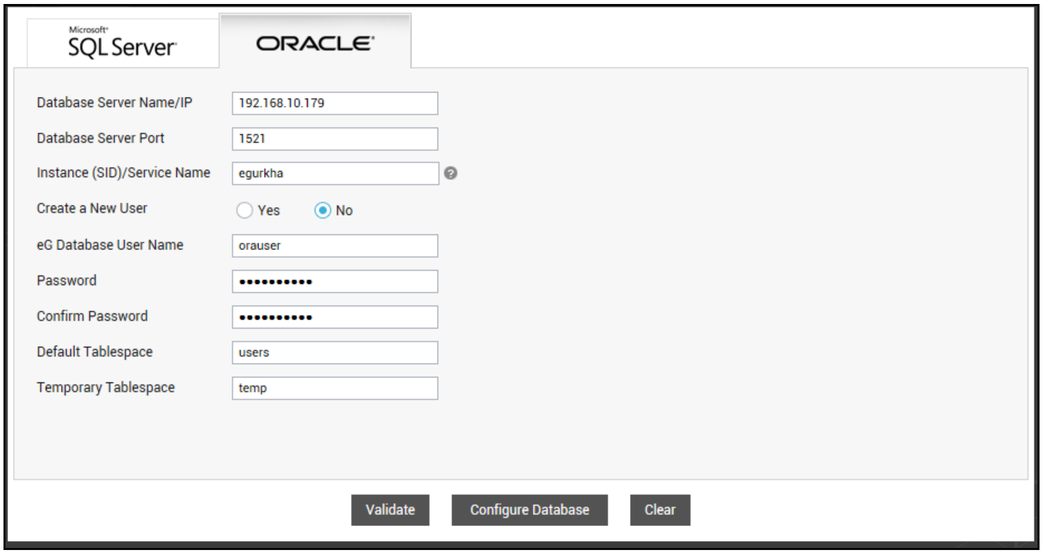
If the user chooses not to have the user account created by the configuration process, the user account has to be created manually on the Oracle database server with *connect, resource, and select_catalog* privileges. To know how to create such a user, refer to the table below, which describes the complete 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 $tspace1; For example: create user james identified by j@m3s default tablespace jdspace temporary tablespace jtspace; Grant connect, resource to james; Grant select_catalog_role to james; alter user james quota unlimited on jdspace;
Oracle 12C (and above) - Multi-tenant	alter session set container=$PDB_Name;

Version	Syntax for User Creation
Setup (PDB and CDB)	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 manager's use.

5. If you want to use an existing database user account for the eG manager, first set the **Create a New User** flag to **No** (see Figure 2.83). 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.



Database Server Name/IP	192.168.10.179
Database Server Port	1521
Instance (SID)/Service Name	egurkha
Create a New User	○ Yes ● No
eG Database User Name	orauser
Password	••••••••••
Confirm Password	••••••••••
Default Tablespace	users
Temporary Tablespace	temp

Figure 2.83: Configuring an existing database user account for the eG manager

Note:

If you set an existing database user as the eG database user at step 5, then before configuring the eG manager 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 2.82). 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 manager 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 manager 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.

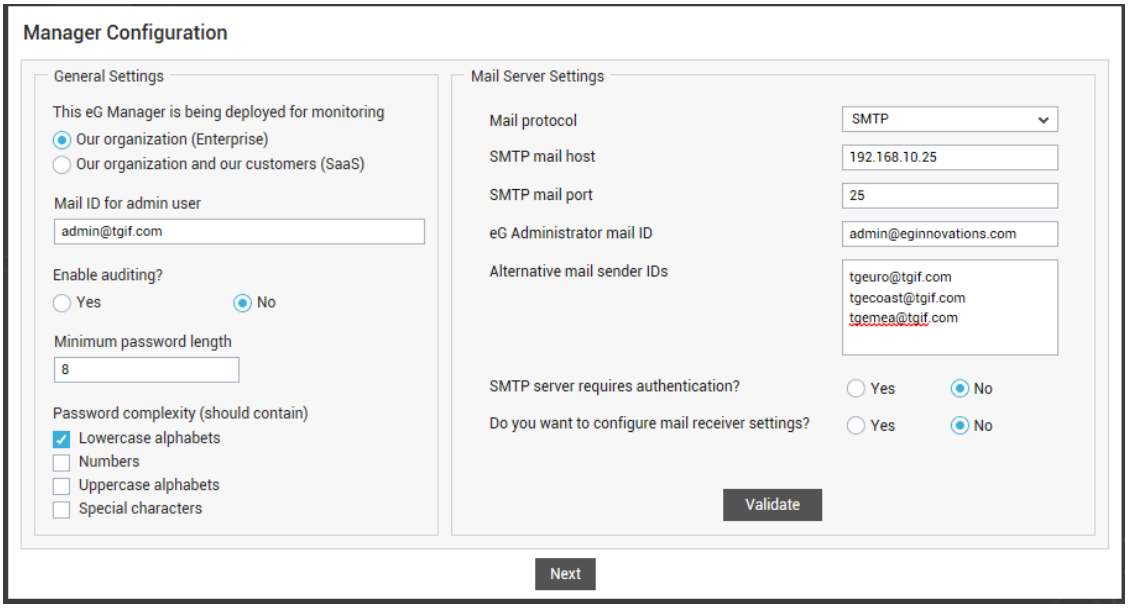
These parameters might have to be tuned further based on an increase in server load.

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 2.82 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 manager, then you will not have to provide database administrator credentials. In this case therefore, the **Database Administrator** section will not appear (see Figure 2.83).
8. To check the veracity of your configuration, click the Validate button in Figure 2.83. 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 manager, 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 2.82. 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 2.83) to configure the specified database user account for use by the eG manager.
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 2.82 or Figure 2.83 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 2.82, 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 manager begins monitoring and alerting in no time! To know what these settings are and how to configure them, refer to Section **2.2.2.3**.

2.2.2.3 Configuring the Basic Manager Settings

Once the eG database is successfully configured, setup automatically opens the **Manager Configuration** page (seeFigure 2.84). This page enables you to indicate what type of environment your eG manager deployment needs to monitor. Depending upon the type of environment, you can even turn on/off certain key capabilities of the eG manager 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 manager operations, without even logging into the eG management console!



Manager Configuration

General Settings

This eG Manager is being deployed for monitoring
● Our organization (Enterprise)
○ Our organization and our customers (SaaS)

Mail ID for admin user
admin@tgif.com

Enable auditing?
○ Yes ● No

Minimum password length
8

Password complexity (should contain)
☑ Lowercase alphabets
□ Numbers
□ Uppercase alphabets
□ Special characters

Mail Server Settings

Mail protocol	SMTP
SMTP mail host	192.168.10.25
SMTP mail port	25
eG Administrator mail ID	admin@eginnovations.com
Alternative mail sender IDs	tgeuro@tgif.com tgecoast@tgif.com tgemea@tgif.com
SMTP server requires authentication?	○ Yes ● No
Do you want to configure mail receiver settings?	○ Yes ● No

Figure 2.84: Configuring the basic manager settings

Using Figure 2.84, do the following:

1. First, choose the deployment model for the eG manager - Enterprise or SaaS. These models are briefly discussed below:

   - Enterprise: This model is ideal if your eG manager 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 manager - 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.

If you want to deploy the eG manager for Enterprise, then select the **Our Organization (Enterprise)** option in Figure 2.84.

- SaaS: This model is ideal if you are a Managed Service Provider (MSP), providing infrastructure hosting and management services to multiple customers. Monitoring is quiet often a cloud-based service that an MSP offers to each of their customers. If you are an MSP, you will want the eG manager to not just monitor your infrastructure, but also that of your customers. This means that an eG manager centrally deployed in the MSP infrastructure will be managing agents deployed in the customer infrastructure as well.

  The SaaS model also helps where a single eG manager manages agents used by different departments (eg., Development, Testing, Support etc.) / support groups (Europe Support, EMEA Support, USA Support etc.) / IT domains (Network administration, Database administration, Windows administration etc.).

  With the SaaS model, eG Enterprise fully supports mult-tenancy. Unlike the Enterprise model, in SaaS, the administrator will not be the sole custodian of administrative rights. Instead, these rights will be delegated to the individual tenants - say, MSP customers, department heads/workers, support personnel who are part of different support groups, or IT domain experts. The tenants are thus empowered to deploy the agents they want, manage the components they wish to monitor, and customize accesses, monitoring, and alerting based on the requirements of their infrastructure. The central administrator will continue to hold unrestricted administrative rights, which will enable him/her to manage monitoring licenses of the tenants, oversee performance and problems across tenant infrastructures, and even override a tenant's monitoring configuration if required.

  If you want to deploy the eG manager for SaaS, then select the **Our Organization and our customers (SaaS)** option in Figure 2.84.

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 manager 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 manager 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 2.84, you can also enable/disable audit logging for your eG manager. An audit log can be best described as a simple log of changes, typically used for tracking temporal information. The eG manager 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 2.84).

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 2.84, 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 2.84.

Note:

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

5. Then, proceed to configure **Mail Server Settings**. Here, you provide details of the mail server that eG should use for sending emails. This specification is optional for an Enterprise deployment, but is mandatory for a SaaS deployment.

   In case of an Enterprise deployment, you need to configure a mail server only if you want to enable email alerting - i.e., only if you want your users to receive problem alerts by email. If you do not want to enable email alerting, then the mail server settings need not be defined.

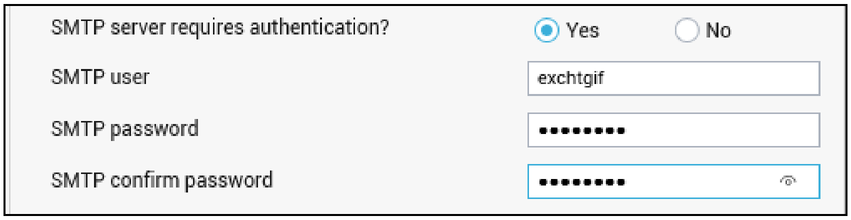
   In case of a SaaS deployment on the other hand, it is mandatory to configure a mail server. This is because, without a mail server, verification codes cannot be emailed to MSP customers who attempt to register with the eG manager. In the absence of a verification code, the registration will fail. As a result, eG Enterprise will be unable to monitor customer environments for the MSP.

   To configure a mail server, specify the following:

   - The protocol through which you wish to transmit or send the outgoing mail messages across the Internet Protocol (IP) networks has to be selected from the **Mail protocol** list box. The **SMTP** option would be selected by default in this list box. If the mail server through which you wish to send the mail messages is **SSL-enabled**, then select, **SMTP-SSL** from the **Mail protocol** list box. If your mail server offers enhanced security and provides certificate based authentication, select the **SMTP-TLS** option from the **Mail protocol** list.
   - The identity (IP address or host name) of the mail server to be used by the eG manager for generating alarms has to be entered in the **SMTPmail host** text box. The port at which the mail host listens has to be provided in the **SMTP mail port** text box.
   - In MSP environments typically, different support groups are created to address performance issues relating to different customers. These support groups might prefer to receive problem intimation from customer-specific mail IDs instead of the global admin mail ID, so that they can instantly identify the customer environment that is experiencing problems currently. Moreover, this way, every support group will be enabled to send status updates on reported issues directly to the concerned customer, instead of overloading the admin mailbox. To facilitate this,

Figure 2.84 allows the administrator to configure multiple **Alternative Mail sender IDs** - normally, one each for every customer in case of an MSP environment. While configuring multiple sender IDs in the space provided, ensure that you press the **Enter** key on your keyboard after every mail ID. This way, every ID will occupy one row of the text area. Later, while creating a new user using the eG administrative interface, the administrator can select one of these configured sender IDs from the **Mail sender** list and assign it to the new user. This ensures that all email alerts received by the user are generated by the chosen ID only.

- If the mail server requires users to login before sending mails, then select the **Yes** option against the **SMTP server requires authentication?** field. By default, authentication is set to **No**. Upon selecting **Yes**, you will be required to provide a valid **SMTP user** name and **SMTP password** for logging into the mail server. Confirm the password by retyping it in the **SMTP confirm password** text box.



SMTP server requires authentication? ● Yes ○ No

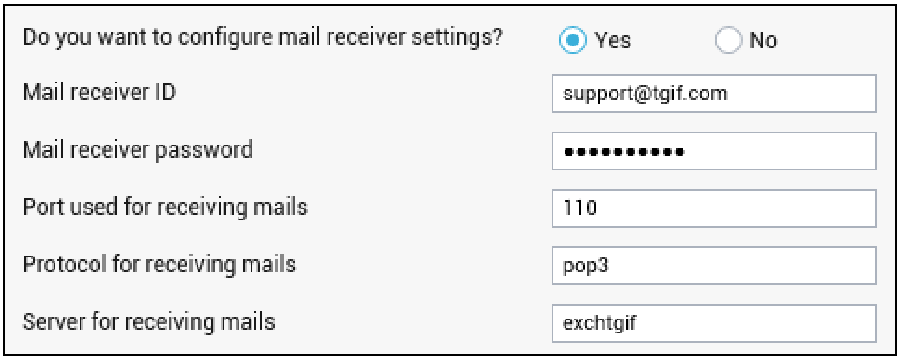
SMTP user: exchtgif

SMTP password: ••••••••

SMTP confirm password: ••••••••

Figure 2.85: Configuring the SMTP login credentials, if SMTP server requires authentication

- To safeguard from spam, some mail servers are configured so that they will allow mails to be sent from a system only if that system is also used to receive mails. To allow the eG manager to use such mail servers to send email alerts, additional configuration is needed. In such a case, select the **Yes** option against the **Do you want to configure mail receiver settings?** field.



Do you want to configure mail receiver settings? ● Yes ○ No

Mail receiver ID: support@tgif.com

Mail receiver password: •••••••••••

Port used for receiving mails: 110

Protocol for receiving mails: pop3

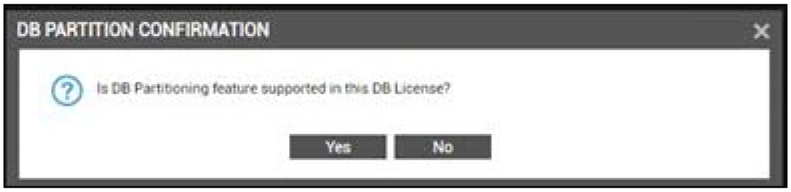
Server for receiving mails: exchtgif

Figure 2.86: Configuring mail receiver settings

By default this field is set to **No**. When you enable this authentication to **Yes**, you need to specify the following details in the corresponding text boxes (see Figure 2.86):

- ○ **Mail receiver ID:** Specify the login name to be used for receiving mails.
- ○ **Mail receiver password:** The password of the mail receiver needs to be specified here.
- ○ **Port used for receiving mails:** The port number on the mail server to which the mail manager connects needs to be provided here.
- ○ **Protocol for receiving mails:** Mention the protocol used for receiving mails. The protocol can be either POP3 or IMAP
- ○ **Server for receiving mails**: Specify the server to which the mail manager will connect to receive mails.

- To verify whether/not your mail server settings are correct, click the **Validate** button in Figure 2.84. This brings incorrect/invalid specifications to your notice, so you can amend them. Once validation is successful, click the **Next** button in Figure 2.84 to proceed.
- If you have configured an Oracle database backend for the eG manager, thenFigure 2.87 will appear.

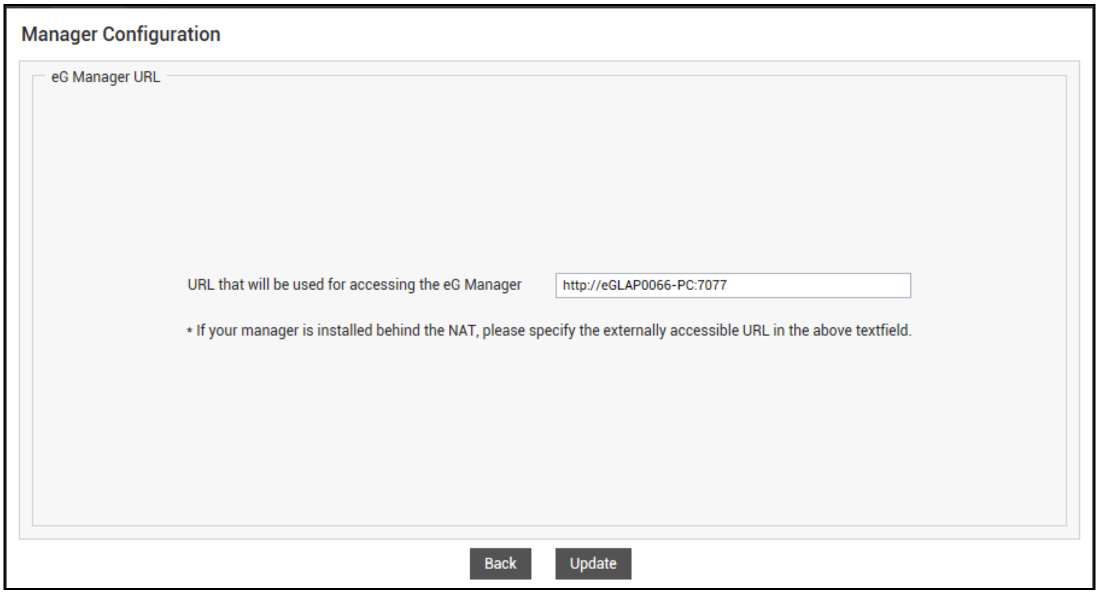


Is DB Partitioning feature supported in this DB License?

Figure 2.87: 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 manager 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 2.87 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 manager 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 2.87. 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 2.88 will then appear, displaying the URL using which the eG manager should be accessed. The default URL will be of the format http://<eGManagerIPorHostName>:<eGManagerPort> or https://<eGManagerIPorHostName>:<eGManagerPort>, depending upon whether/not the manager is SSL-enabled. If your eG manager is behind the NAT, then you may want to replace the default URL with the externally accessible URL. Then, click the **Update** button.



Manager Configuration

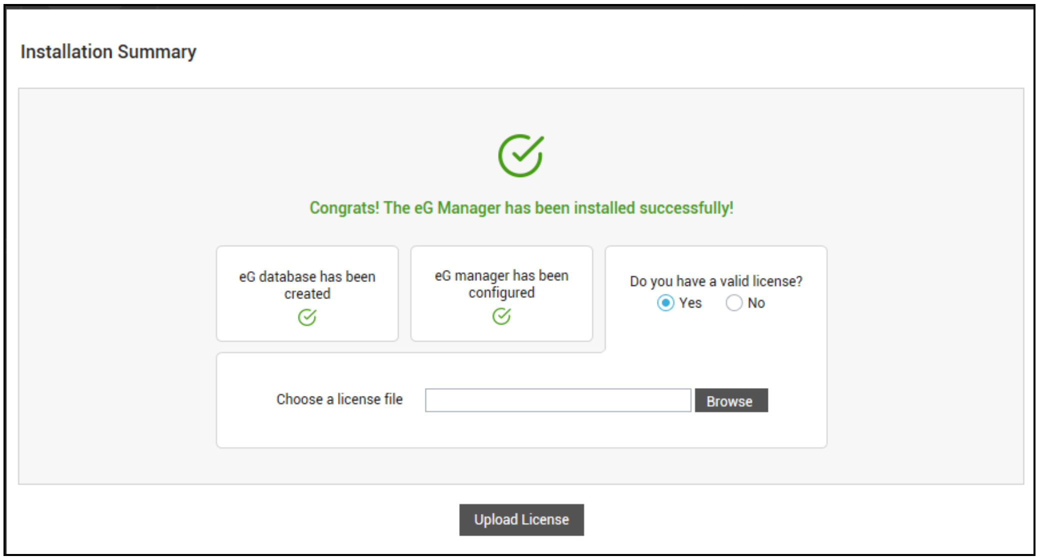
eG Manager URL

URL that will be used for accessing the eG Manager: http://eGLAP0066-PC:7077

* If your manager is installed behind the NAT, please specify the externally accessible URL in the above textfield.

Figure 2.88: The URL that will be used for accessing the eG manager

- Figure 2.89 will then appear informing you of the successful installation of the eG manager. 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.



Installation Summary

Congrats! The eG Manager has been installed successfully!

eG database has been created ✓

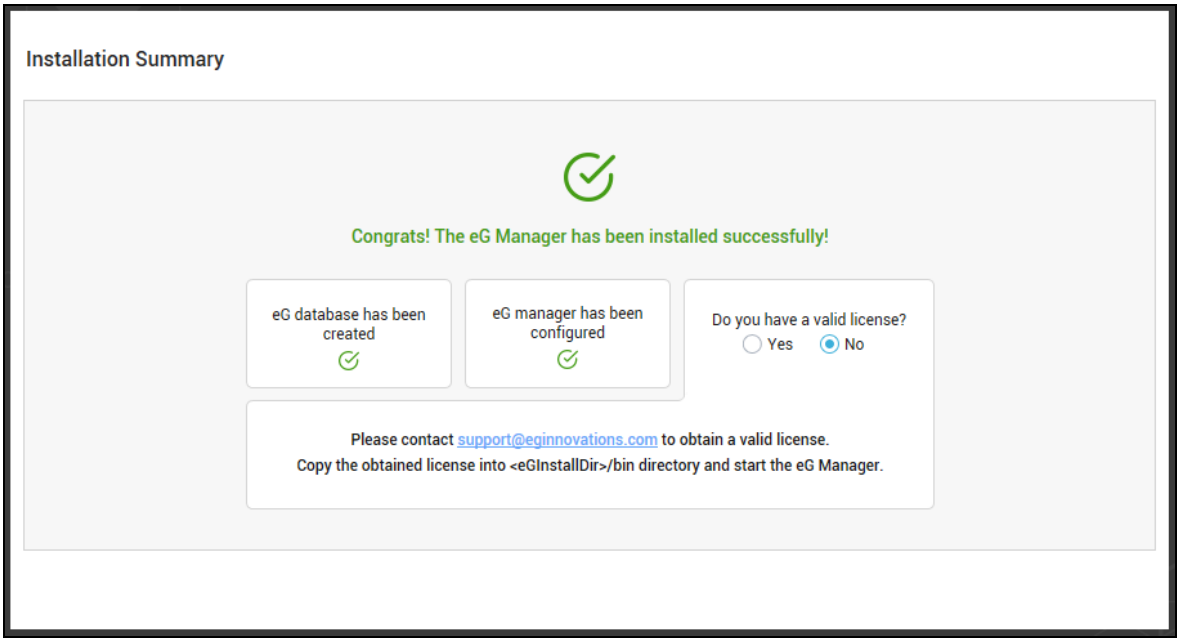
eG manager has been configured ✓

Do you have a valid license? ● Yes ○ No

Choose a license file

Figure 2.89: 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 2.90). 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 /opt/egurkha/bin folder. Then, start the manager.



Installation Summary

Congrats! The eG Manager has been installed successfully!

eG database has been created ✓

eG manager has been configured ✓

Do you have a valid license? ○ Yes ● No

Please contact support@eginnovations.com to obtain a valid license.
Copy the obtained license into <eGInstallDir>/bin directory and start the eG Manager.

Figure 2.90: Requesting a valid license

2.2.3 Configuring Manager Redundancy

If you had not chosen to configure manager redundancy while configuring the eG manager, then you can do so at a later point in time, by executing the **setup_cluster** script in the **/opt/egurkha/bin** directory. To execute the script, do the following:

1. First, login as the eG user.
2. From the command prompt, move to the **/opt/egurkha/bin** directory, and execute the following command: **./setup_cluster**.
3. Upon execution, the **setup_cluster** script will first request for the location of the Java home directory.

   ```
   Please enter the location of your Java home directory []: /usr/jdk1.8
   ```

4. Once the location is specified, setup will request your confirmation to proceed with enabling manager redundancy.

   ```
   Would you like to enable eG Manager Redundancy y/n [n]? y
   ```

5. While specifying **n** at step 4 will terminate the script execution, entering **y** will enable you to proceed with the setup by providing the IP (or hostname) and port number of the manager being configured.

   ```
   Please enter the hostname (or IP address) of this host: 192.168.10.87
   Please enter the port at which this eG Manager listens: 7077
   ```

   Note:

   - If an eG manager (primary/secondary) in a cluster supports only an IPv6 address, then its best that you configure redundancy for that manager using its hostname and not its IP address.
   - If the eG manager is configured using the hostname, then ensure that cluster setup is also performed using the hostname only. Likewise, if the eG manager is configured using the IP address, then ensure that cluster setup is also performed using the IP address alone.

6. Once the IP and port are provided, steps 10 to 20 of Section **2.2.2.1** will follow.

2.2.4 Installing the eG Manager on Privileged Ports

On Unix, all ports below 1024 are privileged ports. Only super users or users authorized to access this port will be able to bind to these ports. If you wish to have the eG manager listening on a privileged port, you will need to follow the procedure listed below.

When the eG manager is installed on Solaris 10 or higher, you can install the eG manager and have it configured to listen to a privileged port (e.g., 80 or 443). Before starting the manager, login to the Solaris server as a super-user and run the following command to instruct the operating system to allow the eG user to open a privileged port:

```
usermod -K defaultpriv=basic,net_privadd <eG_user>
```

Log out and log back in as the eG user, and then, start the eG manager.

On Linux systems, follow the steps below:

a. Install the eG manager on a port higher than 1024 – e.g., 7077.

b. Use the **iptables** command to set up redirection from a privileged port to the port that the eG manager is using. For example, suppose you have installed the eG manager on port 7077 with SSL support and you would like the manager to listen on port 443; then, do the following:

   - Start the Manager on port 7077 using the **start_manager** command.
   - Execute the iptables command as below on the Linux system hosting the eG manager. These **commands should be executed from a super-user account**.

     ```
     iptables -t nat -A OUTPUT -d <IP/HostName of the eG Manager> -p tcp—dport 443 -j
     REDIRECT—to-ports 7077
     iptables -t nat -A PREROUTING -d <IP/HostName of the eG Manager> -p tcp—dport
     443 -j REDIRECT—to-ports 7077
     ```

   - Once these commands are executed, the eG manager will be accessible on port 443 as well.

c. Entries configured using iptables are lost when the manager reboots. To save the iptables configuration, do the following:

   - Run the following command as root user:

     ```
     /sbin/iptables-save > /opt/egurkha/iptables.fw
     ```

   - Edit the file **/etc/rc.local** and append the following line to this file

     ```
     /sbin/iptables-restore < /opt/egurkha/iptables.fw
     ```

Now, even if the eG manager system is rebooted, the iptables configuration is restored.

2.2.4.1 Configuring Tomcat to Listen on Multiple Ports

By default, Tomcat listens on port 8080. However, if you want to configure Tomcat to listen on say, port 8081 as well, follow the steps below:

1. Edit the **server.xml** file in the <CATALINA_HOME>\conf directory on the eG manager host.
2. Look for the following lines in the **server.xml** file:

   ```
   <Connector port=”8080” protocol=”HTTP/1.1”
   ```

   ```
   connectionTimeout=”20000”
   ```

   ```
   redirectPort=”5443” />
   ```

3. Replace the above-mentioned lines with the following lines:

   ```
   <Connector port=”8080”
   maxThreads=”150” minSpareThreads=”25” maxSpareThreads=”75”
   enableLookups=”false” redirectPort=”8443” acceptCount=”100”
   debug=”0” connectionTimeout=”20000”
   disableUploadTimeout=”true” />

   <Connector port=”8081”
   maxThreads=”150” minSpareThreads=”25” maxSpareThreads=”75”
   enableLookups=”false” redirectPort=”8443” acceptCount=”100”
   debug=”0” connectionTimeout=”20000”
   disableUploadTimeout=”true” />
   ```

   Upon startup, Tomcat will parse the server.xml file and create objects based on the content of the file. A single Connector element specification in the **server.xml** file will hence cause Tomcat to create a Connector object. If you then update the file with another Connector element specification, it will automatically trigger the creation of another instance of the Connector. This is how the above change creates two connectors listening on port 8080 and 8081 respectively. You only have one container though. The connectors create a request and response object for each incoming HTTP request and pass it to the container.

4. Then, save the file.
5. Finally, restart the Tomcat server.

2.2.5 Starting eG Manager

To start the manager, execute the command **/opt/egurkha/bin/start_manager**.

The following message appears when the manager starts successfully:

```
$ ./start_manager
5
Starting the eG manager components ...
Please wait ...
Starting the admin components . . .
Starting the monitor components . . .
Starting the eghelp components . . .
Initializing the eG manager . . .

******************************************************************
The eG manager 5 has been started successfully!
******************************************************************
```

If the manager fails to start, the following message appears.

```
Failed to start the eG manager! ...
Possible reasons for this could be:
(i)Your license located in the file: /opt/egurkha/bin/license may be invalid...
Please check the file "/opt/egurkha/manager/logs/error_log" for details.
(ii)You may not have permissions to start the eG manager...
Please check the permissions for the directory "/opt/egurkha/manager".
```

2.2.6 Increasing the Memory of the eG Manager Process

The eG manager runs as a Java process. Typically, 1/3rdof the total system memory is the maximum heap memory that can be allocated to the eG manager process.

Where a large number of components are to be monitored, you may want to allocate more memory heap to the eG manager process. On a Unix manager, follow the steps below to modify the heap memory allocation:

1. Login to the eG manager host. Edit the **catalina.sh** file in the **/opt/egurkha/manager/tomcat/bin** directory.
2. Search for the entry *JvmMx* in the file. You will then find an entry that reads as follows:

   JvmMx <Heap_memory_allocation_to_manager> –JvmMs <Heap_memory_allocation_to_manager>

3. The *JvmMx* and *JvmMs* specifications govern the heap memory allocations to the eG manager. If

you want to increase it to say, 2 GB, change these specifications as indicated below:

JvmMx 2048 –JvmMs 2048

4. Finally, save the file.

While overriding the default heap memory allocations to the eG manager process, ensure that the allocated heap memory is not greater than the total memory capacity of the eG manager host.

2.2.7 Uninstalling eG Enterprise

The process of uninstalling eG Enterprise varies depending on the operating system used. The steps to be executed to uninstall eG Enterprise are as follows:

1. First stop the execution of the manager using the command:

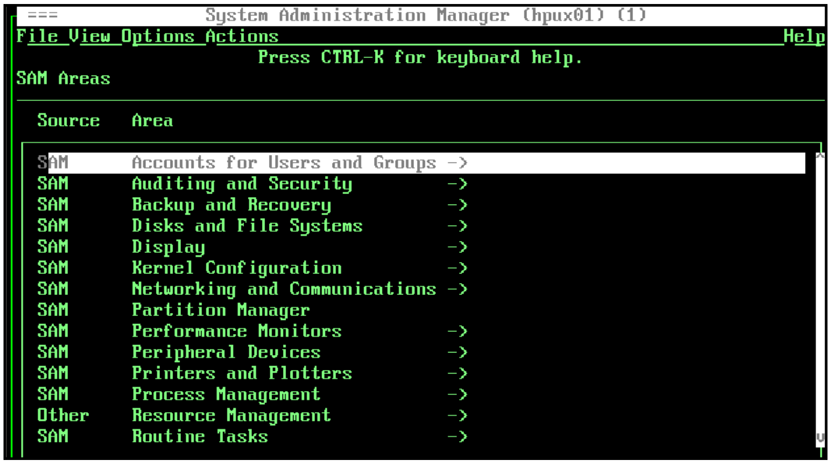
   /opt/egurkha/bin/stop_manager

2. Next, stop the execution of the agent using the command:

   /opt/egurkha/bin/stop_agent

3. Next, on Solaris, use the **pkgrm** command to uninstall the eGmanager and eGagent packages.
4. On Linux and AIX, the **/opt/egurkha** directory has to be manually removed to uninstall the eG Enterprise system.
5. On HP-UX, uninstall the eG agent following the steps given below:

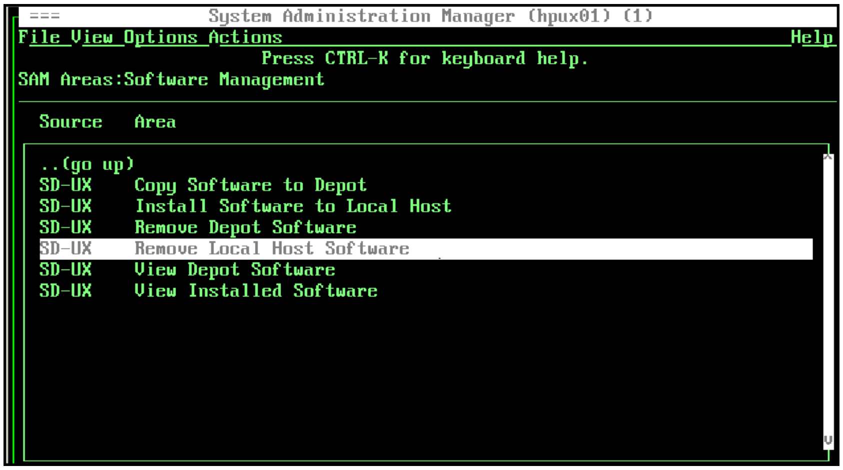
   - The eG agent can be uninstalled only by a super-user. Therefore, login as the super-user and run the command **sam**.
   - Now, press the **Enter** key on the keyboard. A screen depicted by Figure 2.91 below appears next.



```
 ===          System Administration Manager (hpux01) (1)
File View Options Actions                                          Help
                      Press CTRL-K for keyboard help.
SAM Areas

  Source    Area

  SAM       Accounts for Users and Groups ->
  SAM       Auditing and Security         ->
  SAM       Backup and Recovery           ->
  SAM       Disks and File Systems        ->
  SAM       Display                       ->
  SAM       Kernel Configuration          ->
  SAM       Networking and Communications ->
  SAM       Partition Manager
  SAM       Performance Monitors          ->
  SAM       Peripheral Devices            ->
  SAM       Printers and Plotters         ->
  SAM       Process Management            ->
  Other     Resource Management           ->
  SAM       Routine Tasks                 ->
```

Figure 2.91: Selecting the Software Management option

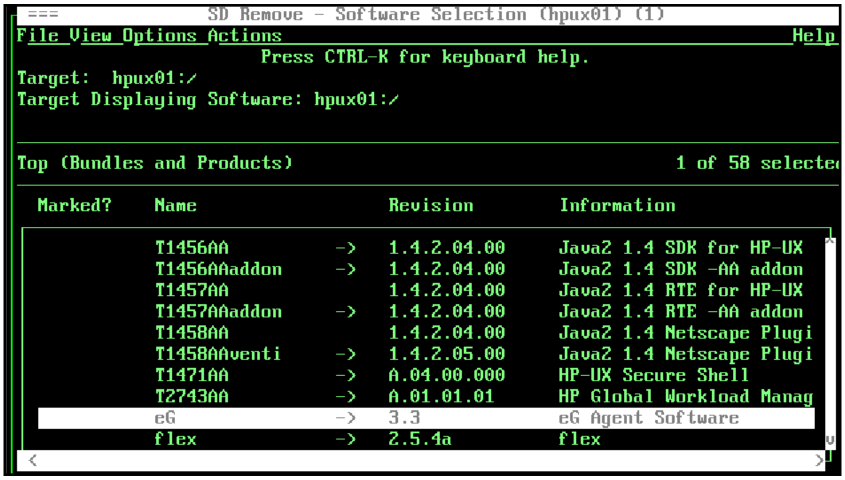
- Using the down-arrow key on the key board, select the **SD-UX Software Management** option from Figure 2.91, and then press Enter.
- Using the next screen (see Figure 2.92), choose to remove the eG agent software executing on the local host, by selecting the **Remove Local Host Software** option. To select this option, use the down-arrow key until the option is reached, and then press the **Enter** key.



```
 ===          System Administration Manager (hpux01) (1)
File View Options Actions                                          Help
                      Press CTRL-K for keyboard help.
SAM Areas:Software Management

  Source    Area

  ..(go up)
  SD-UX     Copy Software to Depot
  SD-UX     Install Software to Local Host
  SD-UX     Remove Depot Software
  SD-UX     Remove Local Host Software
  SD-UX     View Depot Software
  SD-UX     View Installed Software
```

Figure 2.92: Choosing to remove a software on the local host

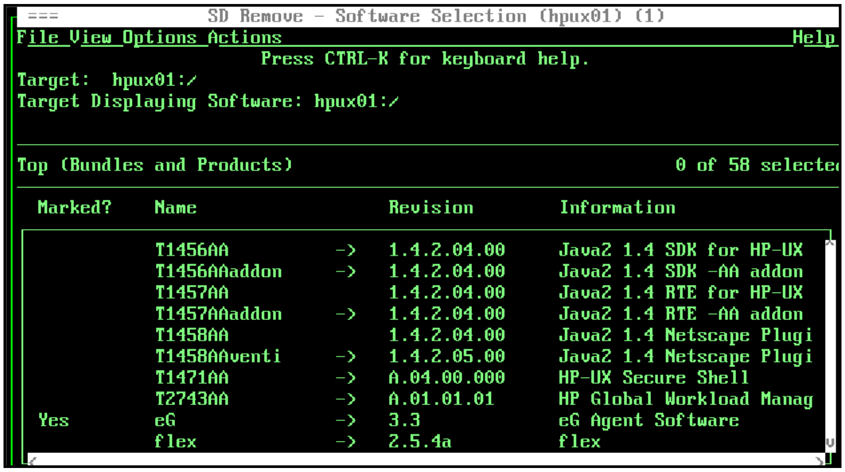
- From the screen that appears next, select the eG Agent software to be removed. To remove the selected eG agent software, first, mark it for removal by pressing the "**m**" key on the keyboard (see Figure 2.93).



```
 ===              SD Remove - Software Selection (hpux01) (1)
File View Options Actions                                        Help
                       Press CTRL-K for keyboard help.
Target:  hpux01:/
Target Displaying Software: hpux01:/

Top (Bundles and Products)                                1 of 58 selecte

  Marked?     Name                  Revision          Information

              T1456AA         ->    1.4.2.04.00       Java2 1.4 SDK for HP-UX
              T1456AAaddon    ->    1.4.2.04.00       Java2 1.4 SDK -AA addon
              T1457AA               1.4.2.04.00       Java2 1.4 RTE for HP-UX
              T1457AAaddon    ->    1.4.2.04.00       Java2 1.4 RTE -AA addon
              T1458AA               1.4.2.04.00       Java2 1.4 Netscape Plugi
              T1458AAventi    ->    1.4.2.05.00       Java2 1.4 Netscape Plugi
              T1471AA         ->    A.04.00.000       HP-UX Secure Shell
              T2743AA         ->    A.01.01.01        HP Global Workload Manag
              eG              ->    3.3               eG Agent Software
              flex            ->    2.5.4a            flex
```

Figure 2.93: Marking the eG agent software for deletion

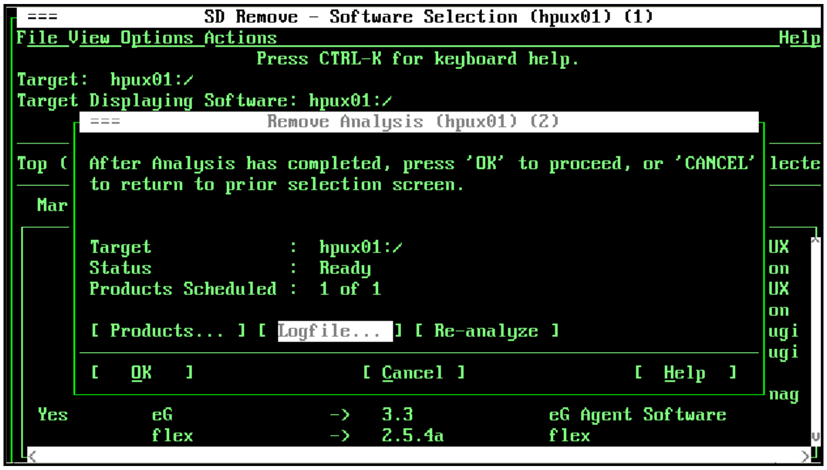
- Then, press the **Tab** key and choose *Actions* -> *Remove* as depicted by Figure 2.94 below.



```
 ===              SD Remove - Software Selection (hpux01) (1)
File View Options Actions                                        Help
                       Press CTRL-K for keyboard help.
Target:  hpux01:/
Target Displaying Software: hpux01:/

Top (Bundles and Products)                                0 of 58 selecte

  Marked?     Name                  Revision          Information

              T1456AA         ->    1.4.2.04.00       Java2 1.4 SDK for HP-UX
              T1456AAaddon    ->    1.4.2.04.00       Java2 1.4 SDK -AA addon
              T1457AA               1.4.2.04.00       Java2 1.4 RTE for HP-UX
              T1457AAaddon    ->    1.4.2.04.00       Java2 1.4 RTE -AA addon
              T1458AA               1.4.2.04.00       Java2 1.4 Netscape Plugi
              T1458AAventi    ->    1.4.2.05.00       Java2 1.4 Netscape Plugi
              T1471AA         ->    A.04.00.000       HP-UX Secure Shell
              T2743AA         ->    A.01.01.01        HP Global Workload Manag
  Yes         eG              ->    3.3               eG Agent Software
              flex            ->    2.5.4a            flex
```

Figure 2.94: Selecting the Remove option from the Actions menu

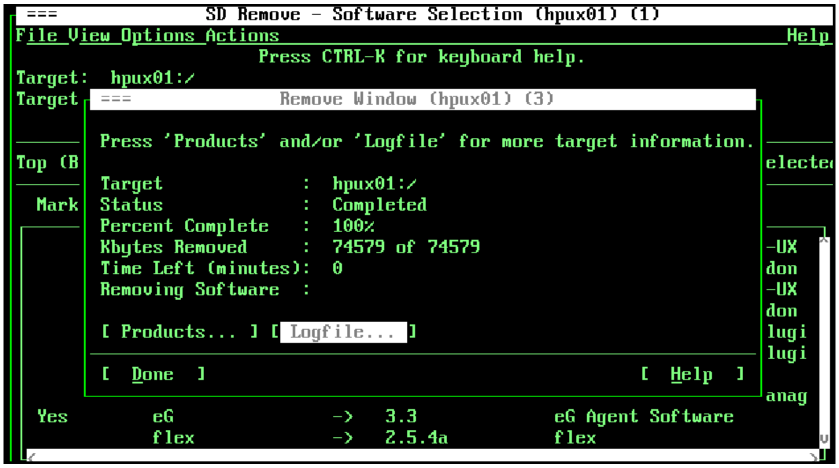
- Then, press the **Enter** key and wait until the **Status** of the remove analysis changes to **Ready** (see Figure 2.95). Then, using the **Tab** key, choose the **OK** button to confirm deletion of the selected eG software.



```
===              SD Remove - Software Selection (hpux01) (1)
File View Options Actions                                          Help
                  Press CTRL-K for keyboard help.
Target:  hpux01:/
Target Displaying Software: hpux01:/
      ===             Remove Analysis (hpux01) (2)

Top ( After Analysis has completed, press 'OK' to proceed, or 'CANCEL' lecte
      to return to prior selection screen.
  Mar

      Target             :  hpux01:/                                UX
      Status             :  Ready                                   on
      Products Scheduled :  1 of 1                                  UX
                                                                    on
      [ Products... ] [ Logfile... ] [ Re-analyze ]                 ugi
                                                                    ugi
      [   OK   ]             [ Cancel ]            [  Help  ]
                                                                    nag
  Yes        eG          ->    3.3           eG Agent Software
             flex        ->    2.5.4a        flex
```

Figure 2.95: Confirming removal of the eG software by selecting the OK button

- Once the software is removed, status will become **Completed** (see Figure 2.96). Now, click the **Done** button, specified by an arrow in the figure.



```
===              SD Remove - Software Selection (hpux01) (1)
File View Options Actions                                          Help
                  Press CTRL-K for keyboard help.
Target:  hpux01:/
Target ===             Remove Window (hpux01) (3)

       Press 'Products' and/or 'Logfile' for more target information.
Top (B                                                               electe
       Target              :  hpux01:/
  Mark Status              :  Completed
       Percent Complete    :  100%
       Kbytes Removed      :  74579 of 74579                         -UX
       Time Left (minutes):  0                                       don
       Removing Software   :                                         -UX
                                                                     don
       [ Products... ] [ Logfile... ]                                lugi
                                                                     lugi
       [  Done  ]                                      [  Help  ]
                                                                     anag
  Yes        eG          ->    3.3           eG Agent Software
             flex        ->    2.5.4a        flex
```

Figure 2.96: Status changing to Completed

- Finally, exit the uninstall process using the menu sequence: *File -> Exit SAM.*

Note:

If an agent monitoring a web server is uninstalled, then the web adapter should be manually removed. To do so, open the **httpd.conf** file (in the <WEB_SERVER_HOME_DIR>/conf directory) of the web server, and comment the LoadModule egurkha_module entry and the AddModule mod_egurkha entry.

2.3 SSL-Enabling the eG Manager

The eG Web Console is accessed via different browsers (Recommended Browser Settings for the eG Manager). To establish secure connections with the browsers, eG Enterprise allows you to enable the SSL certificate for the eG manager. Doing so will instantly enable the eG agent to communicate with the eG manager via secure protocol HTTPS. This will ensure secure data transfer between the eG agent and eG manager.

The detailed procedure for enabling the SSL for the eG manager on Windows and Unix is explained in the following sections:

- Section **2.4**
- Section **2.8.1**

2.4 SSL-Enabling the eG Manager on Windows

The eG manager on Windows includes a default SSL certificate. If you SSL-enable the eG manager using this default certificate, then all you need to do is click the **Yes** button when the eG manager setup process requests you to indicate whether the manager is to be SSL-enabled or not. Doing so will instantly enable the eG agent to communicate with the eG manager via HTTPS.

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

a. You can obtain a signed certificate from an internal certifying authority (eg., Microsoft Active Directory Certificate Services) and use this certificate to SSL-enable the eG manager, (OR)

b. You can obtain a signed certificate from a valid, external certifying authority (eg., Verisign) and use this certificate to SSL-enable the eG manager

If you go with option (a), use the procedure detailed in the Section **2.8.0.1** topic. If you pick option (b), use the procedure detailed in Section **2.8.1.3** topic.

the SSL-enabled eG manager uses TLS 1.2 protocol to communicate with the eG agent, secondary manager or any target host. By default, the eG manager is bundled with the latest version of Tomcat server and uses JDK 1.8 or its variants. Since the JDK 1.8 uses TLS 1.2 as default, the eG manager responds only to the communications made through TLS 1.2. Therefore, it is apparent that the communication to the eG manager is possible only if the eG agent/ runs on JRE 1.8 or its variants.

This means that the eG manager will respond only when the eG agent communicates via the TLS 1.2.

Likewise, the eG agent also uses TLS 1.2 to communicate the eG manager when it runs on the JRE version 1.8 or its variants. If the eG agent is bundled with the earlier versions of JRE which don't support TLS 1.2 by default, the eG manager will not respond as the connection is not secure. To avoid this, eG allows administrators to enforce the eG agent to use TLS 1.2 when it runs on the earlier version of JRE. **Note that the minimum JRE requirement for enabling the eG manager-agent communication over TLS 1.2 is 1.7**.

For instance, let's say that the eG agent is running on JRE 1.7 and trying to communicate with the eG manager through the earlier version of TLS protocol such as TLS 1.0 or 1.1. Here, the eG manager-agent communication will not happen as the TLS version of the eG agent is not complied with that of the eG manager. In such cases, follow the steps provided in the sections below to enable the eG agent to use TLS 1.2.

2.5 Upgrading TLS version

To provide higher level of security, the eG manager 7.1 is bundled with the Tomcat server 9.x and open JDK 10. The open JDK 10 uses TLS 1.2 as a default protocol to establish more secure connection. This implies that the eG manager is enabled by default to use TLS 1.2 for communicating with the eG agent or any target host. When the eG agent 6.3.1 is trying to communicate with the eG manager 7.1, it uses any of the earlier versions of TLS such as TLS 1.0 or 1.1. In this case, the eG manager-agent communication will not happen since the eG manager will not respond to the communication made through the earlier versions of TLS protocol. To avoid this, you may need to enforce the eG agent 6.3.1 to use TLS 1.2 by editing the **start_agent** script in the /opt/egurkha/bin directory. The steps for enabling the eG agent to use TLS 1.2 are explained in the sections below .

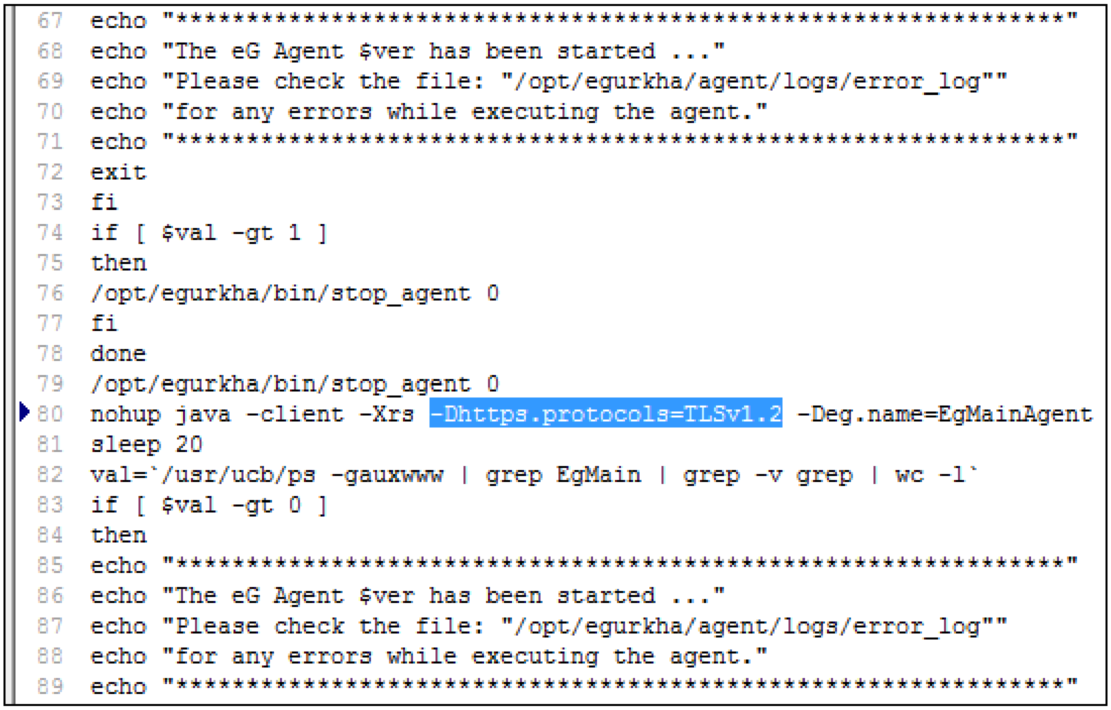
The eG manager 7.1 is bundled with the Tomcat server 9.x and OpenJDK 10 that uses TLS 1.2 as default to establish secure connections. This implies that the SSL-enabled eG manager 7.1 will use TLS 1.2 as a default communication protocol. By default, the eG agent 6.3.1 is set to use TLS 1.1 to communicate with the eG manager. Hence, if the administrators want to establish a connection between the eG agent 6.3.1 and the SSL-enabled eG manager 7.1, they have to enable the eG agent 6.3.1 to use TLS 1.2 . This can be easily done by editing the **start_agent** script in the /opt/egurkha/bin directory. The steps for doing so are explained in the sections below .

If the eG agent 6.3.1 communicates with the SSL-enabled eG manager 7.1 through TLS 1.1, the eG manager 7.1 will not respond since the communication is not made through TLS 1.2. To avoid this, you may need to enforce the eG agent 6.3.1 to use TLS 1.2 by editing the **start_agent** script in the /opt/egurkha/bin directory. The steps for enabling the eG agent to use TLS 1.2 are explained in the sections below .

2.6 For Linux

To enable the eG agent on Linux to use TLS 1.2, edit the **start_agent** script in the /opt/egurkha/bin directory. The steps are discussed below:

1. Login to the eG agent host.
2. Edit the **/opt/egurkha/bin/start_agent** script file.
3. Look for the line that begins with *nohup java*.
4. In that line, insert **-Dhttps.protocols=TLSv1.2** next to *-Xrs.*
5. The line will now look as shown in the figure given below:



```
echo "****************************************************************"
echo "The eG Agent $ver has been started ..."
echo "Please check the file: "/opt/egurkha/agent/logs/error_log""
echo "for any errors while executing the agent."
echo "****************************************************************"
exit
fi
if [ $val -gt 1 ]
then
/opt/egurkha/bin/stop_agent 0
fi
done
/opt/egurkha/bin/stop_agent 0
nohup java -client -Xrs -Dhttps.protocols=TLSv1.2 -Deg.name=EgMainAgent
sleep 20
val=`/usr/ucb/ps -gauxwww | grep EgMain | grep -v grep | wc -l`
if [ $val -gt 0 ]
then
echo "****************************************************************"
echo "The eG Agent $ver has been started ..."
echo "Please check the file: "/opt/egurkha/agent/logs/error_log""
echo "for any errors while executing the agent."
echo "****************************************************************"
```

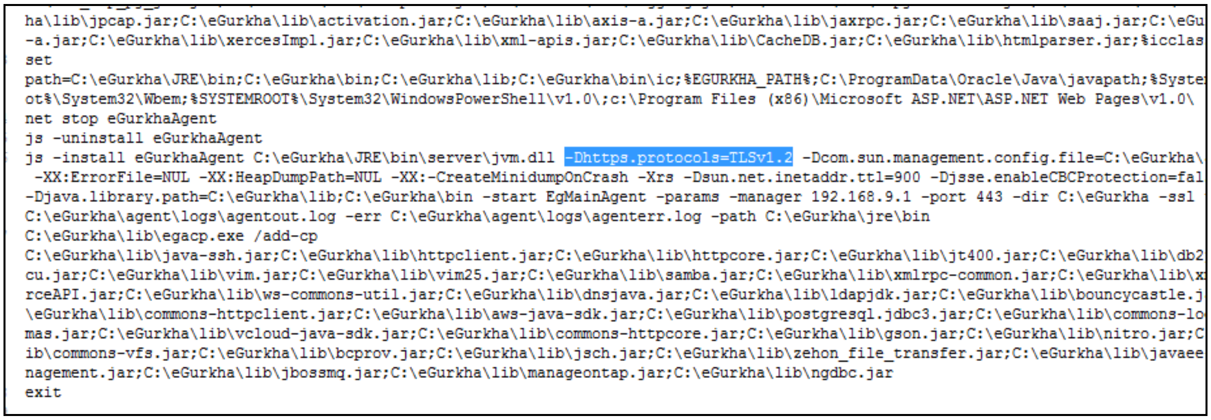
Figure 2.97: The starta script

6. Save the script file.
7. Restart the agent.

2.7 For Windows

To upgrade the JRE version of the eG agent from 1.7 to 1.8 on the Windows host, do the following:

1. Login to the eG agent host.
2. Edit the **start_agent** file in the **/opt/egurkha/bin** directory.
3. Look for the line that begins with *js -install eGurkhaAgent*.
4. In that line, insert **-Dhttps.protocols=TLSv1.2** next to C:\egurkha\JRE\bin\server\jvm.dll.
5. The line will now look as shown in the figure given below:



```
ha\lib\jpcap.jar;C:\eGurkha\lib\activation.jar;C:\eGurkha\lib\axis-a.jar;C:\eGurkha\lib\jaxrpc.jar;C:\eGurkha\lib\saaj.jar;C:\eGu
-a.jar;C:\eGurkha\lib\xercesImpl.jar;C:\eGurkha\lib\xml-apis.jar;C:\eGurkha\lib\CacheDB.jar;C:\eGurkha\lib\htmlparser.jar;%icclas
set
path=C:\eGurkha\JRE\bin;C:\eGurkha\bin;C:\eGurkha\lib;C:\eGurkha\bin\ic;%EGURKHA_PATH%;C:\ProgramData\Oracle\Java\javapath;%Syste
ot%\System32\Wbem;%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\;c:\Program Files (x86)\Microsoft ASP.NET\ASP.NET Web Pages\v1.0\
net stop eGurkhaAgent
js -uninstall eGurkhaAgent
js -install eGurkhaAgent C:\eGurkha\JRE\bin\server\jvm.dll -Dhttps.protocols=TLSv1.2 -Dcom.sun.management.config.file=C:\eGurkha\
 -XX:ErrorFile=NUL -XX:HeapDumpPath=NUL -XX:-CreateMinidumpOnCrash -Xrs -Dsun.net.inetaddr.ttl=900 -Djsse.enableCBCProtection=fal
-Djava.library.path=C:\eGurkha\lib;C:\eGurkha\bin -start EgMainAgent -params -manager 192.168.9.1 -port 443 -dir C:\eGurkha -ssl
C:\eGurkha\agent\logs\agentout.log -err C:\eGurkha\agent\logs\agenterr.log -path C:\eGurkha\jre\bin
C:\eGurkha\lib\egacp.exe /add-cp
C:\eGurkha\lib\java-ssh.jar;C:\eGurkha\lib\httpclient.jar;C:\eGurkha\lib\httpcore.jar;C:\eGurkha\lib\jt400.jar;C:\eGurkha\lib\db2
cu.jar;C:\eGurkha\lib\vim.jar;C:\eGurkha\lib\vim25.jar;C:\eGurkha\lib\samba.jar;C:\eGurkha\lib\xmlrpc-common.jar;C:\eGurkha\lib\x
rceAPI.jar;C:\eGurkha\lib\ws-commons-util.jar;C:\eGurkha\lib\dnsjava.jar;C:\eGurkha\lib\ldapjdk.jar;C:\eGurkha\lib\bouncycastle.j
\eGurkha\lib\commons-httpclient.jar;C:\eGurkha\lib\aws-java-sdk.jar;C:\eGurkha\lib\postgresql.jdbc3.jar;C:\eGurkha\lib\commons-lo
mas.jar;C:\eGurkha\lib\vcloud-java-sdk.jar;C:\eGurkha\lib\commons-httpcore.jar;C:\eGurkha\lib\gson.jar;C:\eGurkha\lib\nitro.jar;C
ib\commons-vfs.jar;C:\eGurkha\lib\bcprov.jar;C:\eGurkha\lib\jsch.jar;C:\eGurkha\lib\zehon_file_transfer.jar;C:\eGurkha\lib\javaee
nagement.jar;C:\eGurkha\lib\jbossmq.jar;C:\eGurkha\lib\manageontap.jar;C:\eGurkha\lib\ngdbc.jar
exit
```

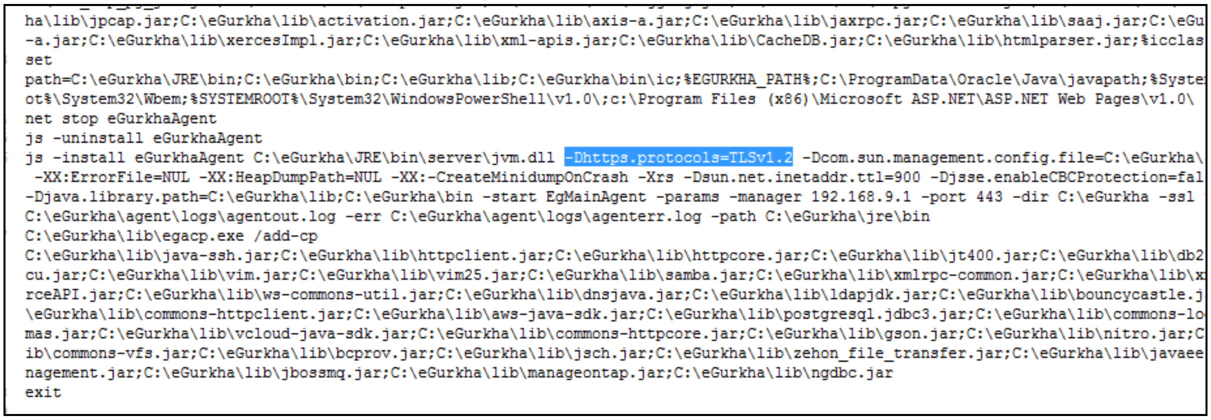
Figure 2.98: The start_agent script

6. Save the script file.
7. Restart the agent.

2.8 For Solaris

To enable the eG agent on Solaris to use TLS 1.2, edit the **start_agent** script in the /opt/egurkha/bin directory. The steps are discussed below:

1. Login to the eG agent host.
2. Edit the **start_agent** file in the **/opt/egurkha/bin** directory.
3. Look for the line that begins with *js -install eGurkhaAgent*.
4. In that line, insert **-Dhttps.protocols=TLSv1.2** next to C:\egurkha\JRE\bin\server\jvm.dll.
5. The line will now look as shown in the figure given below:



```
ha\lib\jpcap.jar;C:\eGurkha\lib\activation.jar;C:\eGurkha\lib\axis-a.jar;C:\eGurkha\lib\jaxrpc.jar;C:\eGurkha\lib\saaj.jar;C:\eGu
-a.jar;C:\eGurkha\lib\xercesImpl.jar;C:\eGurkha\lib\xml-apis.jar;C:\eGurkha\lib\CacheDB.jar;C:\eGurkha\lib\htmlparser.jar;%icclas
set
path=C:\eGurkha\JRE\bin;C:\eGurkha\bin;C:\eGurkha\lib;C:\eGurkha\bin\ic;%EGURKHA_PATH%;C:\ProgramData\Oracle\Java\javapath;%Syste
ot%\System32\Wbem;%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\;c:\Program Files (x86)\Microsoft ASP.NET\ASP.NET Web Pages\v1.0\
net stop eGurkhaAgent
js -uninstall eGurkhaAgent
js -install eGurkhaAgent C:\eGurkha\JRE\bin\server\jvm.dll -Dhttps.protocols=TLSv1.2 -Dcom.sun.management.config.file=C:\eGurkha\
 -XX:ErrorFile=NUL -XX:HeapDumpPath=NUL -XX:-CreateMinidumpOnCrash -Xrs -Dsun.net.inetaddr.ttl=900 -Djsse.enableCBCProtection=fal
-Djava.library.path=C:\eGurkha\lib;C:\eGurkha\bin -start EgMainAgent -params -manager 192.168.9.1 -port 443 -dir C:\eGurkha -ssl
C:\eGurkha\agent\logs\agentout.log -err C:\eGurkha\agent\logs\agenterr.log -path C:\eGurkha\jre\bin
C:\eGurkha\lib\egacp.exe /add-cp
C:\eGurkha\lib\java-ssh.jar;C:\eGurkha\lib\httpclient.jar;C:\eGurkha\lib\httpcore.jar;C:\eGurkha\lib\jt400.jar;C:\eGurkha\lib\db2
cu.jar;C:\eGurkha\lib\vim.jar;C:\eGurkha\lib\vim25.jar;C:\eGurkha\lib\samba.jar;C:\eGurkha\lib\xmlrpc-common.jar;C:\eGurkha\lib\x
rceAPI.jar;C:\eGurkha\lib\ws-commons-util.jar;C:\eGurkha\lib\dnsjava.jar;C:\eGurkha\lib\ldapjdk.jar;C:\eGurkha\lib\bouncycastle.j
\eGurkha\lib\commons-httpclient.jar;C:\eGurkha\lib\aws-java-sdk.jar;C:\eGurkha\lib\postgresql.jdbc3.jar;C:\eGurkha\lib\commons-lo
mas.jar;C:\eGurkha\lib\vcloud-java-sdk.jar;C:\eGurkha\lib\commons-httpcore.jar;C:\eGurkha\lib\gson.jar;C:\eGurkha\lib\nitro.jar;C
ib\commons-vfs.jar;C:\eGurkha\lib\bcprov.jar;C:\eGurkha\lib\jsch.jar;C:\eGurkha\lib\zehon_file_transfer.jar;C:\eGurkha\lib\javaee
nagement.jar;C:\eGurkha\lib\jbossmq.jar;C:\eGurkha\lib\manageontap.jar;C:\eGurkha\lib\ngdbc.jar
exit
```

Figure 2.99: The starta script

6. Save the script file.

7. Restart the agent.

2.8.0.1 SSL-Enabling the eG Manager Using a Certificate Signed by an Internal CA

If you do not want to use the default SSL certificate bundled with the eG manager, then you can obtain a signed certificate from an internal certificate authority and use that certificate for SSL-enabling the eG manager.

For this, follow the steps given below:

- Generate the Keystore file
- Generate a certificate request
- Submit the certificate request to the internal certificate Authority (CA) and obtain a certificate
- Import the certificate into a keystore
- Configure Tomcat for using the keystore file

Each of these steps has been discussed in the sections that follow.

2.8.0.2 Generating the Keystore File

The keystore file stores the details of the **certificates** necessary to make the protocol secure. Certificates contain the information pertaining to the source of the application data, and helps validate the source. To generate the keystore, use the **keytool** command. For this purpose, login to the Windows manager and go to the command prompt. Set the **JAVA_HOME** path if it is not done already. Then, execute the following commands, one after another:

cd %JAVA_HOME%\bin

keytool -genkey -alias ***egitlab1*** *-keyalg* ***RSA*** *-keypass* ***mykey*** *-keystore* ***<Filename>****.keystore -storepass* ***mykey*** *-keysize* ***1024*** *-validity* ***1095***

The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

- **-alias** : an alias name for the certificate being generated
- **-keypass** : a password used to protect the key that is generated; **ensure that you provide the same values for -keypass and -storepass.**
- **-keyalg** : specifies the algorithm that is used to generate the keys. The options are as follows:
  - **DSA**: Digital Signature Algorithm
  - **RSA** : An algorithm used for public-key cryptography
- **-keystore** : the *keytool* command stores the generated key in a *.keystore* file; provide a name for this file as input to the **-keystore** command
- **-keysize** : the size of the key that is generated; the default key size is 1024 bits - the key size must be in the range 512 bits - 1024 bits
- **-validity** : indicates the number of days for which the key/certicate will be valid - 1095 days refer to 3 years.

The command, upon execution, will request the following inputs:

```
What is your first and last name?
[Unknown]: <Type the eG manager’s fully qualified domain name here>
What is the name of your organizational unit?
[Unknown]: United States
What is the name of your organization?
[Unknown]: eG Innovations Inc
What is the name of your City or Locality?
[Unknown]: Bridgewater
What is the name of your State or Province?
[Unknown]: New Jersey
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=eG Innovations Inc, OU=United States, O=eG Innovations Inc, L=Bridge Water, ST=New
Jersey, C=US correct?
[no]: yes
```

When requested for the **first and last name**, indicate the *fully qualified domain name* using which you will be accessing the eG manager. For instance, if the eG manager is to be accessed as http://egmanager.eginnovations.com, where *egmanager.eginnovation.com* is the fully qualified domain name of the eG manager, then specify *egmanager.eginnovations.com* here.

Once all the required inputs are provided, a .keystore file will be generated in the <JAVA_HOME_ DIR>\bin directory with the **<Filename>** you had provided while issuing the command.

2.8.0.3 Generating a Certificate Request

Once a keystore file is generated, proceed to request for a certificate from an internal certifying authority. The procedure for this is as follows:

1. Login to the eG manager and go to the Windows command prompt.
2. Set the **JAVA_HOME** path if it is not done already.
3. Execute the following commands one after another:

   cd %JAVA_HOME%\bin

   keytool -certreq -alias **egitlab1** -keyalg **RSA** -file **<Name_of_the_text_file>** -keypass **mykey** -keystore **<filename>.keystore** –storepass **mykey**

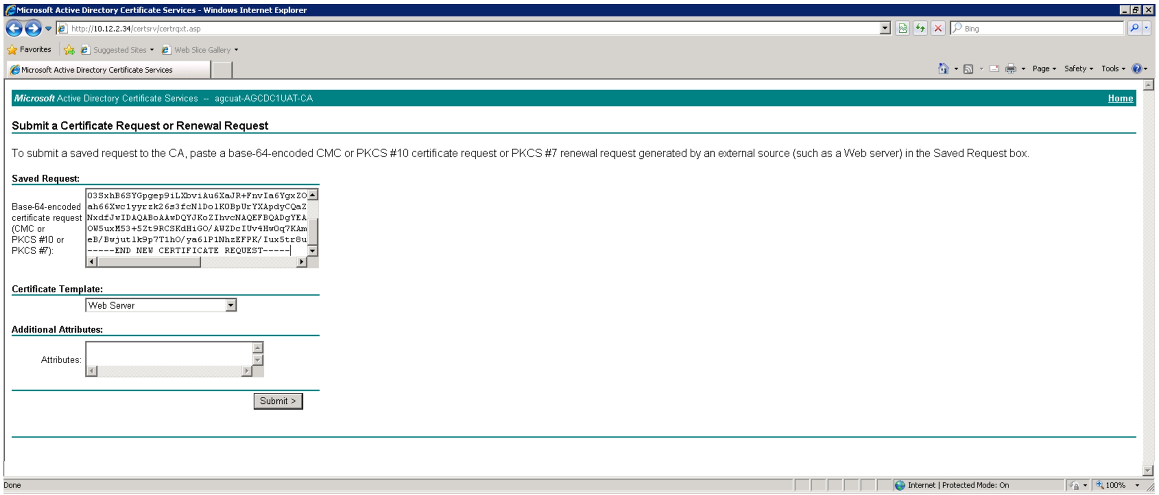
   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; make sure that you provide the same alias name that you provided while generating the keystore file (see Section **2.8.0.2**).
   - **-keyalg** : specifies the algorithm that was used to generate the keys; this can be **RSA** or **DSA**, depending upon which algorithm was used for key generation in the procedure detailed in Section **2.8.0.2**.
   - **-file** : Provide a name for the text file to which the certificate request will be saved.
   - **-keypass** : the password used to protect the key that was generated; make sure that you provide the same password that you provided while generating the keystore file (see Section **2.8.0.2**). Also, note that **-storepass** and **-keypass** should be the same.
   - **-keystore** : Provide the name of the *keystore* file in which the key has been stored; **specify the same file name that you used to store the key** (see 2.8.0.2).

4. If this command executes successfully, then a certificate request will be generated and automatically stored in the text file you specified in step 2 above.

2.8.0.4 Obtaining the Certificate from the Internal CA

1. The first step towards obtaining a certificate is to submit the certificate request to the internal CA. For this connect to the Certificate server of the internal CA and select the option to submit the certificate. For instance, if you are using Microsoft Active Directory Certificate Services to request for a self-signed certificate, then, you need to connect to *http://<YourWebServerName>/certsrv*, and then pick the option to submit the certificate. Figure 2.100 will then appear.


Microsoft Active Directory Certificate Services - Windows Internet Explorer
http://10.12.2.34/certsrv/certrqxt.asp
Bing
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Certificate Services
Page
Safety
Tools
Microsoft Active Directory Certificate Services -- agcuat-AGCDC1UAT-CA
Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
O3SxhB6SYGpgep9iLXbviAu6XaJR+FnvIa6YgxZO
ah66Xwc1yyrzk26s3fcN1Do1KOBpUrYXApdyCQaZ
NxdfJwIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEA
OW5uxM53+5Zt9RCSKdHiGO/AWZDcIUv4HwOq7KAm
eB/Bwjut1k9p7T1hO/ya61P1NhzEFPK/Iux5tr8u
-----END NEW CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

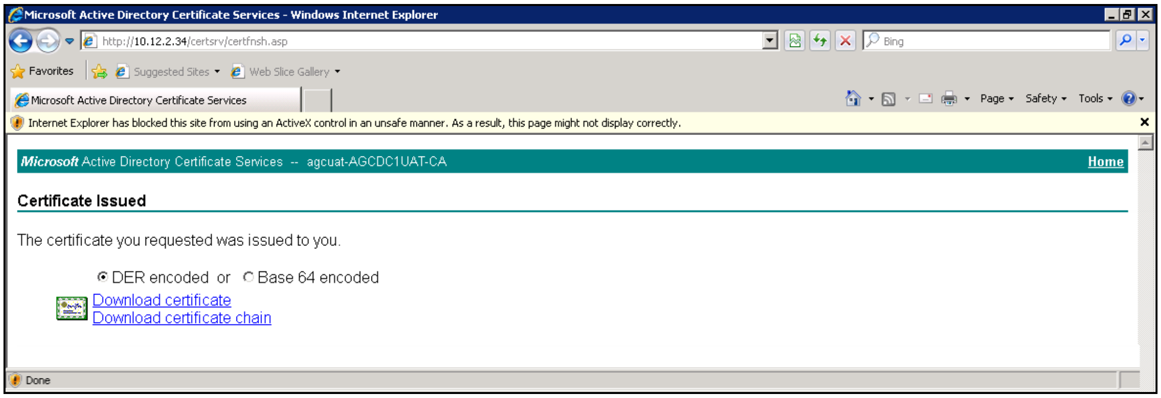
Additional Attributes:

Attributes:

Figure 2.100: Requesting for a certificate

2. Open the text file containing the certificate request (which was created using the procedure detailed in Section **2.8.0.3** above), copy the contents of the file, and then paste it to the text area of the **Base 64-encoded certificate request** text box of Figure 2.100. Then, click the **Submit** button.

3. The certificate will thus be generated. Download the certificate.


Microsoft Active Directory Certificate Services - Windows Internet Explorer
http://10.12.2.34/certsrv/certfnsh.asp
Bing
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Certificate Services
Page
Safety
Tools

Internet Explorer has blocked this site from using an ActiveX control in an unsafe manner. As a result, this page might not display correctly.

Microsoft Active Directory Certificate Services -- agcuat-AGCDC1UAT-CA
Home

Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

Download certificate

Download certificate chain

Figure 2.101: Downloading the certificate

2.8.0.4.1 Importing the Certificates into the Keystore File

The downloaded certificate can be in one of the following forms:

- Can be a single, combined certificate
- Can be accompanied by a certificate chain
- Can be in a PEM format

The procedure for importing certificates differs based on the format of the downloaded certificate. These procedures have been detailed in the sub-sections below.

Importing a Combined Certificate into the Keystore File

In this case, follow the steps below to import the certificate into the keystore file:

1. Set the **JAVA_HOME** path if it is not done already.
2. At the command prompt, execute the following commands, one after another:

   cd %JAVA_HOME%\bin

   keytool -import –trustcacerts -alias ***egitlab1*** *-file* ***<Name_of_the_domain_certificate>*** *-keystore* ***<Name_of_the_keystore_file>.keystore***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; make sure that you provide the same alias name you provided when generating the keystore (see Section **2.8.0.2**).
   - **-file**: the name of the domain certificate that you want to import
   - **-keystore** : Provide the name of the *keystore* file you generated when you followed the procedure detailed in Section **2.8.0.2** above.

Importing a Signed Certificate and the Certificate Chain into the Keystore File

Digital certificates are verified using a chain of trust. The trust anchor for the digital certificate is the Root Certificate Authority (CA). The Certificate Hierarchy is a structure of certificates that allows individuals to verify the validity of a certificate's issuer. Certificates are issued and signed by certificates that reside higher in the certificate hierarchy, so the validity and trustworthiness of a given certificate is determined by the corresponding validity of the certificate that signed it.

The Chain of Trust of a Certificate Chain is an ordered list of certificates, containing an end-user subscriber certificate and intermediate certificates (that represents the Intermediate CA), that enables the receiver to verify that the sender and all intermediate certificates are trustworthy.

A certificate chain will therefore consist of multiple certificates. Before importing each of these certificates, **you will have to understand the hierarchy of the certificates**. To know which is the root and which is the intermediate certificate, refer to the web site of the certificate authority. Then, set the **JAVA_HOME** path if it is not done already. Next, follow the steps below:

1. First, import the Root certificate. For this, execute the following commands, one after another in the command prompt:

   cd %JAVA_HOME%\bin

   keytool -import –trustcacerts -alias ***rootcert*** *-file* ***<Name_of_the_root_certificate>*** *-keystore* ***<Name_of_the_keystore_file>.keystore*** *–keypass* ***mykey*** *–storepass* ***mykey***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; make sure that you provide a unique alias name for the root certificate.
   - **-file**: the name of the root certificate that you want to import
   - **-keystore** : Provide the name of the *keystore* file you generated when you followed the procedure detailed in Section **2.8.0.2** above.
   - **-keypass** and **–storepass** : Provide the same **keypass** and **storepass** that you specified when generating the keystore; refer to Section **2.8.0.2** above for details.

2. Next, import each of the intermediate certificates, one after another, using the following command:

   keytool -import –trustcacerts -alias ***intercert1****-file* ***<Name_of_the_intermediate_certificate>****-keystore* ***<Name_of_the_keystore_file>.keystore****–keypass****mykey****–storepass****mykey***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; **make sure that you provide a unique alias name for every intermediate certificate.**

- **-file**: the name of the intermediate certificate that you want to import
- **-keystore** : Provide the name of the *keystore* file you generated when you followed the procedure detailed in Section **2.8.0.2** above.
- **-keypass** and **–storepass** : Provide the same **keypass** and **storepass** that you specified when generating the keystore; refer to Section **2.8.0.2** above for details.

3. Finally, import the entity/domain certificate into the keystore by issuing the following command:

   keytool -import –trustcacerts -alias ***egitlab1*** *-file* ***<Name_of_the_domain_certificate>*** *-keystore* ***<Name_of_the_keystore_file>.keystore***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; make sure that you provide the same alias name you provided when generating the keystore (see Section **2.8.0.2**) .
   - **-file**: the name of the domain certificate that you want to import
   - **-keystore** : Provide the name of the *keystore* file you generated when you followed the procedure detailed in Section **2.8.0.2** above.

   Note:

   If the domain certificate import command throws an error for any reason, it could be because, all related certificates may not have been imported. Check the web site of the CA for more details.

Importing a Certificate that is in the PEM Format

PEM is a container format that may include just the public certificate (such as with Apache installs, and CA certificate files */etc/ssl/certs*), or may include an entire certificate chain including public key, private key, and root certificates, or may only contain a certificate and a private key.

If the certificate you downloaded is in the PEM format and includes only a certificate file and a private key file, then follow the steps below to import that certificate into a keystore file.

1. Run the following command from the command prompt to export the certificate and private key file into the pkcs12 format:

   openssl pkcs12 -export -in ***certificate.crt*** *-inkey* ***private.key*** *-certfile* ***certificate.crt*** *-name “**My certificate”** -out* ***keystore****.p12*

The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

- **-in** : the name of the certificate that is included in the PEM container
- **-inkey**: the name of the private key file the PEM container consists of
- **-certfile** : the name of the certificate that is included in the PEM container
- **-name** : Provide a **unique name for the certificate file** that is being exported.
- **-out** : Specify the name of the keystore file to which the certificate and private key are to be exported. **The keystore file can have any name of your choice.**

2. Next, you need to convert the keystore file, which is currently in the pkcs12 format, into the Java keystore (i.e., JKS) format. For this, issue the following command at the command prompt:

   keytool -importkeystore –alias ***egitlab1*** -deststorepass ***mykey*** -destkeypass ***mykey*** -destkeystore ***keystore,jks*** -srckeystore ***keystore.pk12*** -srcstoretype PKCS12 -srcstorepass ***mykey***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

- **-alias** : the aliasname of the certificate being requested; make sure that you provide the same alias name that you specified in Section **2.8.0.2**.
- **-deststorepass** : this refers to the **storepass** of the destination keystore file – i.e., the keystore file in the JKS format. The storepass of the destination keystore should be the same as the storepass of the source keystore.
- **-destkeypass** : this refers to the **keypass** of the destination keystore file - i.e., the keystore file in the JKS format. **The storepass and keypass of the destination keystore file should be the same**.
- **-destkeystore**: the name of the destination keystore file – i.e., the keystore file in the JKS format.
- **-srckeystore** : the name of the destination keystore file – i.e., the keystore file in the PKCS12 format.
- **-srcstorepass** : The **storepass** of the source keystore file – i.e., the keystore file in the PKCS12 firmat. make sure that you provide the same storepass you specified in Section **2.8.0.2**.

2.8.0.4.2 Configuring Tomcat for Using the Keystore File

The eG manager on Windows uses Tomcat as the web server. Therefore, to SSL-enable the eG manager, you need to configure the **server.xml** file of Tomcat with the name and full path to the keystore file which was created earlier.

1. Edit the **server.xml** file in the <CATALINA_HOME>\conf directory.
2. In the file, search for the XML block where the SSL Coyote HTTP connector on port 8443 is defined. If this block is commented, it indicates that the eG manager is not SSL-enabled and is hence listening on an HTTP port only. To SSL-enable the eG manager, first uncomment this block as indicated below:

```
<Connector protocol=”HTTP/1.1”
```

```
enableLookups=”false” acceptCount=”10”  connectionTimeout=”20000”
```

```
useURIValidationHack=”false” URIEncoding=”UTF-8” tcpNoDelay=”true” compression=”on”
compressionMinSize=”1024” noCompressionUserAgents=”gozilla, traviata”
compressableMimeType=”text/html,text/xml,text/plain,application/x-java-
applet,application/octet-
stream,application/xml,text/javascript,text/css,image/png,image/jpeg,
image/gif,application/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml”
```

```
SSLEnabled=”true” scheme=”https” secure=”true”
```

```
clientAuth=”false” sslProtocol=”TLS” sslEnabledProtocols=”TLSv1” ciphers=”TLS_ECDHE_
RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_
256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_
RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_
SHA,SSL_RSA_WITH_RC4_128_SHA” />
```

3. Then, proceed to make the changes indicated in **Bold** below in the SSL XML block:

```
<Connector protocol=”HTTP/1.1”
```

```
port=”<eG_Manager_Port>” minSpareThreads=”64” maxThreads=”512”
```

```
enableLookups=”false” acceptCount=”10”  connectionTimeout=”20000”
```

```
useURIValidationHack="false" URIEncoding="UTF-8" tcpNoDelay="true" compression="on"
compressionMinSize="1024" noCompressionUserAgents="gozilla, traviata"
compressableMimeType="text/html,text/xml,text/plain,application/x-java-
applet,application/octet-
stream,application/xml,text/javascript,text/css,image/png,image/jpeg,
image/gif,application/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml"
```

```
SSLEnabled="true" scheme="https" secure="true"
```

```
clientAuth="false"  sslProtocol="TLS"  sslEnabledProtocols="TLSv1"  ciphers="TLS_ECDHE_
RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_
256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_
RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_
SHA,SSL_RSA_WITH_RC4_128_SHA" keyAlias="<Alias_set_when_generating_certificate file>"
keystoreFile="<Full_path_to_keystore_file>"keystorePass="<Keypass_set_for_certificate_
request_generation>" />
```

Set the *port* parameter in the XML block to reflect the SSL port number that you have configured for the eG manager. Also, note that three new parameters, namely - **keyAlias, keystoreFile** and **keystorePass** - have been inserted into the SSL block. While the **keystoreFile** parameter has to be set to the full path to the **.keystore** file that you generated earlier, the **keystorePass** parameter should be set to the keystore password that you specified while issuing the **keytool** command. Likewise, the **keyAlias** parameter is to be set to the **alias name** that you provided for the certificate file, when you generated it in Section **2.8.0.2** above.

With that change, the eG manager on Windows has acquired the capability to listen on two ports - the SSL port and the non-SSL port. To configure the eG manager to listen only on the SSL port, simply comment that section of the **server.xml** file where the non-SSL Coyote HTTP connector on port 8081 has been defined, as indicated below:

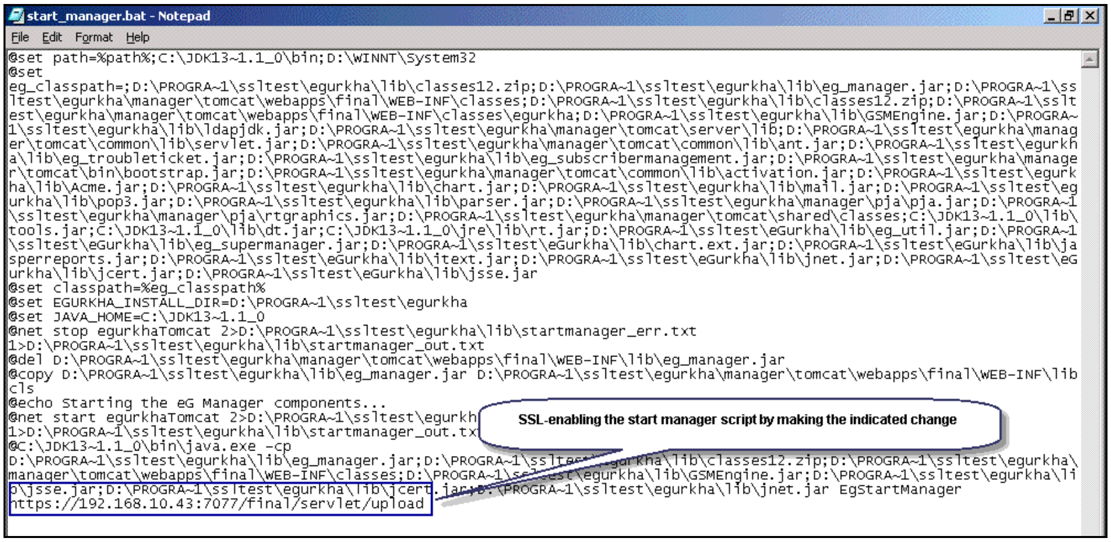
```
<!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 8081 -->
<!--
<Connector protocol="HTTP/1.1"
port="7077" minSpareThreads="64" maxThreads="512"
enableLookups="false" redirectPort="8443"
acceptCount="10" connectionTimeout="20000"
```

```
useURIValidationHack=”false”  URIEncoding=”UTF-8” tcpNoDelay=”true” compression=”on”
compressionMinSize=”1024” noCompressionUserAgents=”gozilla, traviata”
compressableMimeType=”text/html,text/xml,text/plain,application/x-java-
applet,application/octet-
stream,application/xml,text/javascript,text/css,image/png,image/jpeg,
image/gif,application/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml” server=”eG Tomcat Server”/>
```

```
-->
```

4. Save the file.

5. Then, SSL-enable the **start_manager.bat** script. For this, first open the **start_manager.bat** file (see Figure 2.102) residing in the <EG_INSTALL_DIR>\lib directory. Change the URL *http://<eGmanagerIp>:<eGmanagerdefaultTCPPort>/final/servlet/upload* present in the last line of the batch file to *https://<eGmanagerIp>:<eGmanagerPort>/final/servlet/upload* (see Figure 2.102).


start_manager.bat - Notepad
File
Edit
Format
Help
SSL-enabling the start manager script by making the indicated change

```
@set path=%path%;C:\JDK13~1.1_0\bin;D:\WINNT\System32
@set
eg_classpath=;D:\PROGRA~1\ssltest\egurkha\lib\classes12.zip;D:\PROGRA~1\ssltest\egurkha\lib\eg_manager.jar;D:\PROGRA~1\ss
ltest\egurkha\manager\tomcat\webapps\final\WEB-INF\classes;D:\PROGRA~1\ssltest\egurkha\lib\classes12.zip;D:\PROGRA~1\sslt
est\egurkha\manager\tomcat\webapps\final\WEB-INF\classes\egurkha;D:\PROGRA~1\ssltest\egurkha\lib\GSMEngine.jar;D:\PROGRA~
1\ssltest\egurkha\lib\ldapjdk.jar;D:\PROGRA~1\ssltest\egurkha\manager\tomcat\server\lib;D:\PROGRA~1\ssltest\egurkha\manag
er\tomcat\common\lib\servlet.jar;D:\PROGRA~1\ssltest\egurkha\manager\tomcat\common\lib\ant.jar;D:\PROGRA~1\ssltest\egurkh
a\lib\eg_troubleticket.jar;D:\PROGRA~1\ssltest\egurkha\lib\eg_subscribermanagement.jar;D:\PROGRA~1\ssltest\egurkha\manage
r\tomcat\bin\bootstrap.jar;D:\PROGRA~1\ssltest\egurkha\manager\tomcat\common\lib\activation.jar;D:\PROGRA~1\ssltest\egurk
ha\lib\Acme.jar;D:\PROGRA~1\ssltest\egurkha\lib\chart.jar;D:\PROGRA~1\ssltest\egurkha\lib\mail.jar;D:\PROGRA~1\ssltest\eg
urkha\lib\pop3.jar;D:\PROGRA~1\ssltest\egurkha\lib\parser.jar;D:\PROGRA~1\ssltest\egurkha\manager\pja\pja.jar;D:\PROGRA~1
\ssltest\egurkha\manager\pja\rtgraphics.jar;D:\PROGRA~1\ssltest\egurkha\manager\tomcat\shared\classes;C:\JDK13~1.1_0\lib\
tools.jar;C:\JDK13~1.1_0\lib\dt.jar;C:\JDK13~1.1_0\jre\lib\rt.jar;D:\PROGRA~1\ssltest\eGurkha\lib\eg_util.jar;D:\PROGRA~1
\ssltest\eGurkha\lib\eg_supermanager.jar;D:\PROGRA~1\ssltest\eGurkha\lib\chart.ext.jar;D:\PROGRA~1\ssltest\eGurkha\lib\ja
sperreports.jar;D:\PROGRA~1\ssltest\eGurkha\lib\itext.jar;D:\PROGRA~1\ssltest\eGurkha\lib\jnet.jar;D:\PROGRA~1\ssltest\eG
urkha\lib\jcert.jar;D:\PROGRA~1\ssltest\eGurkha\lib\jsse.jar
@set classpath=%eg_classpath%
@set EGURKHA_INSTALL_DIR=D:\PROGRA~1\ssltest\egurkha
@set JAVA_HOME=C:\JDK13~1.1_0
@net stop egurkhaTomcat 2>D:\PROGRA~1\ssltest\egurkha\lib\startmanager_err.txt
1>D:\PROGRA~1\ssltest\egurkha\lib\startmanager_out.txt
@del D:\PROGRA~1\ssltest\egurkha\manager\tomcat\webapps\final\WEB-INF\lib\eg_manager.jar
@copy D:\PROGRA~1\ssltest\egurkha\lib\eg_manager.jar D:\PROGRA~1\ssltest\egurkha\manager\tomcat\webapps\final\WEB-INF\lib
cls
@echo Starting the eG Manager components...
@net start egurkhaTomcat 2>D:\PROGRA~1\ssltest\egurkh
1>D:\PROGRA~1\ssltest\egurkha\lib\startmanager_out.tx
@C:\JDK13~1.1_0\bin\java.exe -cp
D:\PROGRA~1\ssltest\egurkha\lib\eg_manager.jar;D:\PROGRA~1\ssltest\egurkha\lib\classes12.zip;D:\PROGRA~1\ssltest\egurkha\
manager\tomcat\webapps\final\WEB-INF\classes;D:\PROGRA~1\ssltest\egurkha\lib\GSMEngine.jar;D:\PROGRA~1\ssltest\egurkha\li
b\jsse.jar;D:\PROGRA~1\ssltest\egurkha\lib\jcert.jar;D:\PROGRA~1\ssltest\egurkha\lib\jnet.jar EgStartManager
https://192.168.10.43:7077/final/servlet/upload
```

Figure 2.102: SSL-enabling the start_manager script

6. Next, make sure that the eG manager URL configured against the **MailHomeURL** parameter in the **[MISC_ ARGS]** section of the **eg_ services.ini** file (in the <EG_ INSTALL_ DIR>\manager\config directory) begins with **https://** instead of **http://**. Then, save the file.

7. Finally, start the eG manager.

Note:

Owing to SSL vulnerabilities that were discovered, many changes have been made in v6.1.2 to harden SSL communication with the eG manager. These include the following:

- Starting from version 6.1.2, TLS v1 will be the default secure protocol that web browsers will use to communicate with the eG manager.
- Recent versions of Firefox and Chrome expect a strong Cipher suite definition in SSL-enabled web/web application servers. HTTPS requests to web/web application servers that do not contain this Cipher Suite definition will be rejected by the Firefox and Chrome browsers. To avoid this, in version 6.1.2, this Cipher Suite definition has been bundled into the Tomcat server on which the eG manager runs.
- In the default SSL certificate that eG bundles with the eG manager, the message signing algorithm has been changed.

All these changes however, **will not be available to any SSL manager that is upgraded from a lower version to v6.1.2**. This is why, after a manager is upgraded to v6.1.2, you will experience problems communicating with the manager via HTTPS.

To avoid this, after an SSL-enabled manager is upgraded to version 6.1.2, you have to harden the SSL communication with the upgraded manager, following the steps detailed below:

- Edit the **server.xml** file in the <CATALINA_HOME>/conf directory (on Unix; on Windows, this will be the <CATALINA_HOME>\conf directory) on the eG manager host:
- Look for the SSL connector definition in the file.
- Locate the *sslProtocol* parameter in the definition.
- After the *sslprotocol* parameter, insert the following:

```
sslEnabledProtocols=”TLSv1”
```

- Then, include the following Cipher Suite definition:

```
ciphers=”TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_
ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,   TLS_RSA_WITH_
AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_
RSA_WITH_AES_256_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA”
```

Note:

- Once the aforesaid changes are made, the SSL connector definition in your **server.xml** will look as shown below:

```
<Connector protocol=”HTTP/1.1”
```

```
port=”<eGManagerPort>” minSpareThreads=”64” maxThreads=”512”
```

```
enableLookups=”false” acceptCount=”10”  connectionTimeout=”20000”
```

```
useURIValidationHack=”false” URIEncoding=”UTF-8” tcpNoDelay=”true” compression=”on”
compressionMinSize=”1024” noCompressionUserAgents=”gozilla, traviata”
compressableMimeType=”text/html,text/xml,text/plain,application/x-java-
applet,application/octet-
stream,application/xml,text/javascript,text/css,image/png,image/jpeg,
image/gif,application/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml”
```

```
SSLEnabled=”true” scheme=”https” secure=”true”
```

```
clientAuth=”false” sslProtocol=”TLS” sslEnabledProtocols=”TLSv1”ciphers=”TLS_ECDHE_
RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_
256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,   TLS_RSA_WITH_AES_128_CBC_
SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_
256_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA”
```

```
keystoreFile=”<PathtoKeystoreFile>” keystorePass=”<Keystorepass>” server=”eG Tomcat
Server”/>
```

- Next, save the file.
- If you had SSL-enabled the eG manager using the default certificate that eG provides, then, once the above changes are made, copy the default certificate from the <EG_ INSTALL_ DIR>\bin\latest_certificate folder (on Windows; on Unix, this will be the **/opt/egurkha/bin/latest_ certificate** folder), to the <EG_INSTALL_DIR>\manager/tomcat/webapps folder (on Windows; on Unix, this will be the **/opt/egurkha/manager/tomcat/webapps** folder).
- Finally, restart the eG manager.

2.8.0.5 SSL-Enabling the eG Manager Using a Signed Certificate Obtained from a Valid Certifying Authority

Self-signed certificates are useful in environments where ‘security’ is not a priority. In highly secure environments, especially where the eG manager is to be frequently accessed via the public internet, using a self-signed certificate may not be preferred. In such a case, you can obtain a valid certificate from a certificate authority and use that certificate to SSL-enable the eG manager.

The broad steps to be followed to achieve this are as follows:

- Generating the keystore file
- Generating a certificate request
- Submitting the certificate request to the Certificate Authority (CA) and obtaining a certificate

- Importing the certificate into a keystore
- Configuring Tomcat for using the keystore file

The sub-sections below elaborate on each of these steps.

2.8.0.6 Generating a Keystore File

The keystore file stores the details of the **certificates** necessary to make the protocol secure. Certificates contain the information pertaining to the source of the application data, and helps validate the source. To generate the keystore, use the **keytool** command. For this purpose, login to the Windows manager and go to the command prompt. Set the **JAVA_HOME** path if it is not done already. Then, execute the following commands, one after another:

cd %JAVA_HOME%\bin

*keytool -genkey -alias **egitlab1** -keyalg **RSA** -keypass **mykey** -keystore **<Filename>**.keystore -storepass **mykey** -keysize **1024** -validity **1095***

The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

- **-alias** : an alias name for the certificate being generated
- **-keypass** : a password used to protect the key that is generated; **ensure that you provide the same values for -keypass and -storepass.**
- **-keyalg** : specifies the algorithm that is used to generate the keys. The options are as follows:
  - **DSA**: Digital Signature Algorithm
  - **RSA** : An algorithm used for public-key cryptography
- **-keystore** : the *keytool* command stores the generated key in a *.keystore* file; provide a name for this file as input to the **-keystore** command
- **-keysize** : the size of the key that is generated; the default key size is 1024 bits - the key size must be in the range 512 bits - 1024 bits
- **-validity** : indicates the number of days for which the key/certicate will be valid - 1095 days refer to 3 years.

The command, upon execution, will request the following inputs:

```
What is your first and last name?
[Unknown]: <Type the eG manager’s fully qualified domain name here>
What is the name of your organizational unit?
[Unknown]: United States
What is the name of your organization?
[Unknown]: eG Innovations Inc
What is the name of your City or Locality?
[Unknown]: Bridgewater
What is the name of your State or Province?
[Unknown]: New Jersey
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=eG Innovations Inc, OU=United States, O=eG Innovations Inc, L=Bridge Water, ST=New
Jersey, C=US correct?
[no]: yes
```

When requested for the **first and last name**, indicate the *fully qualified domain name* using which you will be accessing the eG manager. For instance, if the eG manager is to be accessed as http://egmanager.eginnovations.com, where *egmanager.eginnovation.com* is the fully qualified domain name of the eG manager, then specify *egmanager.eginnovations.com* here.

Once all the required inputs are provided, a .keystore file will be generated in the <JAVA_HOME_DIR>\bin directory with the **<Filename>** you had provided while issuing the command.

2.8.0.7 Generating a Certificate Request

Once a keystore file is generated, proceed to request for a certificate from a valid certifying authority. The procedure for this is as follows:

1. Login to the eG manager and go to the Windows command prompt.
2. Set the **JAVA_HOME** path if it is not done already.
3. Execute the following commands one after another:

   cd %JAVA_HOME%\bin

   keytool -certreq -alias ***egitlab1*** *-keyalg* ***RSA*** *-file* ***<Name_of_the_text_file>*** *-keypass* ***mykey*** *-keystore* ***<filename>.keystore*** *–storepass* ***mykey***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

- **-alias** : the alias name of the certificate being requested; **make sure that you provide the same alias name that you provided while generating the keystore file** (see Section **2.8.0.6**).
- **-keyalg** : specifies the algorithm that was used to generate the keys; this can be **RSA** or **DSA**, depending upon which algorithm was used for key generation in the procedure detailed in Section **2.8.0.6**.
- **-file** : Provide a name for the text file to which the certificate request will be saved.
- **-keypass** : the password used to protect the key that was generated; make sure that you provide the same password that you provided while generating the keystore file (see Section **2.8.0.6**). Also, note that **-storepass** and **-keypass** should be the same.
- **-keystore** : Provide the name of the *keystore* file in which the key has been stored; specify the same file name that you used to store the key (see Section **2.8.0.6**).

4. If this command executes successfully, then a certificate request will be generated and automatically stored in the text file you specified in step 2 above.

2.8.0.8 Obtaining the Certificate from the CA

1. The first step towards obtaining a certificate is to submit the certificate request to the CA. For this connect to the Certificate server of the CA and submit the certificate. The procedure for request submission will differ from one CA to another.
2. The certificate will thus be generated. Download the certificate.

2.8.0.9 Importing the Certificates into the Keystore File

The downloaded certificate can be in one of the following forms:

- Can be a single, combined certificate
- Can be accompanied by a certificate chain
- Can be in a PEM format

The procedure for importing certificates differs based on the format of the downloaded certificate. These procedures have been detailed in the sub-sections below.

Importing a Combined Certificate into the Keystore File

In this case, follow the steps below to import the certificate into the keystore file:

1. Set the **JAVA_HOME** path if it is not done already.
2. At the command prompt, execute the following commands, one after another:

   cd %JAVA_HOME%\bin

   keytool -import –trustcacerts -alias ***egitlab1*** *-file* **<Name_of_the_domain_certificate>** *-keystore* ***<Name_of_the_keystore_file>.keystore***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; make sure that you provide the same alias name you provided when generating the keystore (see Section **2.8.0.6**) .
   - **-file**: the name of the domain certificate that you want to import
   - **-keystore** : Provide the name of the *keystore* file you generated when you followed the procedure detailed in Section **2.8.0.6** above.

Importing a Signed Certificate and the Certificate Chain into the Keystore File

Digital certificates are verified using a chain of trust. The trust anchor for the digital certificate is the Root Certificate Authority (CA). The Certificate Hierarchy is a structure of certificates that allows individuals to verify the validity of a certificate's issuer. Certificates are issued and signed by certificates that reside higher in the certificate hierarchy, so the validity and trustworthiness of a given certificate is determined by the corresponding validity of the certificate that signed it.

The Chain of Trust of a Certificate Chain is an ordered list of certificates, containing an end-user subscriber certificate and intermediate certificates (that represents the Intermediate CA), that enables the receiver to verify that the sender and all intermediate certificates are trustworthy.

A certificate chain will therefore consist of multiple certificates. Before importing each of these certificates, **you will have to understand the hierarchy of the certificates**. To know which is the root and which is the intermediate certificate, refer to the web site of the certificate authority. For instance, if Comodo is the Certificate Authority that has issued the SSL certificate, then connect to the following URL, *https://support.comodo.com/index.php?/Default/Knowledgebase/Article/View/620/1/* , to gain clarity.

Then, follow the steps below:

1. Set the **JAVA_HOME** path if it is not done already.
2. Then, import the Root certificate. For this, execute the following commands, one after another in the command prompt:

   cd %JAVA_HOME%\bin

   keytool -import –trustcacerts -alias ***rootcert*** *-file* ***<Name_of_the_root_certificate>*** *-keystore* ***<Name_of_the_keystore_file>.keystore*** *–keypass* ***mykey*** *–storepass* ***mykey***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; **make sure that you provide a unique alias name for the root certificate.**
   - **-file**: the name of the root certificate that you want to import
   - **-keystore** : Provide the name of the *keystore* file you generated when you followed the procedure detailed in Section **2.8.0.6** above.
   - **-keypass** and **–storepass** : Provide the same **keypass** and **storepass** that you specified when generating the keystore; refer to Section **2.8.0.6** above for details.

3. Next, import each of the intermediate certificates, one after another, using the following command:

   keytool -import –trustcacerts -alias ***intercert1****-file* ***<Name_of_the_intermediate_certificate>****-keystore* ***<Name_of_the_keystore_file>.keystore****–keypass****mykey****–storepass****mykey***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; **make sure that you provide a unique alias name for every intermediate certificate.**
   - **-file**: the name of the intermediate certificate that you want to import
   - **-keystore** : Provide the name of the *keystore* file you generated when you followed the procedure detailed in Section **2.8.0.6** above.
   - **-keypass** and **–storepass** : Provide the same **keypass** and **storepass** that you specified when generating the keystore; refer to Section **2.8.0.6** above for details.

4. Finally, import the entity/domain certificate into the keystore by issuing the following command:

keytool -import –trustcacerts -alias ***egitlab1*** *-file* ***<Name_of_the_domain_certificate>*** *-keystore* ***<Name_of_the_keystore_file>.keystore***

The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

- **-alias** : the alias name of the certificate being requested; make sure that you provide the same alias name you provided when generating the keystore (see Section **2.8.0.6**) .
- **-file**: the name of the domain certificate that you want to import
- **-keystore** : Provide the name of the *keystore* file you generated when you followed the procedure detailed in Section **2.8.0.6** above.

Note:

If the domain certificate import command throws an error for any reason, it could be because, all related certificates may not have been imported. Check the web site of the CA for more details.

Importing a Certificate that is in the PEM Format

PEM is a container format that may include just the public certificate (such as with Apache installs, and CA certificate files */etc/ssl/certs*), or may include an entire certificate chain including public key, private key, and root certificates, or may only contain a certificate and a private key.

If the certificate you downloaded is in the PEM format and includes only a certificate file and a private key file, then follow the steps below to import that certificate into a keystore file.

1. Run the following command from the command prompt to export the certificate and private key file into the pkcs12 format:

   openssl pkcs12 -export -in ***certificate.crt*** *-inkey* ***private.key*** *-certfile* ***certificate.crt*** *-name “****My certificate”*** *-out* ***keystore****.p12*

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-in** : the name of the certificate that is included in the PEM container
   - **-inkey**: the name of the private key file the PEM container consists of
   - **-certfile** : the name of the certificate that is included in the PEM container
   - **-name** : Provide a unique name for the certificate file that is being exported.

- **-out** : Specify the name of the keystore file to which the certificate and private key are to be exported. **The keystore file can have any name of your choice.**

2. Next, you need to convert the keystore file, which is currently in the pkcs12 format, into the Java keystore (i.e., JKS) format. For this, issue the following command at the command prompt:

   keytool -importkeystore –alias ***egitlab1*** *-deststorepass* ***mykey*** *-destkeypass* ***mykey*** *-destkeystore* ***keystore,jks*** *-srckeystore* ***keystore.pk12*** *-srcstoretype PKCS12 -srcstorepass* ***mykey***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

- **-alias** : the aliasname of the certificate being requested; make sure that you provide the same alias name that you specified in Section **2.8.0.6**.
- **-deststorepass** : this refers to the **storepass** of the destination keystore file – i.e., the keystore file in the JKS format. **The storepass of the destination keystore should be the same as the storepass of the source keystore.**
- **-destkeypass** : this refers to the **keypass** of the destination keystore file **-** i.e., the keystore file in the JKS format. The storepass and keypass of the destination keystore file should be the same.
- **-destkeystore**: the name of the destination keystore file – i.e., the keystore file in the JKS format.
- **-srckeystore** : the name of the destination keystore file – i.e., the keystore file in the PKCS12 format.
- **-srcstorepass** : The **storepass** of the source keystore file – i.e., the keystore file in the PKCS12 firmat. make sure that you provide the same storepass you specified in Section **2.8.0.6**.

2.8.0.9.1 Configuring Tomcat for Using the Keystore File

The eG manager on Windows uses Tomcat as the web server. Therefore, to SSL-enable the eG manager, you need to configure the **server.xml** file of Tomcat with the name and full path to the keystore file which was created earlier.

1. Edit the **server.xml** file in the <CATALINA_HOME>\conf directory.
2. In the file, search for the XML block where the SSL Coyote HTTP connector on port 8443 is

defined. If this block is commented, it indicates that the eG manager is not SSL-enabled and is hence listening on an HTTP port only. To SSL-enable the eG manager, first uncomment this block as indicated below:

```
<Connector protocol=”HTTP/1.1”
port=”8443” minSpareThreads=”64” maxThreads=”512”
enableLookups=”false” acceptCount=”10”  connectionTimeout=”20000”
useURIValidationHack=”false” URIEncoding=”UTF-8” tcpNoDelay=”true” compression=”on”
compressionMinSize=”1024” noCompressionUserAgents=”gozilla, traviata”
compressableMimeType=”text/html,text/xml,text/plain,application/x-java-
applet,application/octet-
stream,application/xml,text/javascript,text/css,image/png,image/jpeg,
image/gif,application/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml”
SSLEnabled=”true” scheme=”https” secure=”true”
clientAuth=”false” sslProtocol=”TLS” sslEnabledProtocols=”TLSv1” ciphers=”TLS_ECDHE_
RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_
256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_
RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_
SHA,SSL_RSA_WITH_RC4_128_SHA” />
```

3. Then, proceed to make the changes indicated in **Bold** below in the SSL XML block:

```
<Connector protocol=”HTTP/1.1”
port=”<eG_Manager_Port>” minSpareThreads=”64” maxThreads=”512”
enableLookups=”false” acceptCount=”10”  connectionTimeout=”20000”
useURIValidationHack=”false” URIEncoding=”UTF-8” tcpNoDelay=”true” compression=”on”
compressionMinSize=”1024” noCompressionUserAgents=”gozilla, traviata”
compressableMimeType=”text/html,text/xml,text/plain,application/x-java-
applet,application/octet-
stream,application/xml,text/javascript,text/css,image/png,image/jpeg,
image/gif,application/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml”
SSLEnabled=”true” scheme=”https” secure=”true”
```

```
clientAuth=”false” sslProtocol=”TLS” sslEnabledProtocols=”TLSv1” ciphers=”TLS_ECDHE_
RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_
256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_
RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_
SHA,SSL_RSA_WITH_RC4_128_SHA” keyAlias=”<Alias_set_when_generating_certificate file>”
keystoreFile=”<Full_path_to_keystore_file>”keystorePass=”<Keypass_set_for_certificate_
request_generation>” />
```

Set the *port* parameter in the XML block to reflect the SSL port number that you have configured for the eG manager. Also, note that three new parameters, namely - **keyAlias, keystoreFile** and **keystorePass** - have been inserted into the SSL block. While the **keystoreFile** parameter has to be set to the full path to the **.keystore** file that you generated earlier, the **keystorePass** parameter should be set to the keystore password that you specified while issuing the **keytool** command. Likewise, the **keyAlias** parameter is to be set to the **alias name** that you provided for the certificate file, when you generated it in Section **2.8.0.2** above.

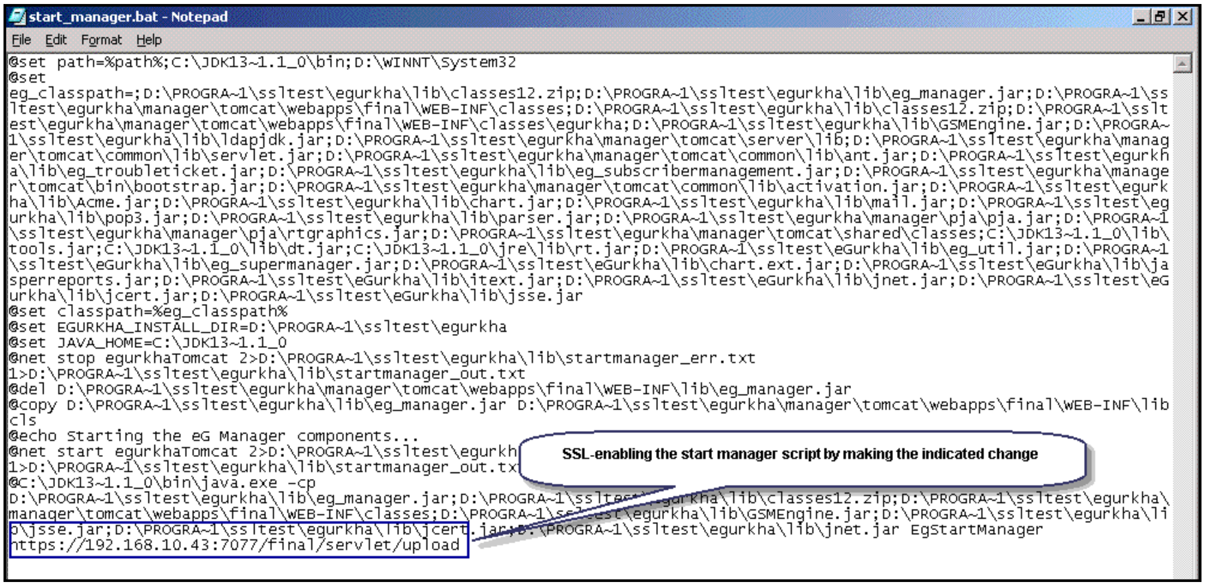
With that change, the eG manager on Windows has acquired the capability to listen on two ports - the SSL port and the non-SSL port. To configure the eG manager to listen only on the SSL port, simply comment that section of the **server.xml** file where the non-SSL Coyote HTTP connector on port 8081 has been defined, as indicated below:

```
<!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 8081 -->
<!--
<Connector protocol=”HTTP/1.1”
port=”7077” minSpareThreads=”64” maxThreads=”512”
enableLookups=”false” redirectPort=”8443”
acceptCount=”10” connectionTimeout=”20000”
useURIValidationHack=”false”  URIEncoding=”UTF-8” tcpNoDelay=”true” compression=”on”
compressionMinSize=”1024” noCompressionUserAgents=”gozilla, traviata”
compressableMimeType=”text/html,text/xml,text/plain,application/x-java-
applet,application/octet-
stream,application/xml,text/javascript,text/css,image/png,image/jpeg,
image/gif,application/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml” server=”eG Tomcat Server”/>
-->
```

4. Save the file.

5. Then, SSL-enable the **start_manager.bat** script. For this, first open the **start_manager.bat** file

residing in the <EG_ INSTALL_ DIR>\lib directory. Change the URL *http://<eGmanagerIp>:<eGmanagerdefaultTCPPort>/final/servlet/upload* present in the last line of the batch file to *https://<eGmanagerIp>:<eGmanagerPort>/final/servlet/upload*.



```
@set path=%path%;C:\JDK13~1.1_0\bin;D:\WINNT\System32
@set
eg_classpath=;D:\PROGRA~1\ssltest\egurkha\lib\classes12.zip;D:\PROGRA~1\ssltest\egurkha\lib\eg_manager.jar;D:\PROGRA~1\ss
ltest\egurkha\manager\tomcat\webapps\final\WEB-INF\classes;D:\PROGRA~1\ssltest\egurkha\lib\classes12.zip;D:\PROGRA~1\sslt
est\egurkha\manager\tomcat\webapps\final\WEB-INF\classes\egurkha;D:\PROGRA~1\ssltest\egurkha\lib\GSMEngine.jar;D:\PROGRA~
1\ssltest\egurkha\lib\ldapjdk.jar;D:\PROGRA~1\ssltest\egurkha\manager\tomcat\server\lib;D:\PROGRA~1\ssltest\egurkha\manag
er\tomcat\common\lib\servlet.jar;D:\PROGRA~1\ssltest\egurkha\manager\tomcat\common\lib\ant.jar;D:\PROGRA~1\ssltest\egurkh
a\lib\eg_troubleticket.jar;D:\PROGRA~1\ssltest\egurkha\lib\eg_subscribermanagement.jar;D:\PROGRA~1\ssltest\egurkha\manage
r\tomcat\bin\bootstrap.jar;D:\PROGRA~1\ssltest\egurkha\manager\tomcat\common\lib\activation.jar;D:\PROGRA~1\ssltest\egurk
ha\lib\Acme.jar;D:\PROGRA~1\ssltest\egurkha\lib\chart.jar;D:\PROGRA~1\ssltest\egurkha\lib\mail.jar;D:\PROGRA~1\ssltest\eg
urkha\lib\pop3.jar;D:\PROGRA~1\ssltest\egurkha\lib\parser.jar;D:\PROGRA~1\ssltest\egurkha\manager\pja\pja.jar;D:\PROGRA~1
\ssltest\egurkha\manager\pja\rtgraphics.jar;D:\PROGRA~1\ssltest\egurkha\manager\tomcat\shared\classes;C:\JDK13~1.1_0\lib\
tools.jar;C:\JDK13~1.1_0\lib\dt.jar;C:\JDK13~1.1_0\jre\lib\rt.jar;D:\PROGRA~1\ssltest\eGurkha\lib\eg_util.jar;D:\PROGRA~1
\ssltest\eGurkha\lib\eg_supermanager.jar;D:\PROGRA~1\ssltest\eGurkha\lib\chart.ext.jar;D:\PROGRA~1\ssltest\eGurkha\lib\ja
sperreports.jar;D:\PROGRA~1\ssltest\eGurkha\lib\itext.jar;D:\PROGRA~1\ssltest\eGurkha\lib\jnet.jar;D:\PROGRA~1\ssltest\eG
urkha\lib\jcert.jar;D:\PROGRA~1\ssltest\eGurkha\lib\jsse.jar
@set classpath=%eg_classpath%
@set EGURKHA_INSTALL_DIR=D:\PROGRA~1\ssltest\egurkha
@set JAVA_HOME=C:\JDK13~1.1_0
@net stop egurkhaTomcat 2>D:\PROGRA~1\ssltest\egurkha\lib\startmanager_err.txt
1>D:\PROGRA~1\ssltest\egurkha\lib\startmanager_out.txt
@del D:\PROGRA~1\ssltest\egurkha\manager\tomcat\webapps\final\WEB-INF\lib\eg_manager.jar
@copy D:\PROGRA~1\ssltest\egurkha\lib\eg_manager.jar D:\PROGRA~1\ssltest\egurkha\manager\tomcat\webapps\final\WEB-INF\lib
cls
@echo Starting the eG Manager components...
@net start egurkhaTomcat 2>D:\PROGRA~1\ssltest\egurkh
1>D:\PROGRA~1\ssltest\egurkha\lib\startmanager_out.tx
@C:\JDK13~1.1_0\bin\java.exe -cp
D:\PROGRA~1\ssltest\egurkha\lib\eg_manager.jar;D:\PROGRA~1\ssltest\egurkha\lib\classes12.zip;D:\PROGRA~1\ssltest\egurkha\
manager\tomcat\webapps\final\WEB-INF\classes;D:\PROGRA~1\ssltest\egurkha\lib\GSMEngine.jar;D:\PROGRA~1\ssltest\egurkha\li
b\jsse.jar;D:\PROGRA~1\ssltest\egurkha\lib\jcert.jar;D:\PROGRA~1\ssltest\egurkha\lib\jnet.jar EgStartManager
https://192.168.10.43:7077/final/servlet/upload
```

SSL-enabling the start manager script by making the indicated change

Figure 2.103: SSL-enabling the start_manager script

6. Next, make sure that the eG manager URL configured against the **MailHomeURL** parameter in the **[MISC_ ARGS]** section of the **eg_ services.ini** file (in the <EG_ INSTALL_ DIR>\manager\config directory) begins with **https://** instead of http://. Then, save the file.
7. Finally, start the eG manager.

Note:

Owing to SSL vulnerabilities that were discovered, many changes have been made in v6.1.2 to harden SSL communication with the eG manager. These include the following:

- Starting from version 6.1.2, TLS v1 will be the default secure protocol that web browsers will use to communicate with the eG manager.
- Recent versions of Firefox and Chrome expect a strong Cipher suite definition in SSL-enabled web/web application servers. HTTPS requests to web/web application servers that do not contain this Cipher Suite definition will be rejected by the Firefox and Chrome browsers. To avoid this, in version 6.1.2, this Cipher Suite definition has been bundled into the Tomcat server on which the eG manager runs.
- In the default SSL certificate that eG bundles with the eG manager, the message signing algorithm has been changed.

All these changes however, **will not be available to any SSL manager that is upgraded from a lower version to v6.1.2**. This is why, after a manager is upgraded to v6.1.2, you will experience problems communicating with the manager via HTTPS.

To avoid this, after an SSL-enabled manager is upgraded to version 6.1.2, you have to harden the SSL communication with the upgraded manager, following the steps detailed below:

- Edit the **server.xml** file in the <CATALINA_HOME>/conf directory (on Unix; on Windows, this will be the <CATALINA_HOME>\conf directory) on the eG manager host:
- Look for the SSL connector definition in the file.
- Locate the *sslProtocol* parameter in the definition.
- After the *sslprotocol* parameter, insert the following:

```
sslEnabledProtocols=”TLSv1”
```

- Then, include the following Cipher Suite definition:

```
ciphers=”TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_
ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,   TLS_RSA_WITH_
AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_
RSA_WITH_AES_256_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA”
```

Note:

- Once the aforesaid changes are made, the SSL connector definition in your **server.xml** will look as shown below:

```
<Connector protocol=”HTTP/1.1”
```

```
port=”<eGManagerPort>” minSpareThreads=”64” maxThreads=”512”
```

```
enableLookups=”false” acceptCount=”10”  connectionTimeout=”20000”
```

```
useURIValidationHack=”false” URIEncoding=”UTF-8” tcpNoDelay=”true” compression=”on”
compressionMinSize=”1024” noCompressionUserAgents=”gozilla, traviata”
compressableMimeType=”text/html,text/xml,text/plain,application/x-java-
applet,application/octet-
stream,application/xml,text/javascript,text/css,image/png,image/jpeg,
image/gif,application/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml”
```

```
SSLEnabled=”true” scheme=”https” secure=”true”
```

```
clientAuth=”false” sslProtocol=”TLS” sslEnabledProtocols=”TLSv1”ciphers=”TLS_ECDHE_
RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_
256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,   TLS_RSA_WITH_AES_128_CBC_
SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_
256_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA”
```

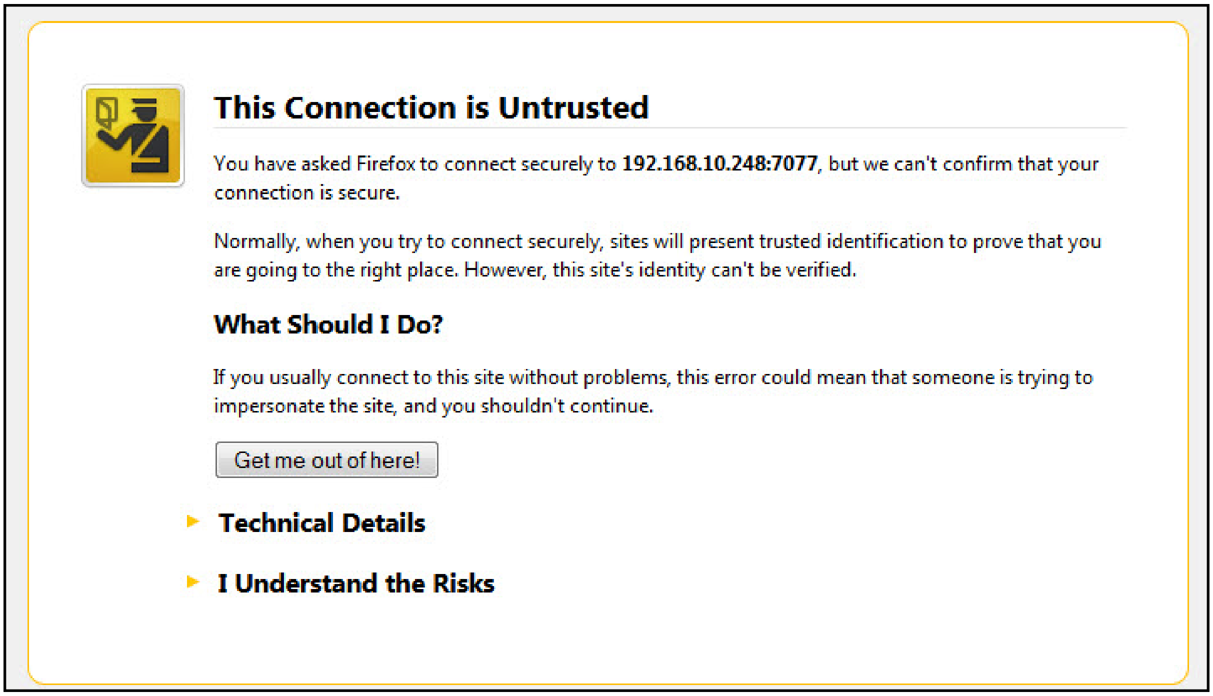
```
keystoreFile=”<PathtoKeystoreFile>” keystorePass=”<Keystorepass>” server=”eG Tomcat
Server”/>
```

- Next, save the file.
- If you had SSL-enabled the eG manager using the default certificate that eG provides, then, once the above changes are made, copy the default certificate from the <EG_INSTALL_DIR>\bin\latest_certificate folder (on Windows; on Unix, this will be the **/opt/egurkha/bin/latest_certificate** folder), to the <EG_INSTALL_DIR>\manager/tomcat/webapps folder (on Windows; on Unix, this will be the **/opt/egurkha/manager/tomcat/webapps** folder).
- Finally, restart the eG manager.

2.8.0.10 SSL-Enabling the eG Manager

How to differentiate between a public and private certificate?

A private certificate is often a self-signed certificate that is not validated by any certifying authority. This is why, when connecting to an eG manager that has been SSL-enabled using a self-signed certificate, the following error message appears:



This Connection is Untrusted

You have asked Firefox to connect securely to **192.168.10.248:7077**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Figure 2.104: The error message that appears when connecting to an eG manager using a self-signed SSL certificate

A public certificate on the other hand is a trusted certificate issued by a valid Certificate Authority. If such a certificate is used to SSL-enable an eG manager, then, a ‘lock’ symbol will appear in the address bar of the browser when attempting to connect to that manager (see Figure 2.105).

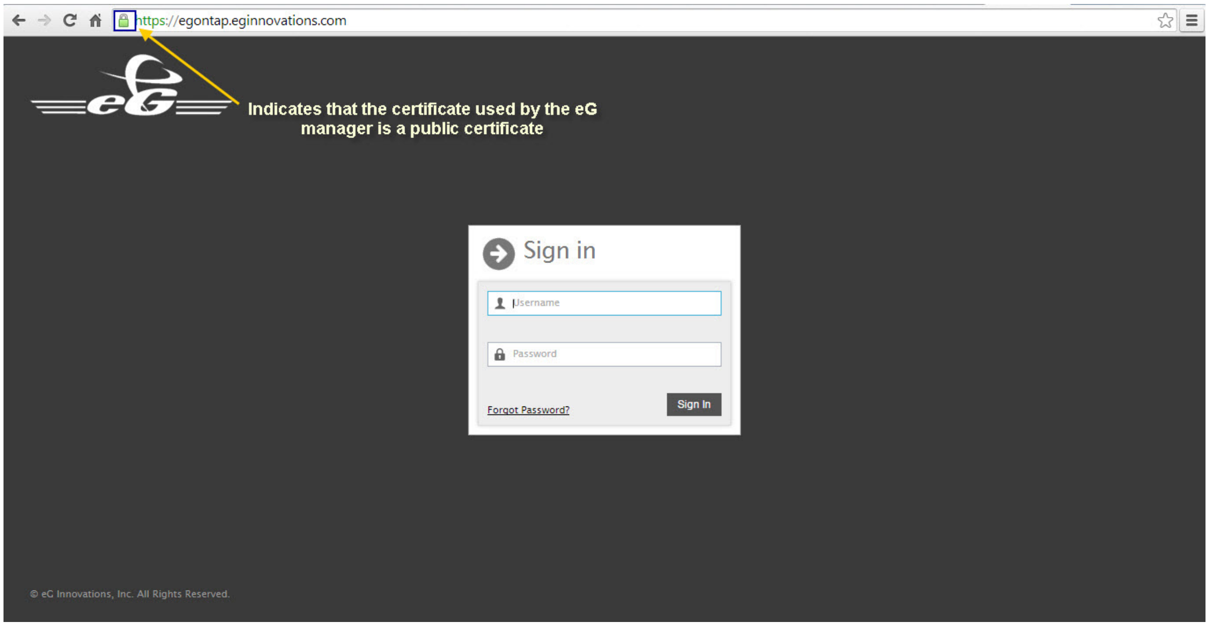
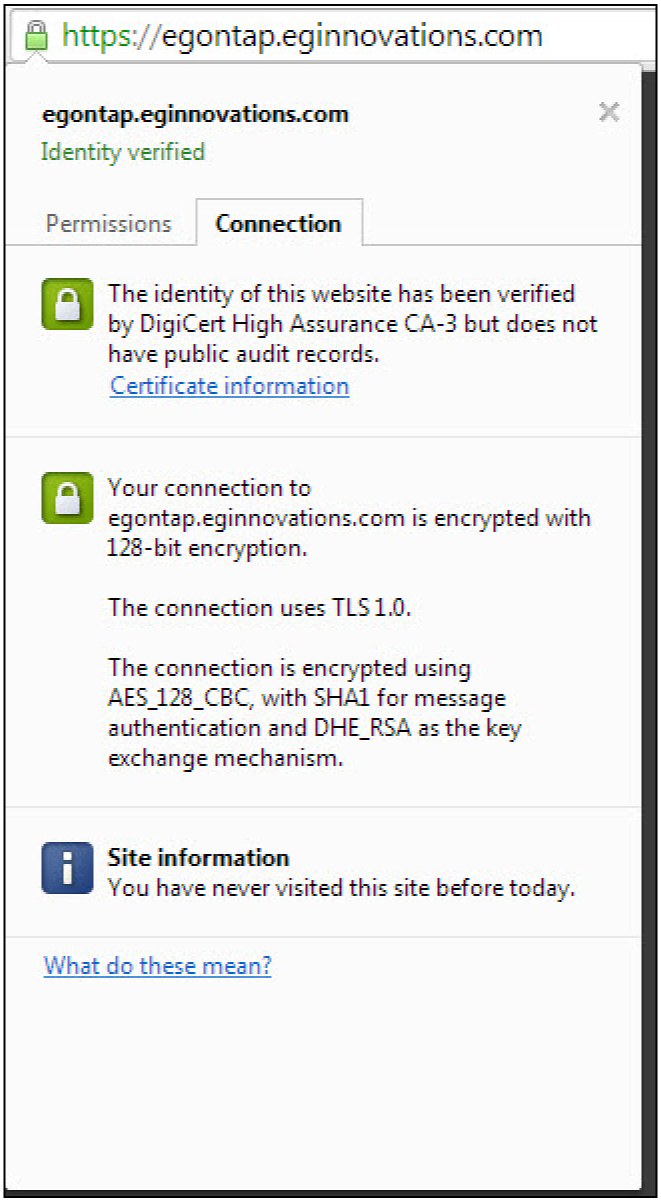

https://egontap.eginnovations.com
Indicates that the certificate used by the eG manager is a public certificate
Sign in
Username
Password
Forgot Password?
Sign In
© eG Innovations, Inc. All Rights Reserved.

Figure 2.105: A lock symbol in the address bar indicating that the SSL certificate used by the eG manager is a public certificate

To view the certificate, click the 'lock symbol'. From the options that drop down, select the **Connection** tab page (see Figure 2.106).



egontap.eginnovations.com

Identity verified

The identity of this website has been verified by DigiCert High Assurance CA-3 but does not have public audit records.

Certificate information

Your connection to egontap.eginnovations.com is encrypted with 128-bit encryption.

The connection uses TLS 1.0.

The connection is encrypted using AES_128_CBC, with SHA1 for message authentication and DHE_RSA as the key exchange mechanism.

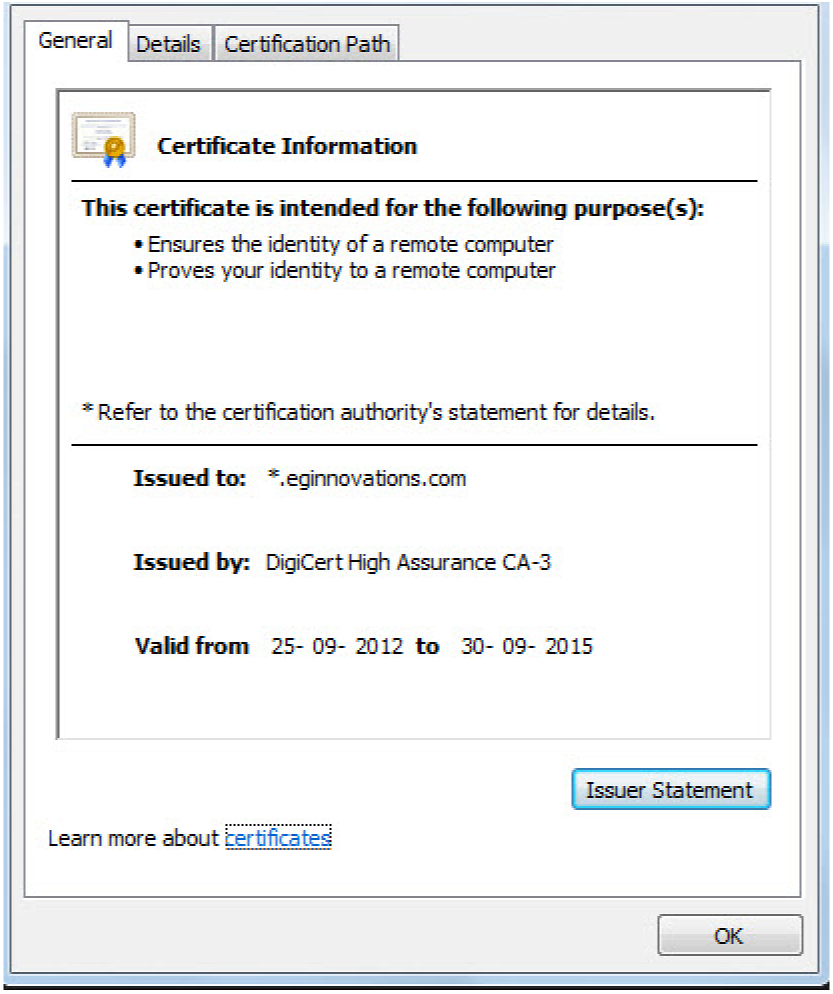
Site information

You have never visited this site before today.

What do these mean?

Figure 2.106: Viewing the connection details

To view the certificate details, click the **Certificate Information** link in Figure 2.106. Figure 2.107 will then appear, revealing the details of the SSL certificate.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer

* Refer to the certification authority's statement for details.

Issued to: *.eginnovations.com

Issued by: DigiCert High Assurance CA-3

Valid from 25- 09- 2012 to 30- 09- 2015

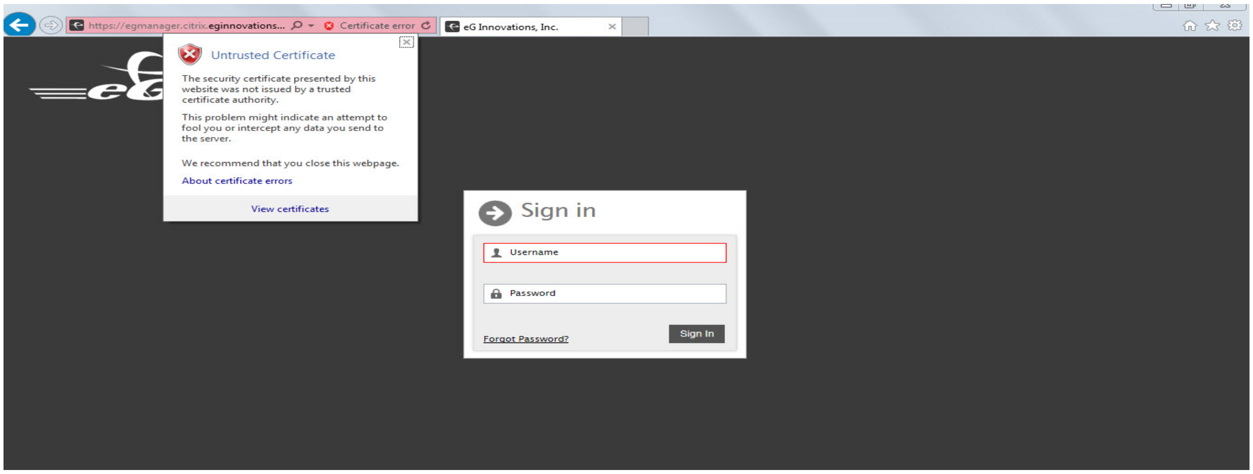
Figure 2.107: Viewing the Certificate information

Troubleshooting the error message “Public keys in reply and keystore don’t match”

If the above error message appears when importing a certificate into a keystore, it could imply that you have not downloaded all the certificates that are part of the certificate chain. In this case, go to the web site of the certifying authority to download the certificates. Then, try to import each certificate in sequence of their type – i.e., import the root certificate first, the intermediate certificates next, and the domain certificate last.

Troubleshooting the “Certificate error” that occurs when accessing an eG manager that is SSL-enabled using a certificate from an internal CA

Typically, when you attempt to access an eG manager that has been SSL-enabled using the certificate obtained from an internal CA, the browser will throw the following error message:



Untrusted Certificate

The security certificate presented by this website was not issued by a trusted certificate authority.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

Figure 2.108: The “Certificate error” that the browser reports

To avoid this error, you will have to import the internal CA’s root certificate to the browser and store it as a ‘trusted root certificate’. For this, follow the broad steps outlined below:

1. Copy the internal CA’s root certificate to the host from which you are accessing the eG manager (i.e., the browser host). For instance, if Microsoft Active Directory Certificate Services is your internal CA, then, you will find the root certificate of this CA on your domain server. So, in this case, you will have to copy the root certificate from the domain server to your browser host.
2. Next, using Windows Explorer, browse for the certificate, and once found, right-click on it. From the shortcut menu that appears, select the **Install Certificate** option (see Figure 2.109) to import the certificate to the browser.

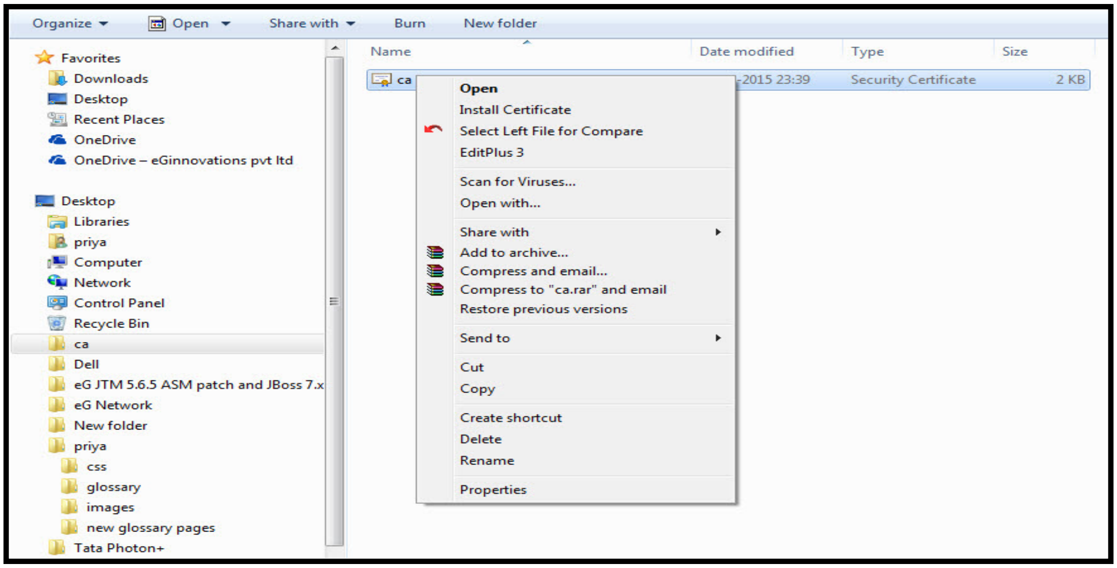
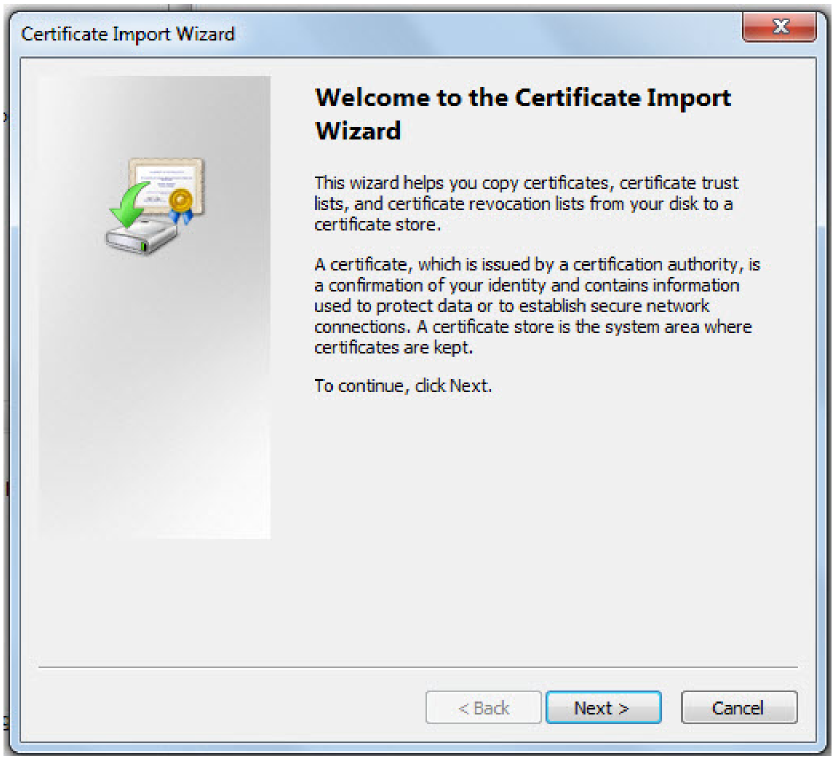


Figure 2.109: Selecting the option to install the certificate on the browser host

3. Figure 2.110 will then appear. Click **Next** here to continue.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

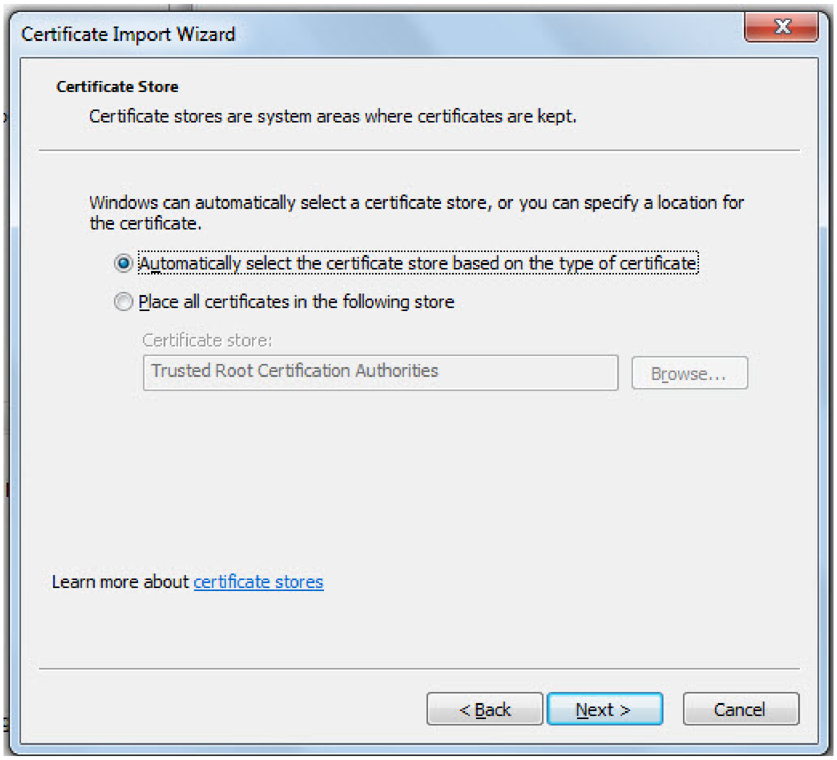
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Figure 2.110: Welcome screen of the Certificate Import Wizard

4. Figure 2.111 will then appear. Here, select the **Place all certificates in the following store**

option, and click the **Browser** button to indicate where the certificate is to be stored.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

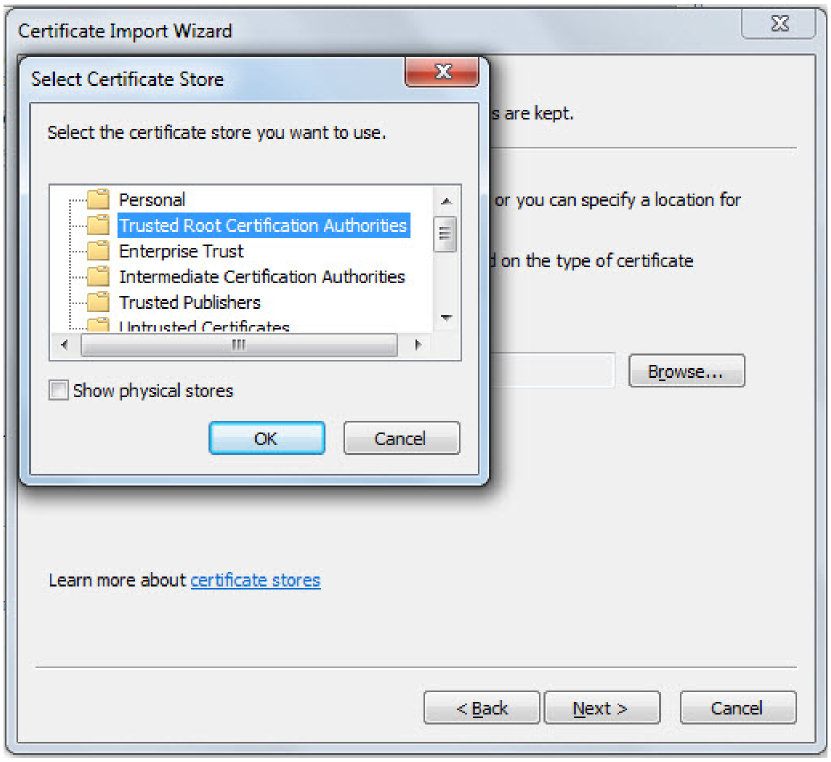
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Figure 2.111: Choosing to place the certificate in a specific store

5. From Figure 2.112 that then appears, select the **Trusted Root Certificate Authorities** store and click **OK**.



Select the certificate store you want to use.

s are kept.

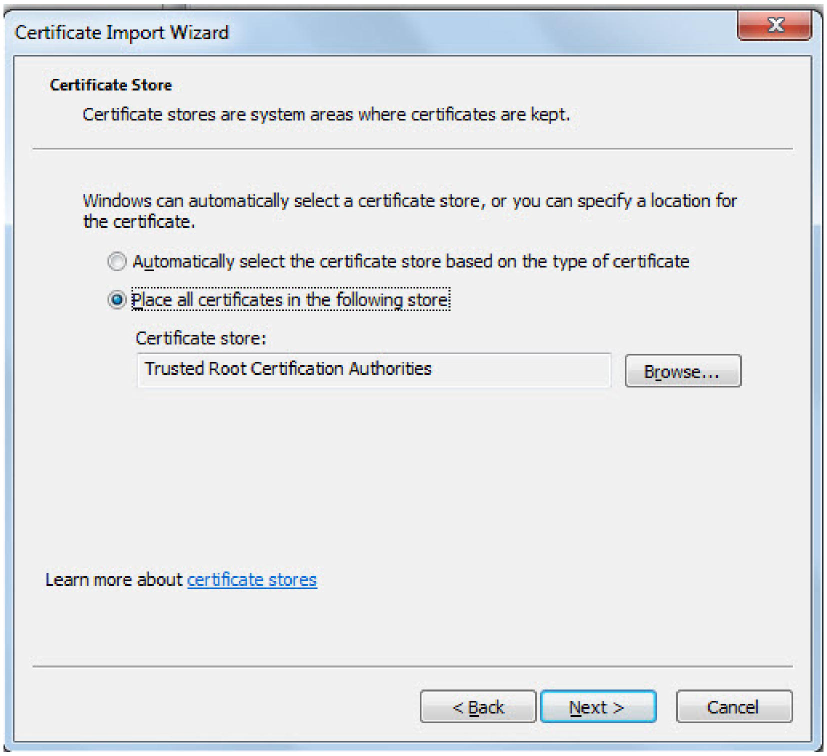
or you can specify a location for

d on the type of certificate

Learn more about certificate stores

Figure 2.112: Storing the certificate in the Trusted Root Certificate Authorities store

6. The chosen store will then appear in the text box below **Place all certificates in the following store** option, as depicted by Figure 2.113. Click **Next** in Figure 2.113 to continue.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

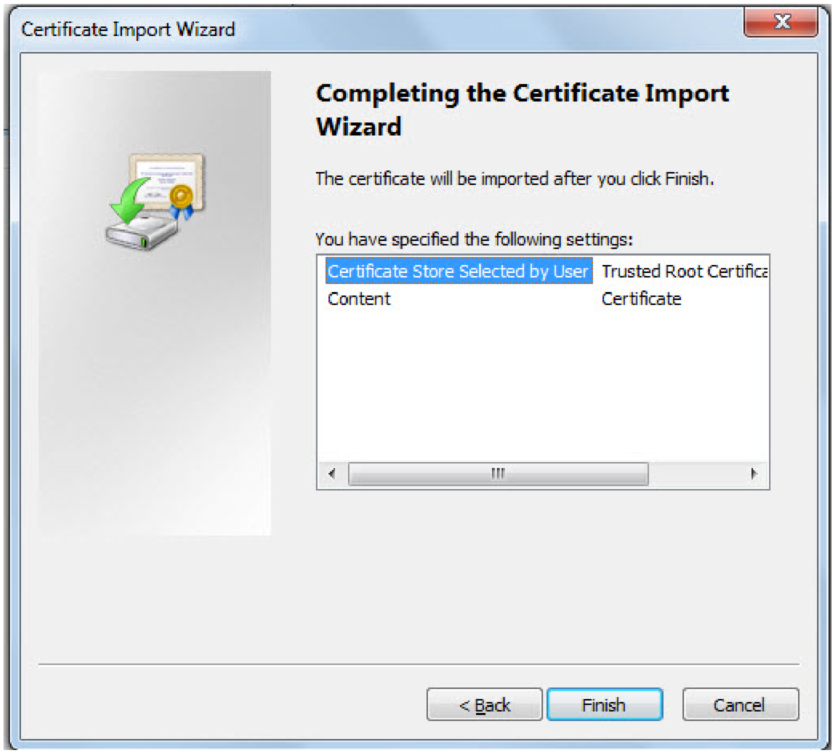
● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Figure 2.113: The chosen store displayed

7. A quick summary of your selections will appear in Figure 2.114. Review your specifications and click **Finish** to complete the import.



Certificate Import Wizard

Completing the Certificate Import Wizard

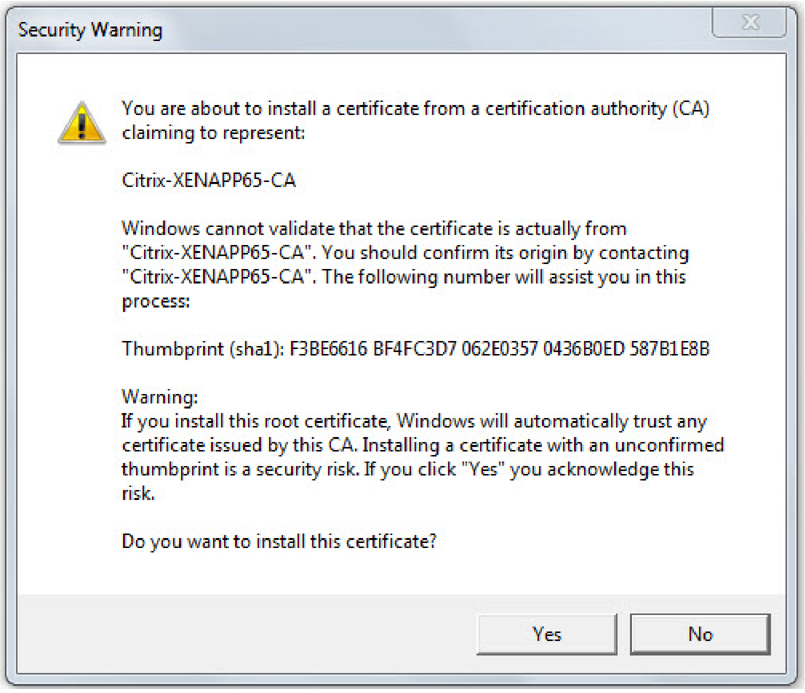
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certifica
Content	Certificate

Figure 2.114: Finishing the import

8. The following warning message will appear. Click **Yes** in Figure 2.115 to proceed with the import.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

Citrix-XENAPP65-CA

Windows cannot validate that the certificate is actually from "Citrix-XENAPP65-CA". You should confirm its origin by contacting "Citrix-XENAPP65-CA". The following number will assist you in this process:

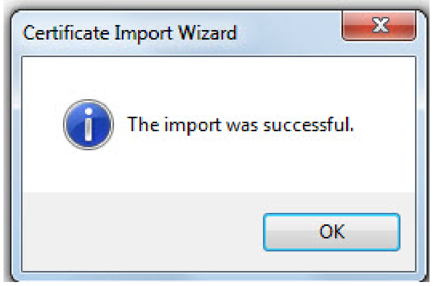
Thumbprint (sha1): F3BE6616 BF4FC3D7 062E0357 0436B0ED 587B1E8B

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Figure 2.115: A warning message that appears when importing a certificate issued by an internal CA

9. If import is successful, the following message will appear. Click **OK**.



Certificate Import Wizard

The import was successful.

Figure 2.116: A message box informing you that the certificate has been successfully imported

You will now be able to access the eG manager without a glitch!

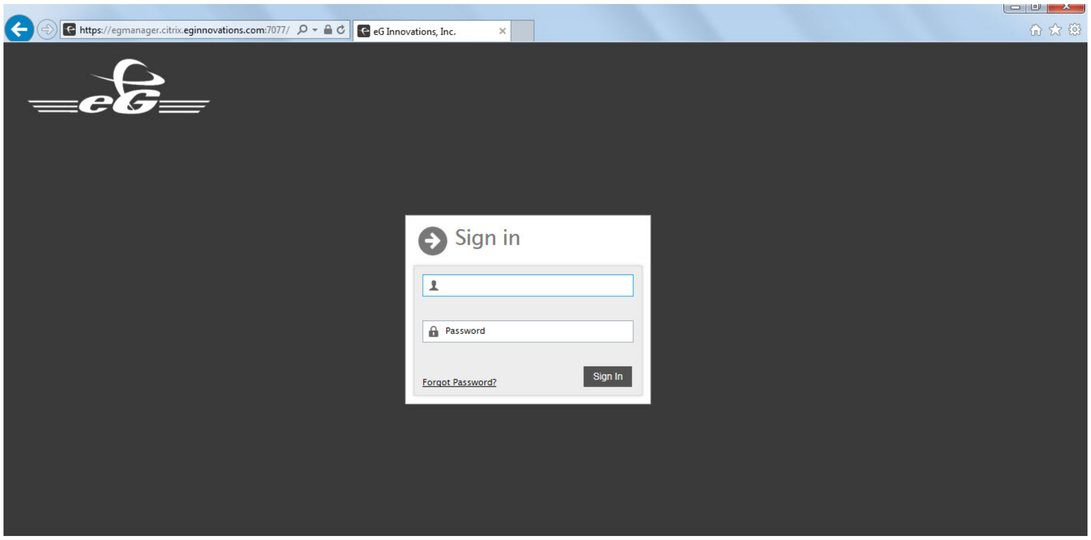


Figure 2.117: The login screen of the eG manager, without the 'Certificate error'

How to convert a certificate from the p7b format to a PEM format?

Digital certificates issued by Microsoft are in a format (p7b) that cannot be used by Tomcat. Therefore, if you have obtained a valid certificate using Microsoft Active Directory Certificate Services as the CA, then, before attempting to import that certificate into a keystore file (i.e., before getting to the 2.8.0.9), you will have to convert the digital certificate in p7b (PKCS#7) format to PEM format on Windows. To achieve this, follow the steps below:

1. Login to the eG manager host.
2. In Windows Explorer, search for the certificate file with the extension **.p7b**.
3. Once you find it, double-click on it. This will open the **Certificates** window (see Figure 2.118).

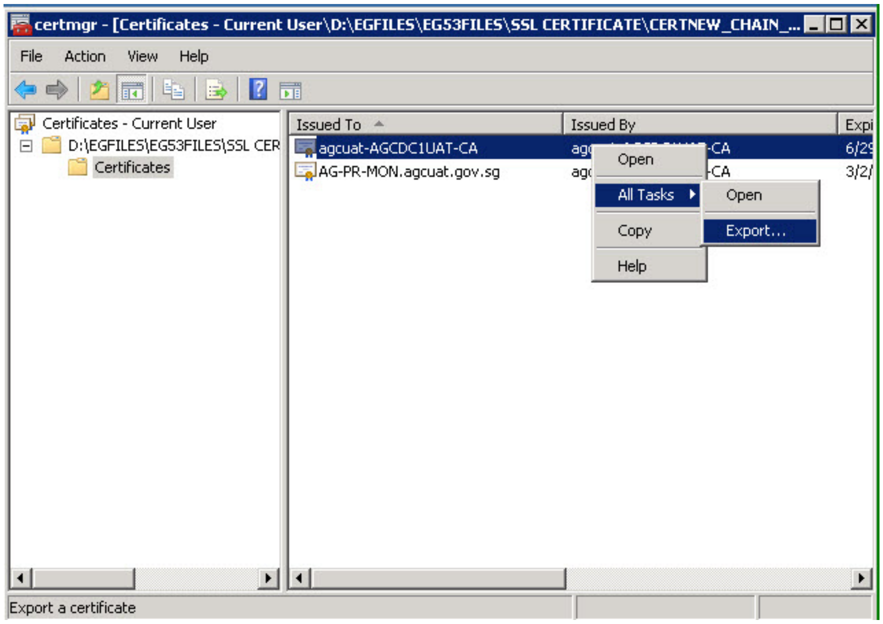

certmgr - [Certificates - Current User\D:\EGFILES\EG53FILES\SSL CERTIFICATE\CERTNEW_CHAIN_...
File
Action
View
Help
Certificates - Current User
D:\EGFILES\EG53FILES\SSL CER
Certificates
Issued To
Issued By
Expi
agcuat-AGCDC1UAT-CA
AG-PR-MON.agcuat.gov.sg
Open
All Tasks
Copy
Help
Open
Export...
Export a certificate

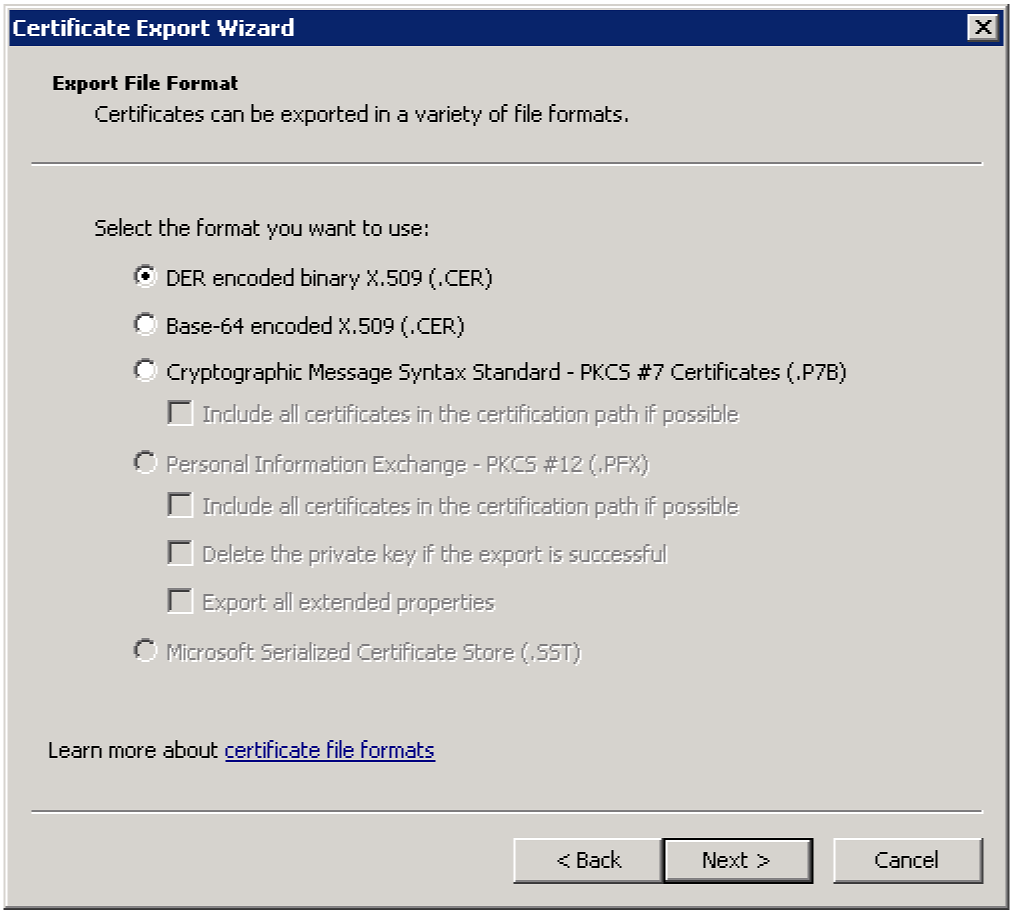
Figure 2.118: The Certificates window

4. In the left panel of the **Certificates** window, you will find a tree-structure with a list of certificate files available on the eG manager host for the current user. Expand the SSL Certificate file node and then click on the **Certificates** sub-node within. The right panel will then display the certificates.

5. From the certificates list in the right panel, select the certificate that needs to converted into the PEM format, right-click on it, and follow the *All Tasks* -> *Export* menu sequence in the shortcut menu that appears (see Figure 2.118).

6. A wizard will appear. Click **Next** in the wizard to proceed.

7. Figure 2.119 will then appear. Select the **DER encoded binary X.509 (.CER)** option in Figure 2.119 and click the **Next** button.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Figure 2.119: Converting the certificate into PEM format

8. You will now be prompted for a **File name**. Provide a name for the converted digital certificate, and click **Next**.

2.8.1 SSL-enabling the eG Manager on Unix

The eG manager on Unix includes a default SSL certificate. If you SSL-enable the eG manager using this default certificate, then all you need to do is enter **y** when the eG manager setup process requests you to indicate whether the manager is to be SSL-enabled or not. Doing so will instantly enable the eG agent to communicate with the eG manager via HTTPS.

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

a. You can obtain a signed certificate from an internal certifying authority (eg., Microsoft Active Directory Certificate Services) and use this certificate to SSL-enable the eG manager, (OR)

b. You can obtain a signed certificate from a valid, external certifying authority (eg., Verisign) and use this certificate to SSL-enable the eG manager

If you go with option (a), use the procedure detailed in the Section **2.8.1.1** topic. If you pick option (b), use the procedure detailed in Section **2.8.0.5** topic.

2.8.1.1 SSL-Enabling the eG Manager Using a Certificate Signed by an Internal CA

If you do not want to use the default SSL certificate bundled with the eG manager, then you can generate a self-signed certificate using an internal certificate authority and use it instead for SSL-enabling the agent-manager communication.

For this, follow the steps given below:

- Generate the Keystore file
- Generate a certificate request
- Submit the certificate request to the internal certificate Authority (CA) and obtain a certificate
- Import the certificate into a keystore
- Configure Tomcat for using the keystore file

Each of these steps has been discussed in the sections that follow.

2.8.1.2 Generating the Keystore File

The keystore file stores the details of the **certificates** necessary to make the protocol secure. Certificates contain the information pertaining to the source of the application data, and helps validate the source. To generate the keystore, use the **keytool** command. For this purpose, login to the manager and go to the shell prompt. Set the **JAVA_HOME** path if it is not done already. Then, execute the following commands, one after another:

cd $JAVA_HOME/bin

*keytool -genkey -alias **egitlab1** -keyalg **RSA** -keypass mykey -keystore <Filename>.keystore -storepass **mykey** -keysize **1024** -validity **1095***

The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

- **-alias :** an alias name for the certificate being generated
- **-keypass :** a password used to protect the key that is generated; ensure that you provide the same values for **-keypass** and **-storepass**.
- **-keyalg :** specifies the algorithm that is used to generate the keys. The options are as follows:

  - **DSA :** Digital Signature Algorithm
  - **RSA :** An algorithm used for public-key cryptography

- **-keystore** : the *keytool* command stores the generated key in a *.keystore* file; provide a name for this file as input to the **-keystore** command
- **-keysize** : the size of the key that is generated; the default key size is 1024 bits - the key size must be in the range 512 bits - 1024 bits
- **-validity** : indicates the number of days for which the key/certicate will be valid - 1095 days refer to 3 years.

The command, upon execution, will request the following inputs:

```
What is your first and last name?
[Unknown]: <Type the eG manager's Fully qualified domain name here>
What is the name of your organizational unit?
[Unknown]: United States
What is the name of your organization?
[Unknown]: eG Innovations Inc
What is the name of your City or Locality?
[Unknown]: Bridge Water
What is the name of your State or Province?
[Unknown]: New Jersey
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=eG Innovations Inc, OU=United States, O=eG Innovations Inc, L=Bridge Water, ST=New
Jersey, C=US correct?
[no]: yes
```

When requested for the **first and last name**, indicate the *fully qualified domain name* using which you will be accessing the eG manager. For instance, if the eG manager is to be accessed as *http://egmanager.eginnovations.com*, where *egmanager.eginnovations.com* is the fully qualified domain name of the eG manager, then specify *egmanager.eginnovations.com* here.

Once all the required inputs are provided, a .keystore file will be generated in the <JAVA_HOME_DIR>/bin directory with the <Filename> you had provided while issuing the command.

2.8.1.2.1 Generating a Certificate Request

Once a keystore file is generated, proceed to request for a certificate from an internal certifying authority. The procedure for this is as follows:

1. Login to the eG manager and go to the command prompt.
2. Set the **JAVA_HOME** path if it is not done already.
3. Execute the following commands one after another:

   cd $JAVA_HOME/bin

   keytool -certreq -alias *egitlab1* ***-keyalg RSA*** *-file <Name_of_the_text_file> -**keypass** mykey **-keystore** <filename>.keystore **–storepass** mykey*

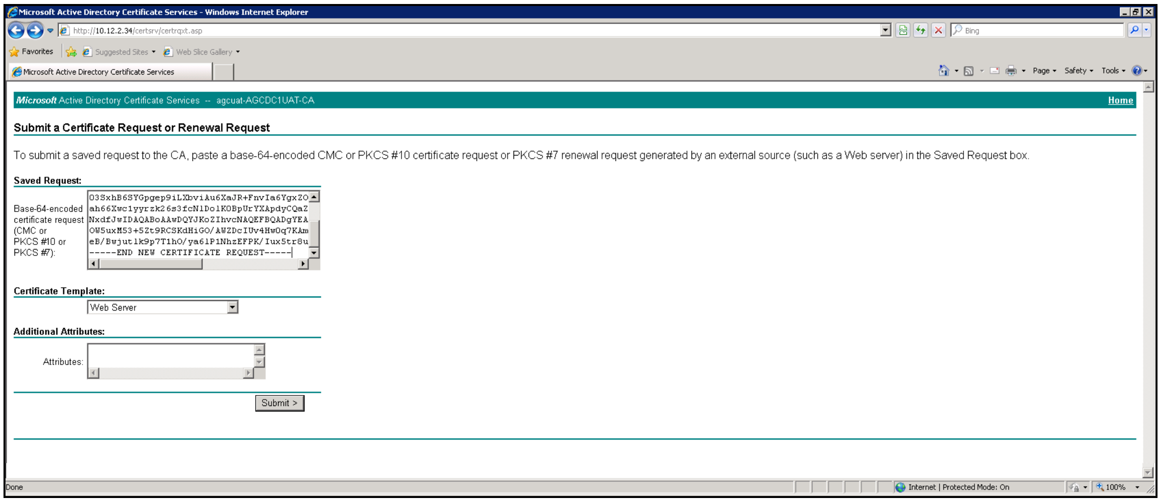
   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; **make sure that you provide the same alias name that you provided while generating the keystore file** (see Section **2.8.1.2**).
   - **-keyalg** : specifies the algorithm that was used to generate the keys; this can be **RSA** or **DSA**, depending upon **which algorithm was used for key generation in the procedure detailed in** Section **2.8.1.2**
   - **-file** : Provide a name for the text file to which the certificate request will be saved.
   - **-keypass** : the password used to protect the key that was generated; **make sure that you provide the same password that you provided while generating the keystore file** (see Section **2.8.1.2**). Also, note that **-storepass** and **-keypass** should be the same.
   - **-keystore** : Provide the name of the *keystore* file in which the key has been stored; **specify the same file name that you used to store the key** (see Section **2.8.1.2**).

4. If this command executes successfully, then a certificate request will be generated and automatically stored in the text file you specified in step 2 above.

2.8.1.2.2 Obtaining the Certificate from the Internal CA

1. The first step towards obtaining a certificate is to submit the certificate request to the internal CA. For this connect to the Certificate server of the internal CA and select the option to submit the certificate. For instance, if you are using Microsoft Active Directory Certificate Services to request for a self- signed certificate, then, you need to connect to **http://<YourWebServerName>/certsrv**, and then pick the option to submit the certificate. Figure 2.120 will then appear.



Microsoft Active Directory Certificate Services - Windows Internet Explorer
http://10.12.2.34/certsrv/certrqxt.asp
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Certificate Services
Page
Safety
Tools
Home

Microsoft Active Directory Certificate Services -- agcuat-AGCDC1UAT-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
O3SxhB6SYGpgep9iLXbviAu6XaJR+FnvIa6YgxZO
ah66Xwc1yyrzk26s3fcNlDolKOBpUrYXApdyCQaZ
NxdfJwIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEA
OW5uxM53+5Zt9RCSKdHiGO/AWZDcIUv4HwOq7KAm
eB/Bwjutlk9p7T1hO/ya6lP1NhzEFPK/Iux5tr8u
-----END NEW CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

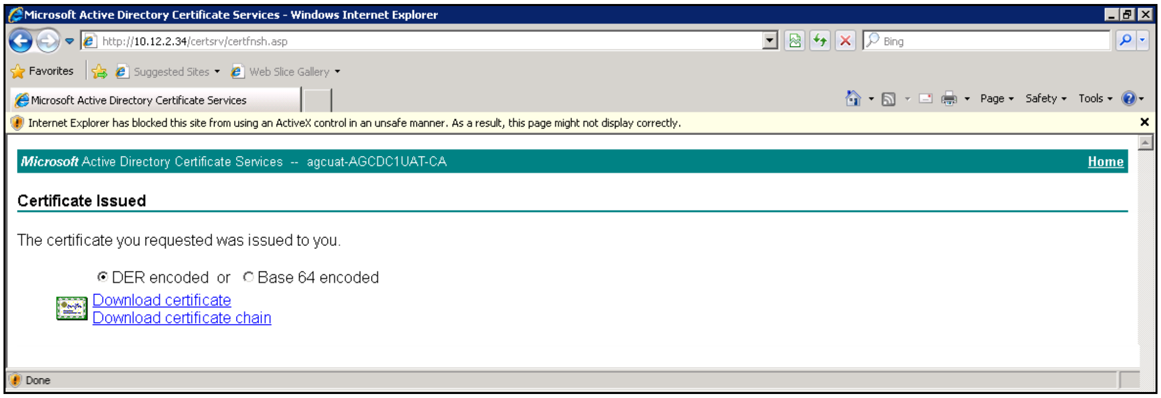
Attributes:

Submit >

Figure 2.120: Requesting for a certificate

2. Open the text file containing the certificate request (which was created using the procedure detailed in Section **2.8.0.3** above), copy the contents of the file, and then paste it to the text area of the **Base 64-encoded certificate request** text box of Figure 2.120. Then, click the **Submit** button.

3. The certificate will thus be generated. Download the certificate.



Microsoft Active Directory Certificate Services - Windows Internet Explorer
http://10.12.2.34/certsrv/certfnsh.asp
Bing
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Certificate Services
Page
Safety
Tools
Home

Internet Explorer has blocked this site from using an ActiveX control in an unsafe manner. As a result, this page might not display correctly.

Microsoft Active Directory Certificate Services -- agcuat-AGCDC1UAT-CA

Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

Download certificate
Download certificate chain

Figure 2.121: Downloading the certificate

2.8.1.2.3 Importing the Certificates into the Keystore File

The downloaded certificate can be in one of the following forms:

- Can be a single, combined certificate
- Can be accompanied by a certificate chain

- Can be in a PEM format

The procedure for importing certificates differs based on the format of the downloaded certificate. These procedures have been detailed in the sub-sections below.

Importing a Combined Certificate into the Keystore File

In this case, follow the steps below to import the certificate into the keystore file:

1. Set the **JAVA_HOME** path if it is not done already.
2. At the command prompt, execute the following commands, one after another:

   cd $JAVA_HOME/bin

   keytool -import –trustcacerts -alias ***egitlab1*** *-file* ***<Name_of_the_domain_certificate>*** *-keystore* ***<Name_of_the_keystore_file>.keystore***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; **make sure that you provide the same alias name you provided when generating the keystore** (see Section **2.8.1.2**) .
   - **-file**: the name of the domain certificate that you want to import
   - **-keystore** : Provide the name of the *keystore* file you generated when you followed the procedure detailed in Section **2.8.1.2** above.

Importing a Signed Certificate and the Certificate Chain into the Keystore File

Digital certificates are verified using a chain of trust. The trust anchor for the digital certificate is the Root Certificate Authority (CA). The Certificate Hierarchy is a structure of certificates that allows individuals to verify the validity of a certificate's issuer. Certificates are issued and signed by certificates that reside higher in the certificate hierarchy, so the validity and trustworthiness of a given certificate is determined by the corresponding validity of the certificate that signed it.

The Chain of Trust of a Certificate Chain is an ordered list of certificates, containing an end-user subscriber certificate and intermediate certificates (that represents the Intermediate CA), that enables the receiver to verify that the sender and all intermediate certificates are trustworthy.

A certificate chain will therefore consist of multiple certificates. Before importing each of these certificates, **you will have to understand the hierarchy of the certificates**. To know which is the root and which is the intermediate certificate, refer to the web site of the certificate authority. Then, set the **JAVA_HOME** path if it is not done already. Next, follow the steps below:

1. First, import the Root certificate. For this, execute the following commands, one after another in the command prompt:

   cd $JAVA_HOME/bin

   keytool -import –trustcacerts -alias ***rootcert*** *-file* ***<Name_of_the_root_certificate>*** *-keystore* ***<Name_of_the_keystore_file>.keystore*** *–keypass* ***mykey*** *–storepass* ***mykey***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; **make sure that you provide a unique alias name for the root certificate.**
   - **-file**: the name of the root certificate that you want to import
   - **-keystore** : Provide the name of the *keystore* file you generated when you followed the procedure detailed in Section **2.8.1.2** above.
   - **-keypass** and **–storepass** : Provide the same **keypass** and **storepass** that you specified when generating the keystore; refer to Section **2.8.1.2** above for details.

2. Next, import each of the intermediate certificates, one after another, using the following command:

   keytool -import –trustcacerts -alias ***intercert1****-file* ***<Name_of_the_intermediate_certificate>****-keystore* ***<Name_of_the_keystore_file>.keystore****–keypass* ***mykey****–storepass* ***mykey***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; **make sure that you provide a unique alias name for every intermediate certificate.**
   - **-file**: the name of the intermediate certificate that you want to import
   - **-keystore** : Provide the name of the *keystore* file you generated when you followed the procedure detailed in Section **2.8.1.2** above.
   - **-keypass** and **–storepass** : Provide the same **keypass** and **storepass** that you specified when generating the keystore; refer to Section **2.8.1.2** above for details.

3. Finally, import the entity/domain certificate into the keystore by issuing the following command:

   keytool -import –trustcacerts -alias ***egitlab1*** *-file* ***<Name_of_the_domain_certificate>*** *-keystore* ***<Name_of_the_keystore_file>.keystore***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; **make sure that you provide the same alias name you provided when generating the keystore** (see Section **2.8.1.2**) .
   - **-file**: the name of the domain certificate that you want to import
   - **-keystore** : Provide the name of the *keystore* file you generated when you followed the procedure detailed in Section **2.8.1.2**.

   Note:

   If the domain certificate import command throws an error for any reason, it could be because, all related certificates may not have been imported. Check the web site of the CA for more details.

Importing a Certificate that is in the PEM Format

PEM is a container format that may include just the public certificate (such as with Apache installs, and CA certificate files */etc/ssl/certs*), or may include an entire certificate chain including public key, private key, and root certificates, or may only contain a certificate and a private key.

If the certificate you downloaded is in the PEM format and includes only a certificate file and a private key file, then follow the steps below to import that certificate into a keystore file.

1. Run the following command from the command prompt to export the certificate and private key file into the pkcs12 format:

   openssl pkcs12 -export -in ***certificate.crt*** *-inkey* ***private.key*** *-certfile* ***certificate.crt*** *-name "****My certificate"*** *-out* ***keystore****.p12*

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-in** : the name of the certificate that is included in the PEM container
   - **-inkey**: the name of the private key file the PEM container consists of
   - **-certfile** : the name of the certificate that is included in the PEM container

- **-name** : Provide a **unique name for the certificate file** that is being exported.
- **-out** : Specify the name of the keystore file to which the certificate and private key are to be exported. **The keystore file can have any name of your choice.**

2. Next, you need to convert the keystore file, which is currently in the pkcs12 format, into the Java keystore (i.e., JKS) format. For this, issue the following command at the command prompt:

   keytool -importkeystore –alias ***egitlab1*** *-deststorepass* ***mykey*** *-destkeypass* ***mykey*** *-destkeystore* ***keystore,jks*** *-srckeystore* ***keystore.pk12*** *-srcstoretype PKCS12 -srcstorepass* ***mykey***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the aliasname of the certificate being requested; **make sure that you provide the same alias name that you specified in** Section **2.8.1.2**.
   - **-deststorepass** : this refers to the **storepass** of the destination keystore file – i.e., the keystore file in the JKS format. **The storepass of the destination keystore should be the same as the storepass of the source keystore.**
   - **-destkeypass** : this refers to the **keypass** of the destination keystore file - i.e., the keystore file in the JKS format. **The storepass and keypass of the destination keystore file should be the same.**
   - **-destkeystore**: the name of the destination keystore file – i.e., the keystore file in the JKS format.
   - **-srckeystore** : the name of the destination keystore file – i.e., the keystore file in the PKCS12 format.
   - **-srcstorepass** : The **storepass** of the source keystore file – i.e., the keystore file in the PKCS12 format. **Make sure that you provide the same storepass you specified in** Section **2.8.1.2**.

2.8.1.2.4 Configuring Tomcat for Using the Keystore File

The eG manager on Unix uses Tomcat 6.0 as the web server. Therefore, to SSL-enable the eG manager, you need to configure the **server.xml** file of Tomcat with the name and full path to the keystore file which was created earlier.

For this purpose, do the following:

1. Stop the eG manager.
2. Edit the **server.xml** file in the <CATALINA_HOME>/conf directory.
3. In the file, search for the XML block where the SSL Coyote HTTP connector on port 8443 is defined. If this block is commented, it indicates that the eG manager is not SSL-enabled and is hence listening on an HTTP port only. To SSL-enable the eG manager, first uncomment this block as indicated below:

```
<Connector protocol=”HTTP/1.1”
port=”8443” minSpareThreads=”64” maxThreads=”512”
enableLookups=”false” acceptCount=”10”  connectionTimeout=”20000”
useURIValidationHack=”false” URIEncoding=”UTF-8” tcpNoDelay=”true” compression=”on”
compressionMinSize=”1024” noCompressionUserAgents=”gozilla, traviata”
compressableMimeType=”text/html,text/xml,text/plain,application/x-java-
applet,application/octet-
stream,application/xml,text/javascript,text/css,image/png,image/jpeg,
image/gif,application/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml”
SSLEnabled=”true” scheme=”https” secure=”true”
clientAuth=”false” sslProtocol=”TLS” sslEnabledProtocols=”TLSv1” ciphers=”TLS_ECDHE_
RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_
256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_
RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_
SHA,SSL_RSA_WITH_RC4_128_SHA” />
```

4. Then, proceed to make the changes indicated in **Bold** below in the SSL XML block:

```
<Connector protocol=”HTTP/1.1”
port=”<eG_Manager_Port>” minSpareThreads=”64” maxThreads=”512”
enableLookups=”false” acceptCount=”10”  connectionTimeout=”20000”
useURIValidationHack=”false” URIEncoding=”UTF-8” tcpNoDelay=”true” compression=”on”
compressionMinSize=”1024” noCompressionUserAgents=”gozilla, traviata”
compressableMimeType=”text/html,text/xml,text/plain,application/x-java-
applet,application/octet-
stream,application/xml,text/javascript,text/css,image/png,image/jpeg,
image/gif,application/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml”
SSLEnabled=”true” scheme=”https” secure=”true”
clientAuth=”false” sslProtocol=”TLS” sslEnabledProtocols=”TLSv1” ciphers=”TLS_ECDHE_
RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_
256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_
RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_
SHA,SSL_RSA_WITH_RC4_128_SHA”
keystoreFile=”/opt/egurkha/manager/tomcat/conf/<filename>.
keystore”keystorePass=”<Keypass_set_for_certificate_request_generation>” />
```

Set the *port* parameter in the XML block to reflect the port number that you have configured for the eG manager. Also, note that two new parameters, namely - **keystoreFile** and **keystorePass** - have been inserted into the SSL block. While the **keystoreFile** parameter has to be set to the full path to the **.keystore** file that you generated earlier, the **keystorePass** parameter should be set to the keystore password that you specified while issuing the **keytool** command for generating a certificate request.

5. With that change, the eG manager on Linux has acquired the capability to listen on two ports - the SSL port and the non-SSL port. To configure the eG manager to listen only on the SSL port, simply comment that section of the **server.xml** file where the non-SSL Coyote HTTP connector on port 8081 has been defined, as indicated below:

```
<!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 8081 -->
<!--
<Connector protocol=”HTTP/1.1”
port=”7077” minSpareThreads=”64” maxThreads=”512”
enableLookups=”false” redirectPort=”8443”
acceptCount=”10” connectionTimeout=”20000”
useURIValidationHack=”false”  URIEncoding=”UTF-8” tcpNoDelay=”true” compression=”on”
compressionMinSize=”1024” noCompressionUserAgents=”gozilla, traviata”
compressableMimeType=”text/html,text/xml,text/plain,application/x-java-
applet,application/octet-
stream,application/xml,text/javascript,text/css,image/png,image/jpeg,
image/gif,application/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml” server=”eG Tomcat Server”/>
-->
```

6. Save the file.
7. Next, make sure that the eG manager URL configured against the **MailHomeURL** parameter in the **[MISC_ARGS]** section of the **eg_services.ini** file (in the **/opt/egurkha/manager/config** directory) begins with **https://** nstead of http://. Then, save the file.
8. Finally, start the eG manager.

Note:

Owing to SSL vulnerabilities that were discovered, many changes have been made in v6.1.2 to harden SSL communication with the eG manager. These include the following:

- Starting from version 6.1.2, TLS v1 will be the default secure protocol that web browsers will use to communicate with the eG manager.
- Recent versions of Firefox and Chrome expect a strong Cipher suite definition in SSL-enabled web/web application servers. HTTPS requests to web/web application servers that do not contain this Cipher Suite definition will be rejected by the Firefox and Chrome browsers. To avoid this, in version 6.1.2, this Cipher Suite definition has been bundled into the Tomcat server on which the eG manager runs.
- In the default SSL certificate that eG bundles with the eG manager, the message signing algorithm has been changed.

All these changes however, **will not be available to any SSL manager that is upgraded from a lower version to v6.1.2**. This is why, after a manager is upgraded to v6.1.2, you will experience problems communicating with the manager via HTTPS.

To avoid this, after an SSL-enabled manager is upgraded to version 6.1.2, you have to harden the SSL communication with the upgraded manager, following the steps detailed below:

- Edit the **server.xml** file in the <CATALINA_HOME>/conf directory (on Unix; on Windows, this will be the <CATALINA_HOME>/conf directory) on the eG manager host:
- Look for the SSL connector definition in the file.
- Locate the *sslProtocol* parameter in the definition.
- After the *sslprotocol* parameter, insert the following:

  ```
  sslEnabledProtocols=”TLSv1”
  ```

- Then, include the following Cipher Suite definition:

  ```
  ciphers=”TLS_ ECDHE_ RSA_ WITH_ AES_ 128_ CBC_ SHA256,TLS_ ECDHE_ RSA_ WITH_ AES_ 128_ CBC_
  SHA,TLS_ ECDHE_ RSA_ WITH_ AES_ 256_ CBC_ SHA384,TLS_ ECDHE_ RSA_ WITH_ AES_ 256_ CBC_ SHA,
  TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_
  CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA”
  ```

Note:

Owing to SSL vulnerabilities that were discovered, many changes have been made in v6.1.2 to harden SSL communication with the eG manager. These include the following:

- Starting from version 6.1.2, TLS v1 will be the default secure protocol that web browsers will use to communicate with the eG manager.
- Recent versions of Firefox and Chrome expect a strong Cipher suite definition in SSL-enabled web/web application servers. HTTPS requests to web/web application servers that do not contain this Cipher Suite definition will be rejected by the Firefox and Chrome browsers. To avoid this, in version 6.1.2, this Cipher Suite definition has been bundled into the Tomcat server on which the eG manager runs.
- In the default SSL certificate that eG bundles with the eG manager, the message signing algorithm has been changed.

All these changes however, **will not be available to any SSL manager that is upgraded from a lower version to v6.1.2**. This is why, after a manager is upgraded to v6.1.2, you will experience problems communicating with the manager via HTTPS.

To avoid this, after an SSL-enabled manager is upgraded to version 6.1.2, you have to harden the SSL communication with the upgraded manager, following the steps detailed below:

- Edit the **server.xml** file in the <CATALINA_HOME>/conf directory (on Unix; on Windows, this will be the <CATALINA_HOME>\conf directory) on the eG manager host:

- Look for the SSL connector definition in the file.
- Locate the *sslProtocol* parameter in the definition.
- After the *sslprotocol* parameter, insert the following:

```
sslEnabledProtocols=”TLSv1”
```

- Then, include the following Cipher Suite definition:

```
ciphers=”TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_
ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,   TLS_RSA_WITH_
AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_
RSA_WITH_AES_256_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA”
```

- Once the aforesaid changes are made, the SSL connector definition in your **server.xml** will look as shown below:

```
<Connector protocol=”HTTP/1.1”
port=”<eGManagerPort>” minSpareThreads=”64” maxThreads=”512”
enableLookups=”false” acceptCount=”10”  connectionTimeout=”20000”
useURIValidationHack=”false” URIEncoding=”UTF-8” tcpNoDelay=”true” compression=”on”
compressionMinSize=”1024” noCompressionUserAgents=”gozilla, traviata”
compressableMimeType=”text/html,text/xml,text/plain,application/x-java-
applet,application/octet-
stream,application/xml,text/javascript,text/css,image/png,image/
jpeg,image/gif,application/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml”
SSLEnabled=”true” scheme=”https” secure=”true”
clientAuth=”false” sslProtocol=”TLS” sslEnabledProtocols=”TLSv1”ciphers=”TLS_ECDHE_
RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_
256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,   TLS_RSA_WITH_AES_128_CBC_
SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_
256_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA”
keystoreFile=”<PathtoKeystoreFile>” keystorePass=”<Keystorepass>” server=”eG Tomcat
Server”/>
```

- Next, save the file.
- If you had SSL-enabled the eG manager using the default certificate that eG provides, then, once the above changes are made, copy the default certificate from the <EG_INSTALL_DIR>\bin\latest_certificate folder (on Windows; on Unix, this will be the /opt/egurkha/bin/latest_certificate folder), to the <EG_INSTALL_DIR>\manager/tomcat/webapps folder (on Windows; on Unix, this will be the /opt/egurkha/manager/tomcat/webapps folder).
- Finally, restart the eG manager.

2.8.1.3 SSL-Enabling the eG Manager Using a Signed Certificate Obtained from a Valid Certifying Authority

Self-signed certificates are useful in environments where ‘security’ is not a priority. In highly secure environments, especially where the eG manager is to be frequently accessed via the public internet, using a self-signed certificate may not be preferred. In such a case, you can you can obtain a valid certificate from a certificate authority and use that certificate to SSL-enable the eG manager.

The broad steps to be followed to achieve this are as follows:

- Generating the keystore file
- Generating a certificate request
- Submitting the certificate request to the Certificate Authority (CA) and obtaining a certificate
- Importing the certificate into a keystore
- Configuring Tomcat for using the keystore file

The sub-sections below elaborate on each of these steps.

2.8.1.3.1 Generating a Keystore File

The keystore file stores the details of the **certificates** necessary to make the protocol secure. Certificates contain the information pertaining to the source of the application data, and helps validate the source. To generate the keystore, use the **keytool** command. For this purpose, login to the Windows manager and go to the command prompt. Set the **JAVA_HOME** path if it is not done already. Then, execute the following commands, one after another:

cd $JAVA_HOME/bin

*keytool -genkey -alias **egitlab1** -keyalg **RSA** -keypass **mykey** -keystore **<Filename>**.keystore -storepass **mykey** -keysize **1024** -validity **1095***

The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

- **-alias** : an alias name for the certificate being generated
- **-keypass** : a password used to protect the key that is generated; **ensure that you provide the same values for -keypass and -storepass.**
- **-keyalg** : specifies the algorithm that is used to generate the keys. The options are as follows:

  - **DSA**: Digital Signature Algorithm
  - **RSA** : An algorithm used for public-key cryptography

- **-keystore** : the *keytool* command stores the generated key in a *.keystore* file; provide a name for this file as input to the **-keystore** command
- **-keysize** : the size of the key that is generated; the default key size is 1024 bits - the key size must be in the range 512 bits - 1024 bits
- **-validity** : indicates the number of days for which the key/certicate will be valid - 1095 days refer to 3 years.

The command, upon execution, will request the following inputs:

```
What is your first and last name?
[Unknown]: <Type the eG manager’s fully qualified domain name here>
What is the name of your organizational unit?
[Unknown]: United States
What is the name of your organization?
[Unknown]: eG Innovations Inc
What is the name of your City or Locality?
[Unknown]: Bridge Water
What is the name of your State or Province?
[Unknown]: New Jersey
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=eG Innovations Inc, OU=United States, O=eG Innovations Inc, L=Bridge Water, ST=New
Jersey, C=US correct?
[no]: yes
```

When requested for the **first and last name**, indicate the *fully qualified domain name* using which you will be accessing the eG manager. For instance, if the eG manager is to be accessed as http://egmanager.eginnovations.com, where *egmanager.eginnovation.com* is the fully qualified domain name of the eG manager, then specify *egmanager.eginnovations.com* here.

Once all the required inputs are provided, a .keystore file will be generated in the **<JAVA_HOME_DIR>\bin** directory with the **<Filename>** you had provided while issuing the command.

2.8.1.3.2 Generating a Certificate Request

Once a keystore file is generated, proceed to request for a certificate from a valid certifying authority. The procedure for this is as follows:

1. Login to the eG manager and go to the Windows command prompt.
2. Set the **JAVA_HOME** path if it is not done already.
3. Execute the following commands one after another:

   cd $JAVA_HOME/bin

   keytool -certreq -alias egitlab1 -keyalg RSA -file <Name_of_the_text_file> -keypass mykey -keystore <filename>.keystore –storepass mykey

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; **make sure that you provide the same alias name that you provided while generating the keystore file** (see Section **2.8.1.3.1**).
   - **-keyalg** : specifies the algorithm that was used to generate the keys; this can be **RSA** or **DSA**, depending upon **which algorithm was used for key generation in the procedure detailed in** Section **2.8.1.3.1**
   - **-file** : Provide a name for the text file to which the certificate request will be saved.
   - **-keypass** : the password used to protect the key that was generated; **make sure that you provide the same password that you provided while generating the keystore file (see** Section **2.8.1.3.1**). Also, note that **-storepass** and **-keypass** should be the same.
   - **-keystore** : Provide the name of the *keystore* file in which the key has been stored; **specify the same file name that you used to store the key** (see Section **2.8.1.3.1**).

4. If this command executes successfully, then a certificate request will be generated and automatically stored in the text file you specified in step 2 above.

2.8.1.3.3 Obtaining the Certificate from the CA

1. The first step towards obtaining a certificate is to submit the certificate request to the CA. For this connect to the Certificate server of the CA and submit the certificate. The procedure for request submission will differ from one CA to another.
2. The certificate will thus be generated. Download the certificate.

2.8.1.3.4 Importing the Certificates into the Keystore File

The downloaded certificate can be in one of the following forms:

- Can be a single, combined certificate
- Can be accompanied by a certificate chain
- Can be in a PEM format

The procedure for importing certificates differs based on the format of the downloaded certificate. These procedures have been detailed in the sub-sections below.

Importing a Combined Certificate into the Keystore File

In this case, follow the steps below to import the certificate into the keystore file:

1. Set the **JAVA_HOME** path if it is not done already.
2. Execute the following commands, one after another:

   cd $JAVA_HOME/bin

   keytool -import –trustcacerts -alias ***egitlab1*** *-file* ***<Name_of_the_domain_certificate>*** *-keystore* ***<Name_of_the_keystore_file>.keystore***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; **make sure that you provide the same alias name you provided when generating the keystore** (see Section **2.8.1.3.1**) .
   - **-file**: the name of the domain certificate that you want to import
   - **-keystore** : Provide the name of the *keystore* file you generated when you followed the procedure detailed in Section **2.8.1.3.1** above.

Importing a Signed Certificate and the Certificate Chain into the Keystore File

Digital certificates are verified using a chain of trust. The trust anchor for the digital certificate is the Root Certificate Authority (CA). The Certificate Hierarchy is a structure of certificates that allows individuals to verify the validity of a certificate's issuer. Certificates are issued and signed by certificates that reside higher in the certificate hierarchy, so the validity and trustworthiness of a given certificate is determined by the corresponding validity of the certificate that signed it.

The Chain of Trust of a Certificate Chain is an ordered list of certificates, containing an end-user subscriber certificate and intermediate certificates (that represents the Intermediate CA), that enables the receiver to verify that the sender and all intermediate certificates are trustworthy.

A certificate chain will therefore consist of multiple certificates. Before importing each of these certificates, **you will have to understand the hierarchy of the certificates**. To know which is the root and which is the intermediate certificate, refer to the web site of the certificate authority. For instance, if Comodo is the Certificate Authority that has issued the SSL certificate, then connect to the following URL, *https://support.comodo.com/index.php?/Default/Knowledgebase/Article/View/620/1/* , to gain clarity.

Then, follow the steps below:

1. Set the **JAVA_HOME** path if it is not done already.
2. Then, import the Root certificate. For this, execute the following commands, one after another in the command prompt:

   cd $JAVA_HOME/bin

   keytool -import –trustcacerts -alias ***rootcert*** *-file* ***<Name_of_the_root_certificate>*** *-keystore* ***<Name_of_the_keystore_file>.keystore*** *–keypass* ***mykey*** *–storepass* ***mykey***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; **make sure that you provide a unique alias name for the root certificate.**
   - **-file**: the name of the root certificate that you want to import
   - **-keystore** : Provide the name of the *keystore* file you generated when you followed the procedure detailed in Section **2.8.1.3.1** above.
   - **-keypass** and **–storepass** : Provide the same **keypass** and **storepass** that you specified when generating the keystore; refer to Section **2.8.1.3.1** above for details.

3. Next, import each of the intermediate certificates, one after another, using the following command:

   keytool -import –trustcacerts -alias ***intercert1*** *-file* ***<Name_of_the_intermediate_certificate>*** *-keystore* ***<Name_of_the_keystore_file>.keystore*** *–keypass* ***mykey*** *–storepass* ***mykey***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

- **-alias** : the alias name of the certificate being requested; **make sure that you provide a unique alias name for every intermediate certificate.**
- **-file**: the name of the intermediate certificate that you want to import
- **-keystore** : Provide the name of the *keystore* file you generated when you followed the procedure detailed in Section **2.8.1.3.1** above.
- **-keypass** and **–storepass** : Provide the same **keypass** and **storepass** that you specified when generating the keystore; refer to Section **2.8.1.3.1** above for details.

4. Finally, import the entity/domain certificate into the keystore by issuing the following command:

   keytool -import –trustcacerts -alias ***egitlab1*** *-file* ***<Name_of_the_domain_certificate>*** *-keystore* ***<Name_of_the_keystore_file>.keystore***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being requested; **make sure that you provide the same alias name you provided when generating the keystore** (see Section **2.8.1.3.1**) .
   - **-file**: the name of the domain certificate that you want to import
   - **-keystore** : Provide the name of the *keystore* file you generated when you followed the procedure detailed in Section **2.8.1.3.1** above.

   Note:

   If the domain certificate import command throws an error for any reason, it could be because, all related certificates may not have been imported. Check the web site of the CA for more details.

Importing a Certificate that is in the PEM Format

PEM is a container format that may include just the public certificate (such as with Apache installs, and CA certificate files */etc/ssl/certs*), or may include an entire certificate chain including public key, private key, and root certificates, or may only contain a certificate and a private key.

If the certificate you downloaded is in the PEM format and includes only a certificate file and a private key file, then follow the steps below to import that certificate into a keystore file.

1. Run the following command from the command prompt to export the certificate and private key file into the pkcs12 format:

*openssl pkcs12 -export -in **certificate.crt** -inkey **private.key** -certfile **certificate.crt** -name “**My certificate**” -out **keystore**.p12*

The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

- **-in** : the name of the certificate that is included in the PEM container
- **-inkey**: the name of the private key file the PEM container consists of
- **-certfile** : the name of the certificate that is included in the PEM container
- **-name** : Provide a **unique name for the certificate file** that is being exported.
- **-out** : Specify the name of the keystore file to which the certificate and private key are to be exported. **The keystore file can have any name of your choice.**

2. Next, you need to convert the keystore file, which is currently in the pkcs12 format, into the Java keystore (i.e., JKS) format. For this, issue the following command at the command prompt:

*keytool -importkeystore –alias **egitlab1** -deststorepass **mykey** -destkeypass **mykey** -destkeystore **keystore,jks** -srckeystore **keystore.pk12** -srcstoretype PKCS12 -srcstorepass **mykey***

The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

- **-alias** : the aliasname of the certificate being requested; **make sure that you provide the same alias name that you specified in** Section **2.8.1.3.1**.
- **-deststorepass** : this refers to the **storepass** of the destination keystore file – i.e., the keystore file in the JKS format. The storepass of the destination keystore should be the same as the storepass of the source keystore.
- **-destkeypass** : this refers to the **keypass** of the destination keystore file - i.e., the keystore file in the JKS format. **The storepass and keypass of the destination keystore file should be the same.**
- **-destkeystore**: the name of the destination keystore file – i.e., the keystore file in the JKS format.
- **-srckeystore** : the name of the destination keystore file – i.e., the keystore file in the PKCS12 format.
- **-srcstorepass** : The **storepass** of the source keystore file – i.e., the keystore file in the PKCS12 format. Make sure that you provide the same storepass you specified in Section **2.8.1.3.1**.

2.8.1.3.5 Configuring Tomcat for Using the Keystore File

The eG manager on Unix uses Tomcat 6.0 as the web server. Therefore, to SSL-enable the eG manager, you need to configure the **server.xml** file of Tomcat with the name and full path to the keystore file which was created earlier.

For this purpose, do the following:

1. Stop the eG manager.
2. Edit the **server.xml** file in the <CATALINA_HOME>/conf directory.
3. In the file, search for the XML block where the SSL Coyote HTTP connector on port 8443 is defined. If this block is commented, it indicates that the eG manager is not SSL-enabled and is hence listening on an HTTP port only. To SSL-enable the eG manager, first uncomment this block as indicated below:

```
<Connector protocol=”HTTP/1.1”
port=”8443” minSpareThreads=”64” maxThreads=”512”
enableLookups=”false” acceptCount=”10”  connectionTimeout=”20000”
useURIValidationHack=”false” URIEncoding=”UTF-8” tcpNoDelay=”true” compression=”on”
compressionMinSize=”1024” noCompressionUserAgents=”gozilla, traviata”
compressableMimeType=”text/html,text/xml,text/plain,application/x-java-
applet,application/octet-
stream,application/xml,text/javascript,text/css,image/png,image/jpeg,
image/gif,application/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml”
SSLEnabled=”true” scheme=”https” secure=”true”
clientAuth=”false” sslProtocol=”TLS” sslEnabledProtocols=”TLSv1” ciphers=”TLS_ECDHE_
RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_
256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_
RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_
SHA,SSL_RSA_WITH_RC4_128_SHA” />
```

4. Then, proceed to make the changes indicated in **Bold** below in the SSL XML block:

```
<Connector protocol=”HTTP/1.1”
port=”<eG_Manager_Port>” minSpareThreads=”64” maxThreads=”512”
enableLookups=”false” acceptCount=”10”  connectionTimeout=”20000”
useURIValidationHack=”false” URIEncoding=”UTF-8” tcpNoDelay=”true” compression=”on”
compressionMinSize=”1024” noCompressionUserAgents=”gozilla, traviata”
compressableMimeType=”text/html,text/xml,text/plain,application/x-java-
applet,application/octet-
stream,application/xml,text/javascript,text/css,image/png,image/jpeg,
image/gif,application/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml”
SSLEnabled=”true” scheme=”https” secure=”true”
clientAuth=”false” sslProtocol=”TLS” sslEnabledProtocols=”TLSv1” ciphers=”TLS_ECDHE_
RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_
256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_
RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_
SHA,SSL_RSA_WITH_RC4_128_SHA”
keystoreFile=”/opt/egurkha/manager/tomcat/conf/<filename>.keystore”
keystorePass=”<Keypass_set_for_certificate_request_generation>” />
```

Set the *port* parameter in the XML block to reflect the port number that you have configured for the eG manager. Also, note that two new parameters, namely - **keystoreFile** and **keystorePass** - have been inserted into the SSL block. While the **keystoreFile** parameter has to be set to the full path to the **.keystore** file that you generated earlier, the **keystorePass** parameter should be set to the keystore password that you specified while issuing the **keytool** command for generating a certificate request.

5. With that change, the eG manager on Linux has acquired the capability to listen on two ports - the SSL port and the non-SSL port. To configure the eG manager to listen only on the SSL port, simply comment that section of the **server.xml** file where the non-SSL Coyote HTTP connector on port 8081 has been defined, as indicated below:

```
<!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 8081 -->
<!--
<Connector protocol=”HTTP/1.1”
port=”7077” minSpareThreads=”64” maxThreads=”512”
enableLookups=”false” redirectPort=”8443”
acceptCount=”10” connectionTimeout=”20000”
useURIValidationHack=”false”  URIEncoding=”UTF-8” tcpNoDelay=”true” compression=”on”
compressionMinSize=”1024” noCompressionUserAgents=”gozilla, traviata”
compressableMimeType=”text/html,text/xml,text/plain,application/x-java-
applet,application/octet-
stream,application/xml,text/javascript,text/css,image/png,image/jpeg,
image/gif,application/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml” server=”eG Tomcat Server”/>
-->
```

6. Save the file.

7. Next, make sure that the eG manager URL configured against the **MailHomeURL** parameter in the **[MISC_ARGS]** section of the **eg_services.ini** file (in the **/opt/egurkha/manager/config** directory) begins with **https://** nstead of **http://**. Then, save the file.

8. Finally, start the eG manager.

Note:

Owing to SSL vulnerabilities that were discovered, many changes have been made in v6.1.2 to harden SSL communication with the eG manager. These include the following:

- Starting from version 6.1.2, TLS v1 will be the default secure protocol that web browsers will use to communicate with the eG manager.
- Recent versions of Firefox and Chrome expect a strong Cipher suite definition in SSL-enabled web/web application servers. HTTPS requests to web/web application servers that do not contain this Cipher Suite definition will be rejected by the Firefox and Chrome browsers. To avoid this, in version 6.1.2, this Cipher Suite definition has been bundled into the Tomcat server on which the eG manager runs.
- In the default SSL certificate that eG bundles with the eG manager, the message signing algorithm has been changed.

All these changes however, **will not be available to any SSL manager that is upgraded from a lower version to v6.1.2**. This is why, after a manager is upgraded to v6.1.2, you will experience problems communicating with the manager via HTTPS.

To avoid this, after an SSL-enabled manager is upgraded to version 6.1.2, you have to harden the SSL communication with the upgraded manager, following the steps detailed below:

- Edit the **server.xml** file in the <CATALINA_HOME>/conf directory (on Unix; on Windows, this will be the <CATALINA_HOME>/conf directory) on the eG manager host:
- Look for the SSL connector definition in the file.
- Locate the *sslProtocol* parameter in the definition.
- After the *sslprotocol* parameter, insert the following:

  ```
  sslEnabledProtocols=”TLSv1”
  ```

- Then, include the following Cipher Suite definition:

  ```
  ciphers=”TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_
  128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_
  256_CBC_SHA,   TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_
  SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,SSL_RSA_WITH_RC4_128_
  SHA”
  ```

- Once the aforesaid changes are made, the SSL connector definition in your **server.xml** will look as shown below:

  ```
  <Connector protocol=”HTTP/1.1”
  port=”<eGManagerPort>” minSpareThreads=”64” maxThreads=”512”
  enableLookups=”false” acceptCount=”10”  connectionTimeout=”20000”
  useURIValidationHack=”false” URIEncoding=”UTF-8” tcpNoDelay=”true” compression=”on”
  compressionMinSize=”1024” noCompressionUserAgents=”gozilla, traviata”
  compressableMimeType=”text/html,text/xml,text/plain,application/x-java-
  applet,application/octet-
  stream,application/xml,text/javascript,text/css,image/png,image/jpeg,
  image/gif,application/pdf,application/x-
  javascript,application/javascript,application/json,application/x-shockwave-
  flash,application/xhtml+xml,application/xml+xhtml”
  SSLEnabled=”true” scheme=”https” secure=”true”
  clientAuth=”false” sslProtocol=”TLS” sslEnabledProtocols=”TLSv1”ciphers=”TLS_ECDHE_
  RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_
  256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,   TLS_RSA_WITH_AES_128_CBC_
  SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_
  256_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA”
  keystoreFile=”<PathtoKeystoreFile>” keystorePass=”<Keystorepass>” server=”eG Tomcat
  Server”/>
  ```

- Next, save the file.

- If you had SSL-enabled the eG manager using the default certificate that eG provides, then, once the above changes are made, copy the default certificate from the <EG_ INSTALL_ DIR>\bin\latest_certificate folder (on Windows; on Unix, this will be the /opt/egurkha/bin/latest_ certificate folder), to the <EG_INSTALL_DIR>\manager/tomcat/webapps folder (on Windows; on Unix, this will be the /opt/egurkha/manager/tomcat/webapps folder).
- Finally, restart the eG manager.

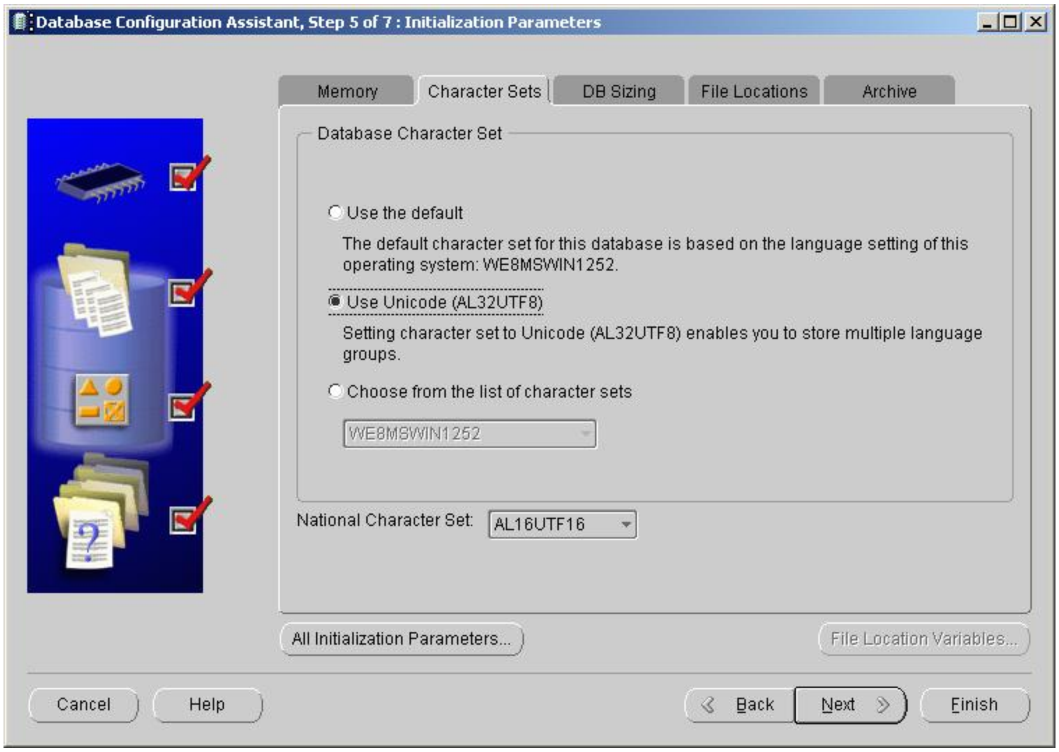
2.9 Configuring Double-byte Support for eG Enterprise

eG Enterprise embeds the ability to store and display data in any language that the user wants. Each user connecting to an eG manager can thus view data in a language that he/she prefers.

While eG Enterprise can support all European languages with minimal configuration, some additional configurations need to be carried out to make sure that the suite supports Chinese, Korean, or Japanese. This is because, unlike their peers, these three languages support a **double-byte character set**. The steps below discuss these special configurations elaborately:

1. The first step towards ensuring that eG Enterprise handles Chinese, Korean, or Japanese characters is to **double-byte enable the eG manager**. This can be performed during manager setup itself. When the setup process prompts you enable/disable double-byte support, press **y** (in the case of a Unix manager)) or click the **OK** button (in the case of a Windows manager) to enable double-byte support.
2. Secondly, you need to configure the eG database to store and process double-byte characters. If an MS SQL server is used as the eG backend, then no additional configuration is necessary to enable double-byte support. However, if an Oracle database is used as the eG backend, then you will have to explicitly change the NLS settings of the Oracle server, so that the database server is able to store double- byte characters. For that, while creating an Oracle database instance, do the following:

   - Click on the **Character Sets** tab
   - Select the **Use Unicode (AL32UTF8)** option
   - Select **AL16UTF16** as the **National Character Set**
   - If a **Database Configuration Assistant** is used to configure the Oracle instance, then the aforesaid parameters can be set as depicted by Figure 4.1 below.


Database Configuration Assistant, Step 5 of 7 : Initialization Parameters
Memory
Character Sets
DB Sizing
File Locations
Archive
All Initialization Parameters...
File Location Variables...
Cancel
Help
Back
Next
Finish

Database Character Set

○ Use the default

The default character set for this database is based on the language setting of this operating system: WE8MSWIN1252.

● Use Unicode (AL32UTF8)

Setting character set to Unicode (AL32UTF8) enables you to store multiple language groups.

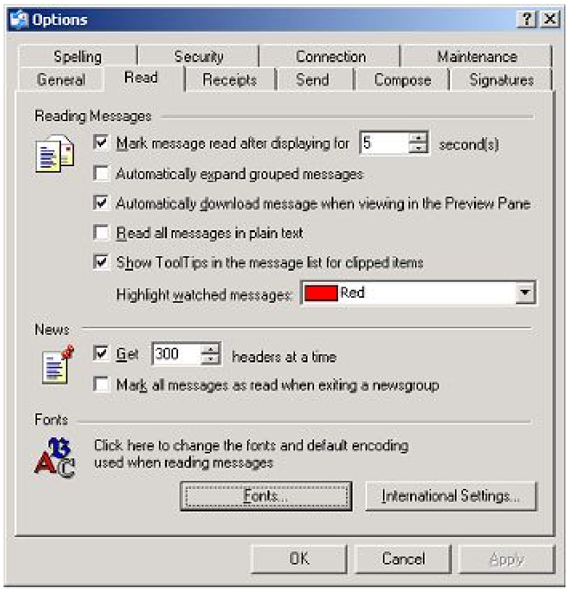
○ Choose from the list of character sets

WE8MSWIN1252

National Character Set: AL16UTF16

Figure 2.122: Configuring the Oracle database instance to support double-byte

- Next, ensure that you add multi-language support to the browser host (i.e., the host from which you will be connecting to the eG manager), and the eG manager host.
- Next, the font and Unicode settings for your mail client should be configured, so that eG alerts received by the client display double-byte characters. For instance, to ensure that your **Outlook Express** client supports double-byte characters, do the following:
- First, open the Outlook Express client, and follow the menu sequence: Tools -> Options.
- Click on the **Read** tab page in the **Option** dialog box that opens, and then click on the **Fonts** button in the **Read** tab.



Reading Messages

☑ Mark message read after displaying for 5 second(s)

☐ Automatically expand grouped messages

☑ Automatically download message when viewing in the Preview Pane

☐ Read all messages in plain text

☑ Show ToolTips in the message list for clipped items

Highlight watched messages: 🟥 Red

News

☑ Get 300 headers at a time

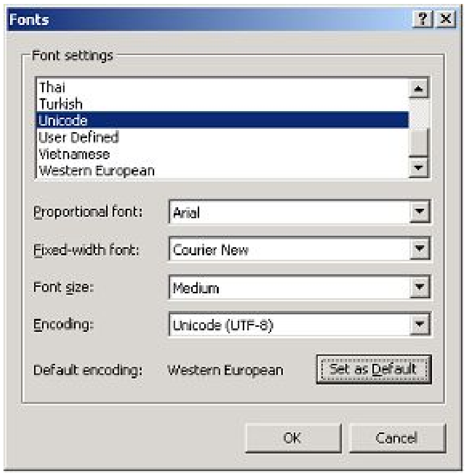
☐ Mark all messages as read when exiting a newsgroup

Fonts

Click here to change the fonts and default encoding used when reading messages

Figure 2.123: Clicking on the Fonts button

- In the Fonts dialog box, select **Unicode** from the **Font Settings** list, select any Universal font from the **Proportional font** list, and choose the **Unicode (UTF-8)** option from the **Encoding** list. Finally, click the **OK** button to save the changes.



Font settings

Thai
Turkish
Unicode
User Defined
Vietnamese
Western European

Proportional font: Arial

Fixed-width font: Courier New

Font size: Medium

Encoding: Unicode (UTF-8)

Default encoding: Western European

Figure 2.124: Defining font settings

3. To display double-byte data, eG Enterprise requires *Universal fonts*. The preferred Universal fonts are:

- **ArialUniCodeMS** - Sutiable for Chinese,Korean,Spanish,german, Japanese,French, Porthugese,German,spanish,Russian

- **Code2000** - Sutiable for French,Porthugese,German,spanish,Russian
- **evermono** - Suitable for Chinese, Korean, Spanish, German, Japanese, French, Portugese,German, Spanish, Russian
- **Cyberbit** - Suitable for Chinese, Korean, Spanish, German, Japanese, Spanish,Russian

Ensure that the *Universal font* file that corresponds to your language preference is downloaded to the eG manager host and copied to the <EG_INSTALL_DIR>\manager\fonts folder.

Note:

While copying the font files to the above-mentioned directory, ensure that the font file extensions are in upper-case - in other words, copy the font files as **.ttf** and not **.\ boldttf**.

4. Also, to ensure that multi-byte support is extended to the eG reports that are saved as PDF documents, do the following:

- Edit the file <EGURKHA_INSTALL_DIR>\manager\fonts\pd4fonts.properties file.
- By default, the path to the multi-byte font file that is bundled with the eG manager will be displayed against the following entries in the **pd4fonts.properties** file:

```
LucidaGrandeRegular=../tomcat/webapps/final/fonts/6216/6216.TTF
```

```
LucidaGradeBold=../tomcat/webapps/final/fonts/6215/6215.TTF
```

```
LucidaGrandeRegular\ bold=../tomcat/webapps/final/fonts/6216/6216.TTF
LucidaGrandeBold\ bold=../tomcat/webapps/final/fonts/6215/6215.TTF
```

- Replace the path configuration against each of the aforesaid entires with the exact name of the font file (with extension) that you downloaded and copied to the <EG_ INSTALL_ DIR>\manager\fonts directory at step 3 above. For example, if you had copied the **Code2000.TTF** file to the <EG_INSTALL_DIR>\manager\fonts directory previously, then specify **Code2000.TTF** against each of the above- mentioned entries in the **pd4fonts.properties** file, as depicted below:

```
LucideGrandeRegular=Code2000.TTF
```

```
LucideGradeBold=Code2000.TTF
```

```
LuncidaGrandeRegular\ bold=Code2000.TTF
```

```
LucidaGrandeBold\ bold=Code2000.TTF
```

- Then, save the file.
- Finally, restart the eG manager.

Note:

If your eG manager is double-byte enabled, but the **Language** preference that you have set in the **USER PROFILE** page is **English**, then, you do not have to follow the steps discussed above to ensure that reports are saved as PDF documents. However, while using a double-byte enabled eG manager, if you have chosen to view data in a **Language** other than **English**, then reports cannot be saved as PDF documents until the above-mentioned steps are followed.

2.10 Troubleshooting the eG Manager

The following sections deal with the queries that may arise while installing and configuring eG manager.

- Section **2.10.1**
- Section **2.10.2**
- Section **2.10.3**
- Section **2.10.4**
- Section **2.11**

2.10.1 Installing the eG Manager

1. **The eG manager installation does not even start. What could be wrong?**

   Please check for the following:

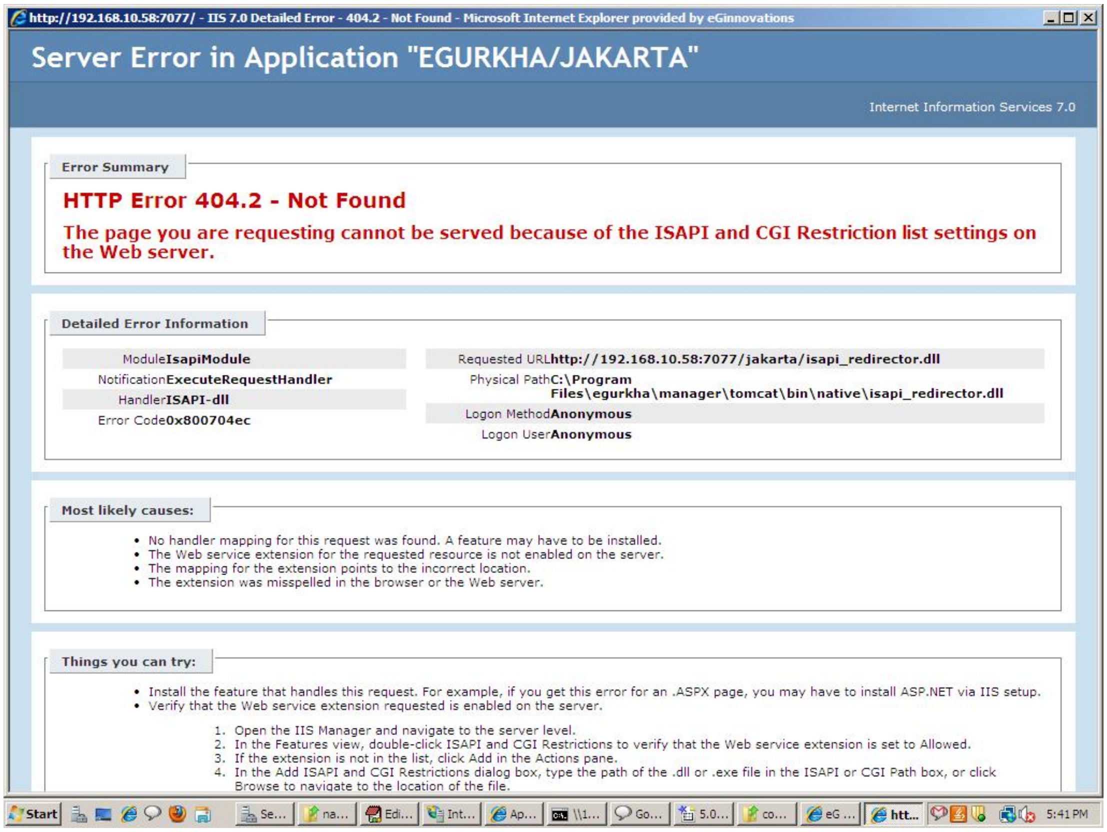
   - Did you accept the license agreement?
   - Check if you possess the administrative privileges on Windows.
   - Do you have the pre-requisites for
     - An operating system version that eG supports
     - The right service pack and option pack (for Windows environments)

2. **The eG manager installation failed. What could be wrong?**

   - Verify that if the eG manager and agent are being installed on the same system, the same user owns the eG directories.
   - Make sure that the operating system locale setting is English.

3. **I installed the eG manager on a Windows 2008 server, but I could not start the**

manager. To troubleshoot the failure, I opened the IIS Manager console, browsed the tree in the left pane to locate the 'egurkha' website, and tried to connect to the web site. Once I did that, the following error message appeared.


http://192.168.10.58:7077/ - IIS 7.0 Detailed Error - 404.2 - Not Found - Microsoft Internet Explorer provided by eGinnovations
Start
Se...
na...
Edi...
Int...
Ap...
\\1...
Go...
5.0...
co...
eG ...
htt...
5:41 PM

Server Error in Application "EGURKHA/JAKARTA"

Internet Information Services 7.0

Error Summary

HTTP Error 404.2 - Not Found

The page you are requesting cannot be served because of the ISAPI and CGI Restriction list settings on the Web server.

Detailed Error Information

Module **IsapiModule**
Notification **ExecuteRequestHandler**
Handler **ISAPI-dll**
Error Code **0x800704ec**
Requested URL **http://192.168.10.58:7077/jakarta/isapi_redirector.dll**
Physical Path **C:\Program Files\egurkha\manager\tomcat\bin\native\isapi_redirector.dll**
Logon Method **Anonymous**
Logon User **Anonymous**

Most likely causes:

- No handler mapping for this request was found. A feature may have to be installed.
- The Web service extension for the requested resource is not enabled on the server.
- The mapping for the extension points to the incorrect location.
- The extension was misspelled in the browser or the Web server.

Things you can try:

- Install the feature that handles this request. For example, if you get this error for an .ASPX page, you may have to install ASP.NET via IIS setup.
- Verify that the Web service extension requested is enabled on the server.
  1. Open the IIS Manager and navigate to the server level.
  2. In the Features view, double-click ISAPI and CGI Restrictions to verify that the Web service extension is set to Allowed.
  3. If the extension is not in the list, click Add in the Actions pane.
  4. In the Add ISAPI and CGI Restrictions dialog box, type the path of the .dll or .exe file in the ISAPI or CGI Path box, or click Browse to navigate to the location of the file.

Figure 2.125: The error message that appeared when the 'egurkha' web site listing in the IIS 2008 manager console was clicked

4. **Why did this happen? What do I do to resolve this?**

This error typically appears if **IIS** and **CGI** restrictions have been imposed on the **egurkha** web site, preventing its execution on the web server. If you receive such an error message, then, do the following to resolve the issue:

- Login to the Windows 2008 server.
- Open the **Internet Information Services (IIS) Manager** console on the server.
- Once the console opens, click on the node representing the IIS web server in the tree-structure in the left pane of the console (see Figure 2.126).

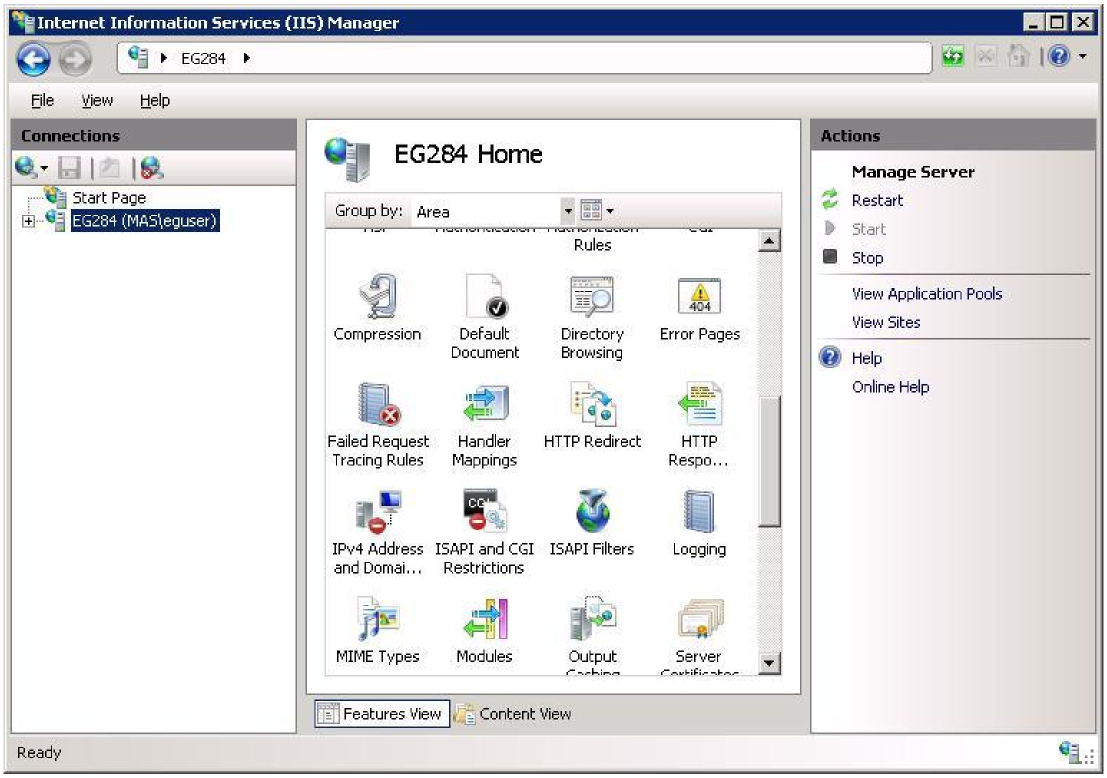
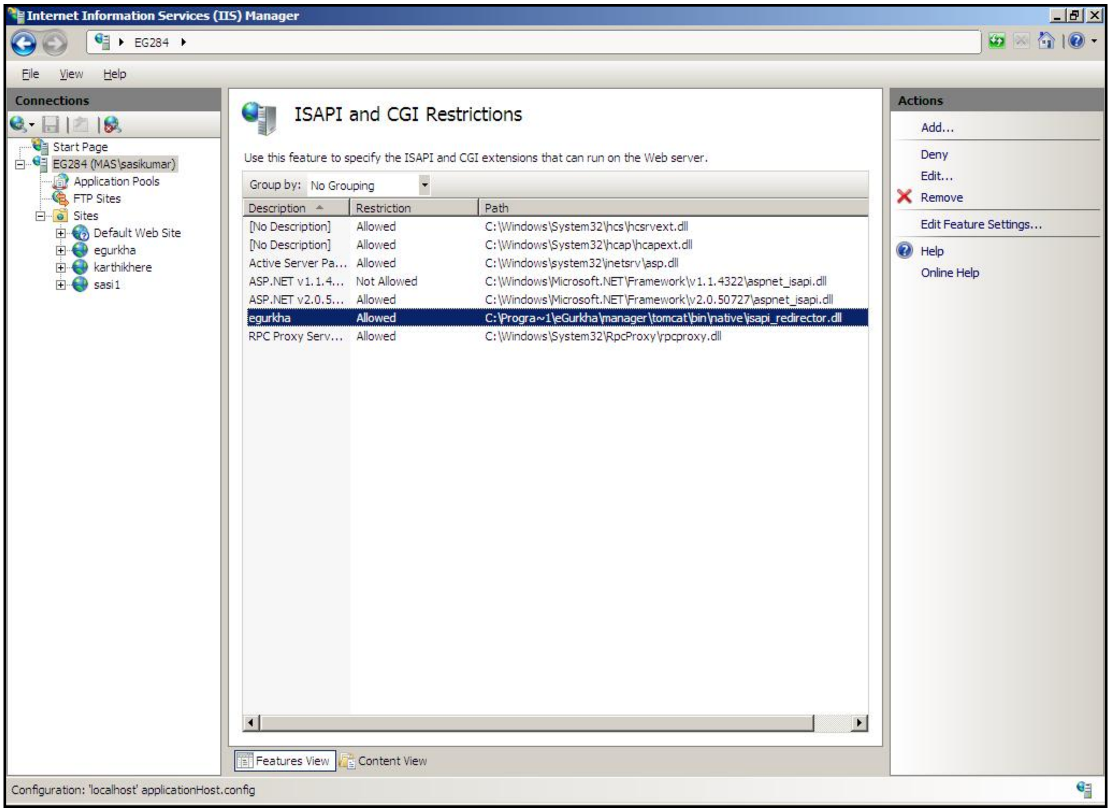


Figure 2.126: Clicking on the node representing the IIS web server in the left pane of the console

- The right pane will then change to display a variety of properties that can be defined for the IIS web server. Browse the list to locate the **ISAPI** and **CGI Restrictions** property, and click on it. Figure 2.127 will then appear listing the ISAPI and CGI extensions that can run on the web server. Look for **egurkha** in the list, and when found, check to see whether it is set to **Allowed**. If not, click on the **Edit Feature Settings** button indicated by Figure 2.127.



ISAPI and CGI Restrictions

Use this feature to specify the ISAPI and CGI extensions that can run on the Web server.

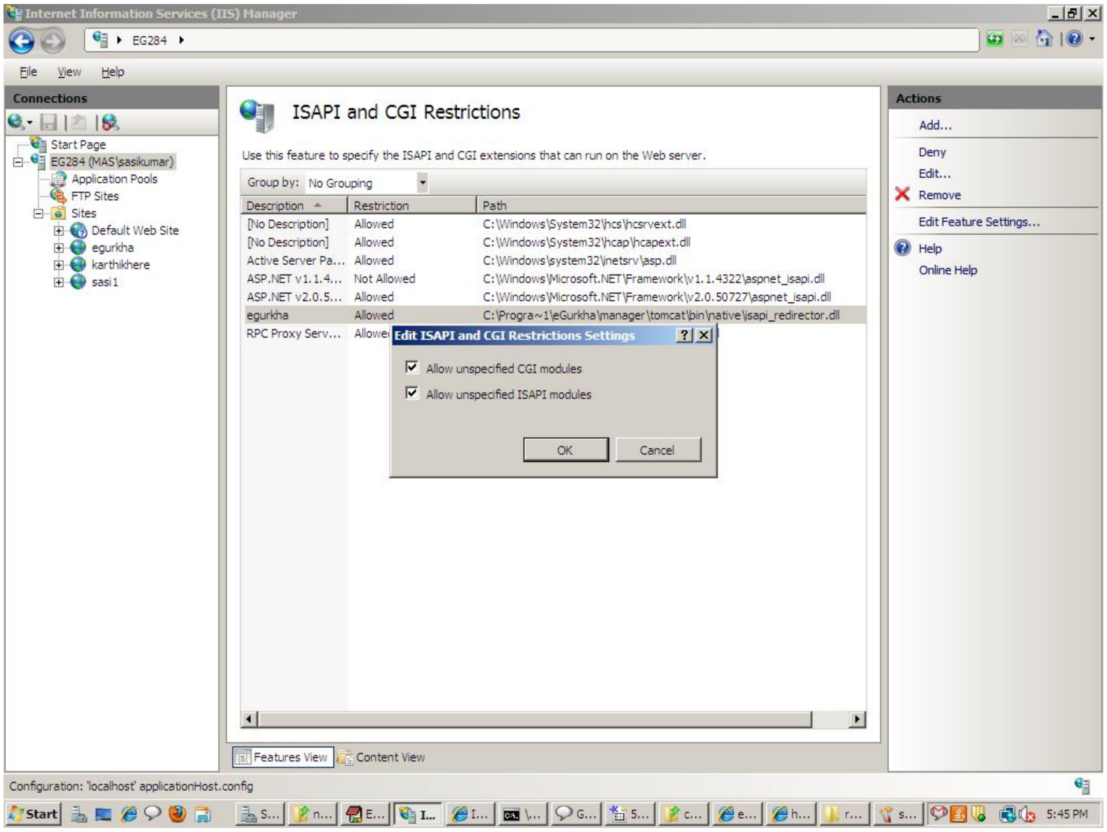
Group by: No Grouping

Description	Restriction	Path
[No Description]	Allowed	C:\Windows\System32\hcs\hcsrvext.dll
[No Description]	Allowed	C:\Windows\System32\hcap\hcapext.dll
Active Server Pa...	Allowed	C:\Windows\system32\inetsrv\asp.dll
ASP.NET v1.1.4...	Not Allowed	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
ASP.NET v2.0.5...	Allowed	C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll
egurkha	Allowed	C:\Progra~1\eGurkha\manager\tomcat\bin\native\isapi_redirector.dll
RPC Proxy Serv...	Allowed	C:\Windows\System32\RpcProxy\rpcproxy.dll

Configuration: 'localhost' applicationHost.config

Figure 2.127: Checking whether the ‘egurkha’ extension is Allowed to run on the web server

- Clicking on the button indicated by Figure 8.3 will invoke Figure 8.4. To lift the ISAPI and CGI restrictions off the **egurkha** extension, select the **Allow unspecified CGI modules** check box and the **Allow unspecified ISAPI modules** check box in Figure 8.4, and click the **OK** button. You will then find that the **egurkha** listing in the **ISAPI** and CGI Restrictions window is set to **Allowed**.



ISAPI and CGI Restrictions

Use this feature to specify the ISAPI and CGI extensions that can run on the Web server.

Group by: No Grouping

Description	Restriction	Path
[No Description]	Allowed	C:\Windows\System32\hcs\hcsrvext.dll
[No Description]	Allowed	C:\Windows\System32\hcap\hcapext.dll
Active Server Pa...	Allowed	C:\Windows\system32\inetsrv\asp.dll
ASP.NET v1.1.4...	Not Allowed	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
ASP.NET v2.0.5...	Allowed	C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll
egurkha	Allowed	C:\Progra~1\eGurkha\manager\tomcat\bin\native\isapi_redirector.dll
RPC Proxy Serv...	Allowe	

Edit ISAPI and CGI Restrictions Settings

☑ Allow unspecified CGI modules

☑ Allow unspecified ISAPI modules

OK Cancel

Figure 2.128: Lifting the ISAPI and CGI restrictions from the egurkha extension

2.10.2 Configuring the eG Manager

1. **The eG manager configuration failed. What could have contributed to this?**

   - Make sure that the database instance you specified is valid. Connect from the “sqlplus” prompt using the database administrator user name and password to make sure that the database instance is up.

   - Make sure that the database instance can be reached from the eG manager system (e.g., firewalls between the manager and the database could result in database connection problems)

   - Check that the tablespaces specified when creating a new user are valid.

   - Ensure that the tablespaces specified have enough space to host the eG database tables.

2. **I have the eG manager working. Now, I have shifted my database to another server.**

Can I reconfigure the manager to work with the new database?

Information regarding the eG manager's database connection is maintained in the file <EG_HOME_DIR>/manager/config/eg_db.ini. By editing this file, you can modify the database that the eG manager will use.

3. **My eG manager is using an Oracle backend. Lately, my manager is experiencing a lot of connection issues. When I checked the manager tomcat debug file, I found the following error message: "java.sql.SQLException: OALL8 is in an inconsistent state". What is the reason for this error, and how do I resolve the connection issues that have surfaced as a result?**

   This error message appears when there is a JDBC driver mismatch - i.e., when the JDBC driver bundled with the eG manager is not compatible with the JDBC driver of the Oracle database that is in use in the monitored environment.

   To resolve this issue, do the following:

   - Take a backup of the JDBC driver that is bundled with the eG manager, from the <EG_INSTALL_DIR>\lib folder.
   - Download the latest release of the JDBC driver that is compatible with the version of the Oracle database server that is in use in your environment, using the link: http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/index.html
   - Rename the downloaded driver as **classes12.zip** in case of Windows, or as **classes11.zip** in case of the Unix manager.
   - Copy the renamed file to the <EG_INSTALL_DIR>\lib directory (in case of the Windows manager), or the **/opt/egurkha/lib** directory in case of the Unix manager.
   - Restart the eG manager.

4. **How do I change the eG manager's port?**

   - Stop the eG manager.
   - Look for the script **start_manager.bat** in the **<EG_HOME_DIR>\lib** directory, and modify the port there, but do not run the script.
   - Next, proceed to change the **egurkha** web site's port. To do so, first, go into the Windows Internet Service Manager (Start -> Programs -> Administrative Tools -> Internet Information Services (IIS) Manager).

- In the **Internet Information Services** window that appears, right-click on the manager host and select **Properties** from the shortcut menu.
- From the **Master Properties** list box therein, select the **egurkha** web site and then, click the **Edit** button alongside it to edit its properties.
- Upon clicking, a **WWW Service Master Properties** dialog box will appear. The **Web Site** tab of the dialog box will open, by default. Change the **TCP Port** entry in that tab, so as to make the eG manager listen to the new port.
- Similarly, you need to reconfigure all agents (manually) to talk to the manager using the new port. You can do this by editing the **debugoff** script (Windows) in the <EG_HOME_DIR>\lib directory, or **start_agent** script file (UNIX) in the same directory.
- Search for port 7077 and replace it with your port number. Save the file and run the script file. Restart the agent and check if it is talking to the new port.

2.10.3 Starting the eG Manager

1. **The eG installation went through fine, but I am not able to start the manager. What could be wrong?**

   - Check to make sure that you have a valid license. The license must be stored in a file named <EG_HOME_DIR>/bin/license.
   - Run the command "**viewCert license**" from the "<EG_HOME_DIR>/bin to make sure that your license has not expired.
   - Make sure that the eG user has permissions to read and write from all the eG directories.
   - When installing the eG manager, you will be asked to enter an IP address or hostname for the host on which the manager is being installed. Make sure that this IP address or hostname (what you specified during the installation) is accessible over the network. E.g., if you specified a hostname and the DNS service is not configured to resolve this hostname, the eG manager will not start.
   - Please make sure that you are logged in as the eG user. Other users will not be allowed to start the eG manager.
   - If an eG manager was previously installed, ensure that this manager was stopped and uninstalled before the new manager is installed and started.

2. **The eG manager used to work. Suddenly, it has stopped working. What could be**

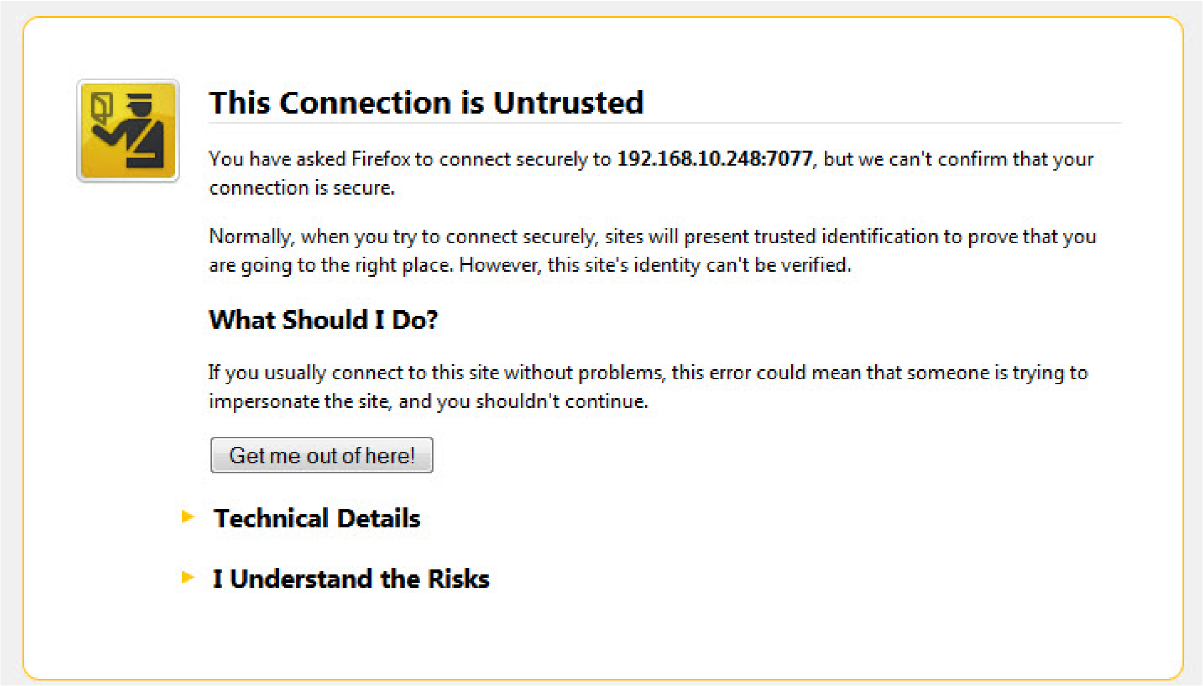
wrong?

- First, check for expiry of the eG license. Run the command “**viewCert license**” from the “<EG_HOME_DIR>/bin to make sure that your license has not expired. If the license has expired, the eG manager will not start.
- If the IP address or hostname of the database server has changed, the eG manager will not start properly. Reconfigure the eG database setting by editing the file <EG_HOME_DIR>/manager/config/eg_db.ini.

2.10.4 SSL-Enabling the eG Manager

How to differentiate between a public and private certificate?

A private certificate is often a self-signed certificate that is not validated by any certifying authority. This is why, when connecting to an eG manager that has been SSL-enabled using a self-signed certificate, the following error message appears:



This Connection is Untrusted

You have asked Firefox to connect securely to **192.168.10.248:7077**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Figure 2.129: The error message that appears when connecting to an eG manager using a self-signed SSL certificate

A public certificate on the other hand is a trusted certificate issued by a valid Certificate Authority. If such a certificate is used to SSL-enable an eG manager, then, a ‘lock’ symbol will appear in the address bar of the browser when attempting to connect to that manager (see Figure 2.130).

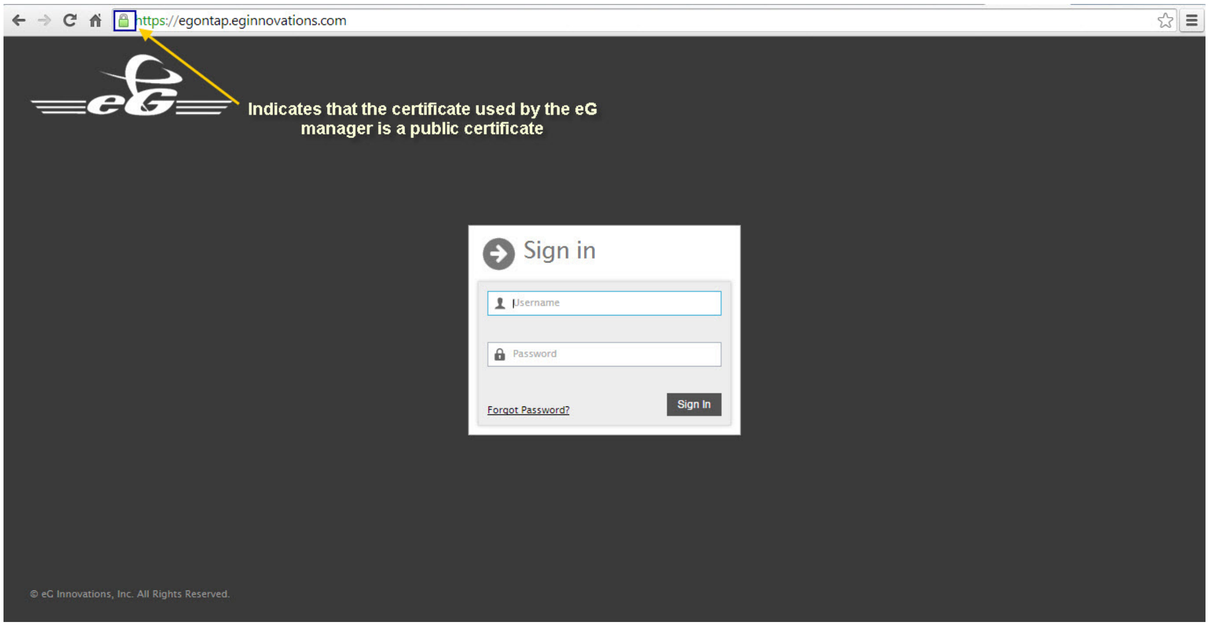
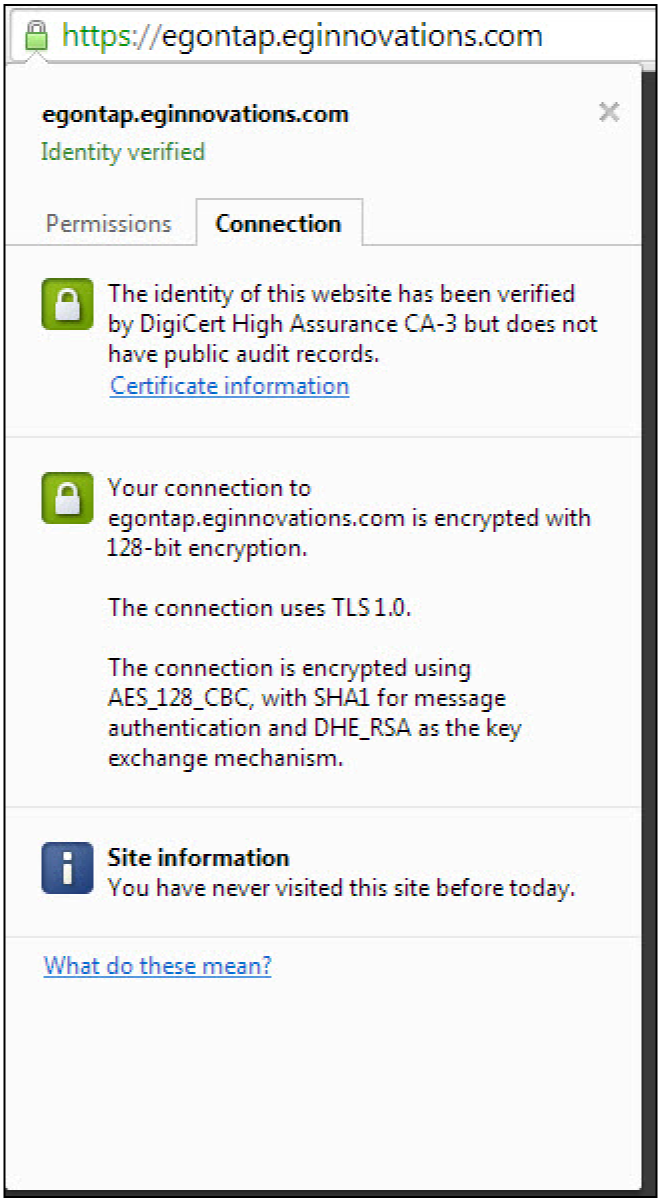

https://egontap.eginnovations.com
Indicates that the certificate used by the eG manager is a public certificate
Sign in
Username
Password
Forgot Password?
Sign In
© eG Innovations, Inc. All Rights Reserved.

Figure 2.130: A lock symbol in the address bar indicating that the SSL certificate used by the eG manager is a public certificate

To view the certificate, click the ‘lock symbol’. From the options that drop down, select the **Connection** tab page (see Figure 2.131).



https://egontap.eginnovations.com

egontap.eginnovations.com

Identity verified

The identity of this website has been verified by DigiCert High Assurance CA-3 but does not have public audit records.

Certificate information

Your connection to egontap.eginnovations.com is encrypted with 128-bit encryption.

The connection uses TLS 1.0.

The connection is encrypted using AES_128_CBC, with SHA1 for message authentication and DHE_RSA as the key exchange mechanism.

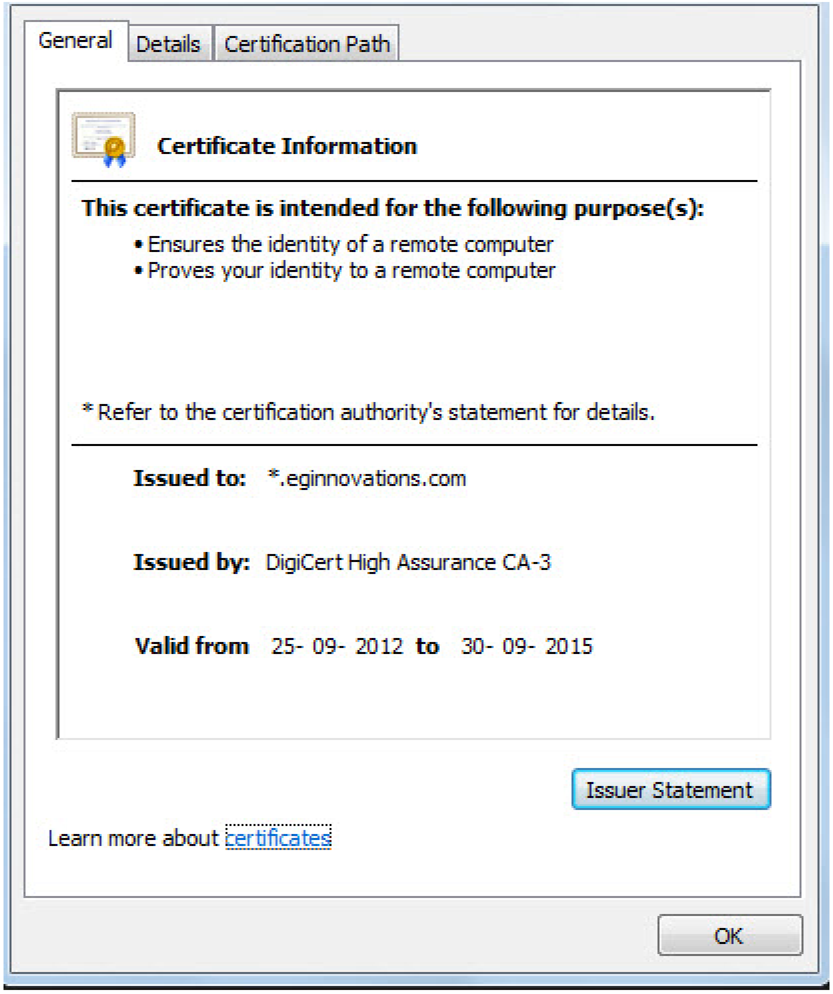
Site information

You have never visited this site before today.

What do these mean?

Figure 2.131: Viewing the connection details

To view the certificate details, click the **Certificate Information** link in Figure 2.131. Figure 2.132 will then appear, revealing the details of the SSL certificate.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer

* Refer to the certification authority's statement for details.

Issued to: *.eginnovations.com

Issued by: DigiCert High Assurance CA-3

Valid from 25- 09- 2012 to 30- 09- 2015

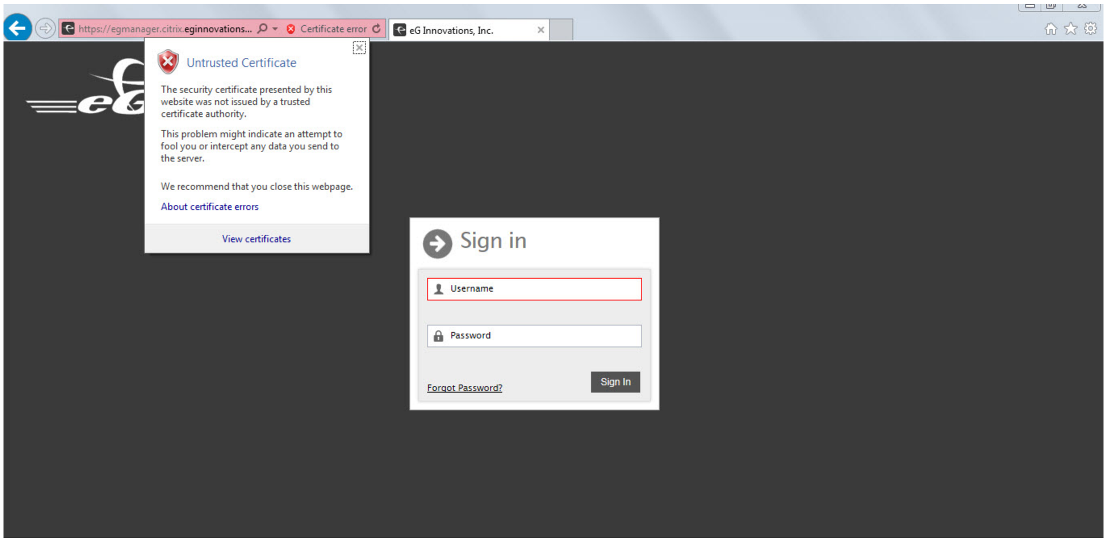
Figure 2.132: Viewing the Certificate information

Troubleshooting the error message “Public keys in reply and keystore don’t match”

If the above error message appears when importing a certificate into a keystore, it could imply that you have not downloaded all the certificates that are part of the certificate chain. In this case, go to the web site of the certifying authority to download the certificates. Then, try to import each certificate in sequence of their type – i.e., import the root certificate first, the intermediate certificates next, and the domain certificate last.

Troubleshooting the “Certificate error” that occurs when accessing an eG manager that is SSL-enabled using a certificate from an internal CA

Typically, when you attempt to access an eG manager that has been SSL-enabled using the certificate obtained from an internal CA, the browser will throw the following error message:



Untrusted Certificate

The security certificate presented by this website was not issued by a trusted certificate authority.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

Figure 2.133: The “Certificate error” that the browser reports

To avoid this error, you will have to import the internal CA’s root certificate to the browser and store it as a ‘trusted root certificate’. For this, follow the broad steps outlined below:

1. Copy the internal CA’s root certificate to the host from which you are accessing the eG manager (i.e., the browser host). For instance, if Microsoft Active Directory Certificate Services is your internal CA, then, you will find the root certificate of this CA on your domain server. So, in this case, you will have to copy the root certificate from the domain server to your browser host.
2. Next, using Windows Explorer, browse for the certificate, and once found, right-click on it. From the shortcut menu that appears, select the **Install Certificate** option (see Figure 2.134) to import the certificate to the browser.

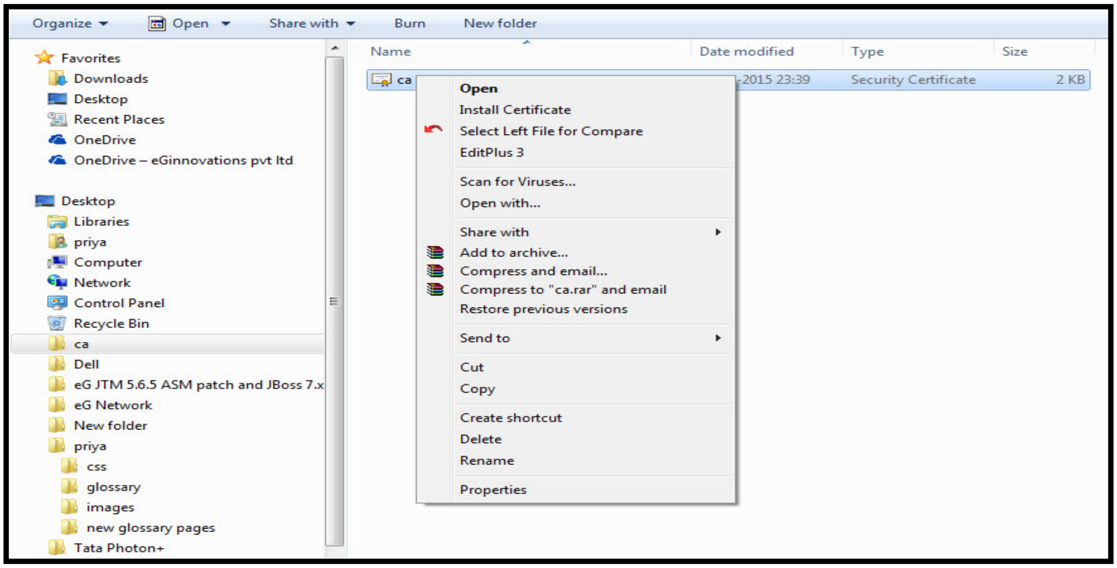
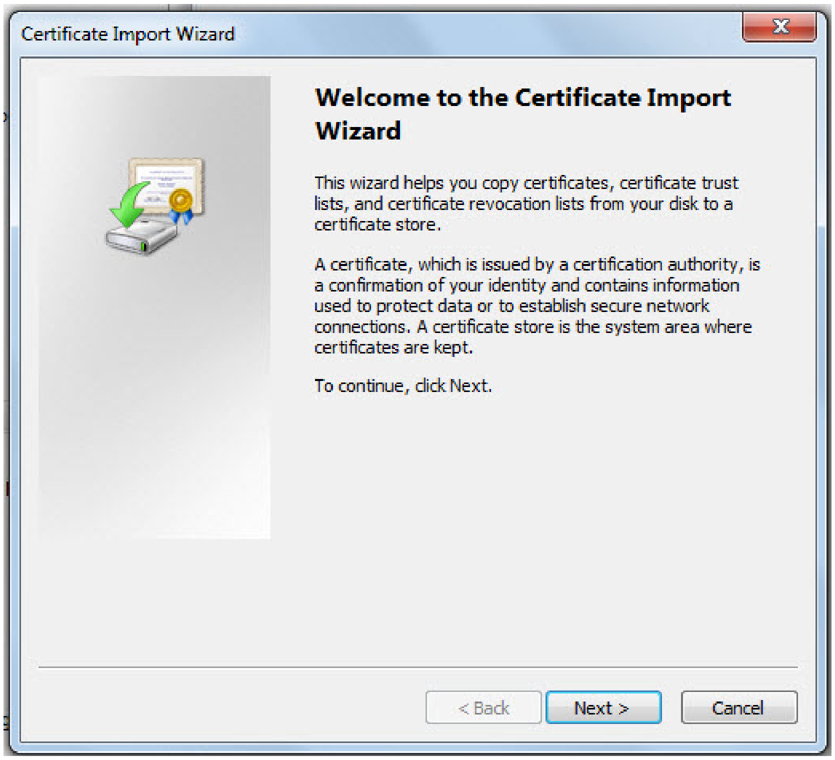


Figure 2.134: Selecting the option to install the certificate on the browser host

3. Figure 2.135 will then appear. Click **Next** here to continue.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

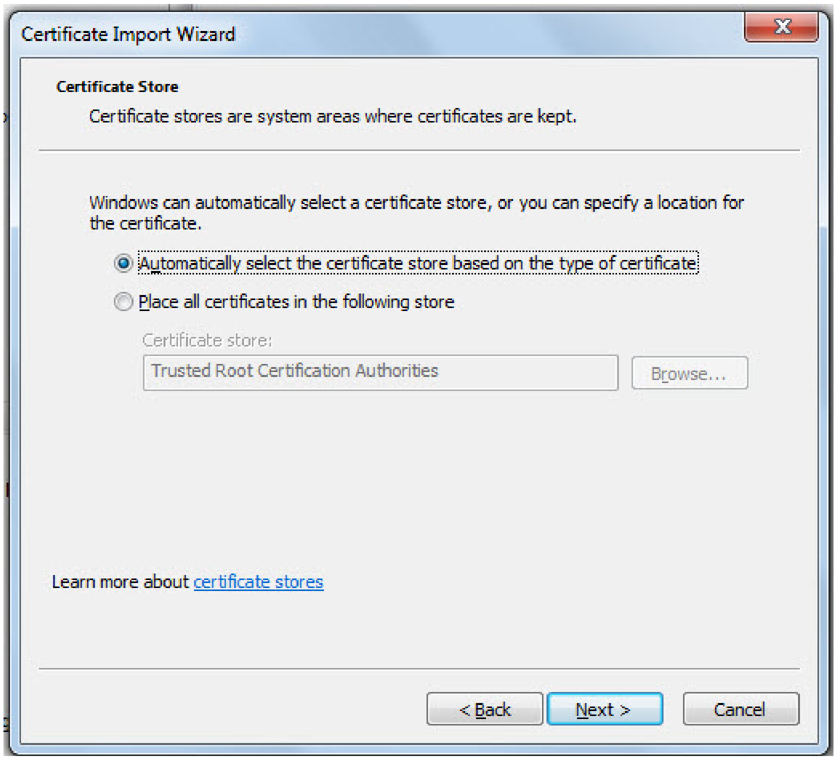
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Figure 2.135: Welcome screen of the Certificate Import Wizard

4. Figure 2.136 will then appear. Here, select the **Place all certificates in the following store**

option, and click the **Browser** button to indicate where the certificate is to be stored.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

● Automatically select the certificate store based on the type of certificate

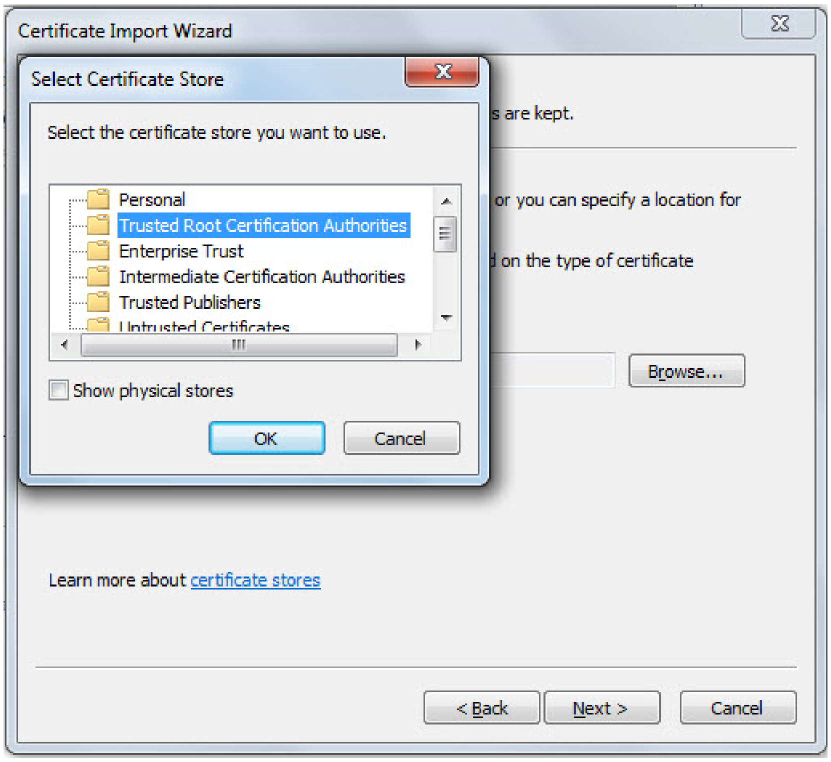
○ Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Learn more about certificate stores

Figure 2.136: Choosing to place the certificate in a specific store

5. From Figure 2.137 that then appears, select the **Trusted Root Certificate Authorities** store and click **OK**.



Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores

s are kept.

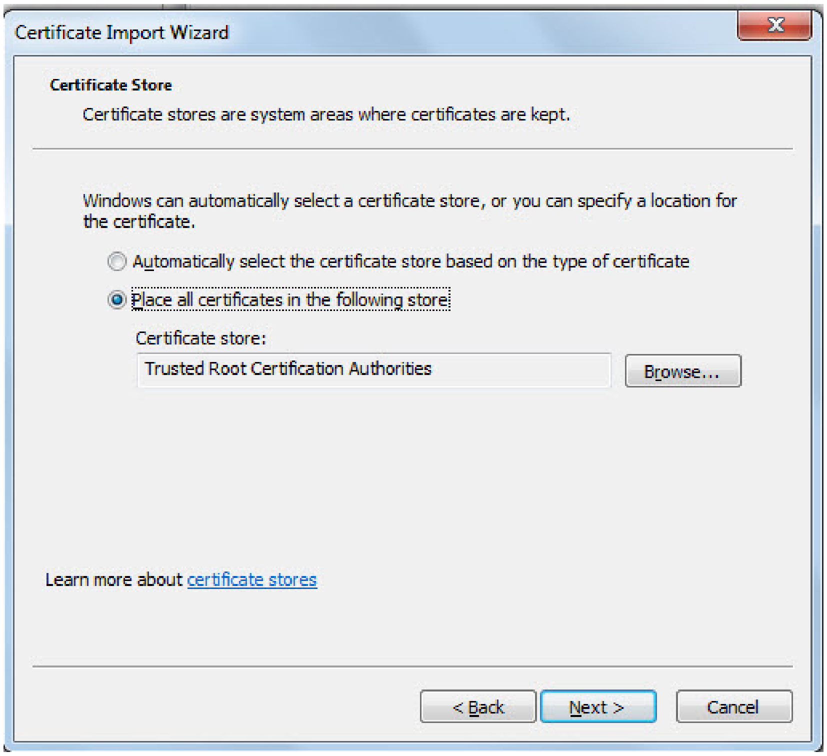
or you can specify a location for

d on the type of certificate

Learn more about certificate stores

Figure 2.137: Storing the certificate in the Trusted Root Certificate Authorities store

6. The chosen store will then appear in the text box below **Place all certificates in the following store** option, as depicted by Figure 2.138. Click **Next** in Figure 2.138 to continue.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

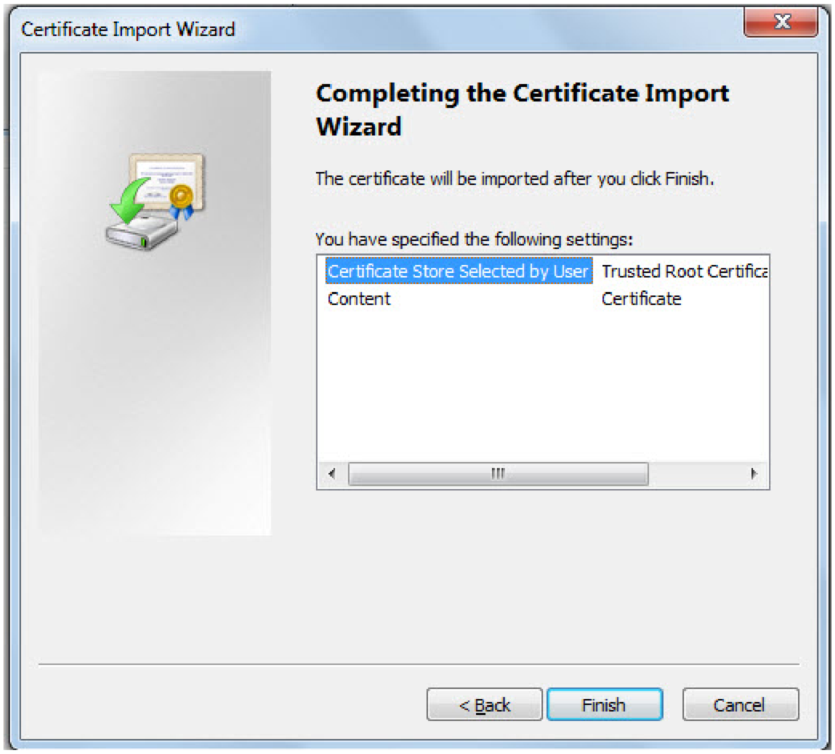
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Figure 2.138: The chosen store displayed

7. A quick summary of your selections will appear in Figure 2.139. Review your specifications and click **Finish** to complete the import.


Certificate Import Wizard

Completing the Certificate Import Wizard

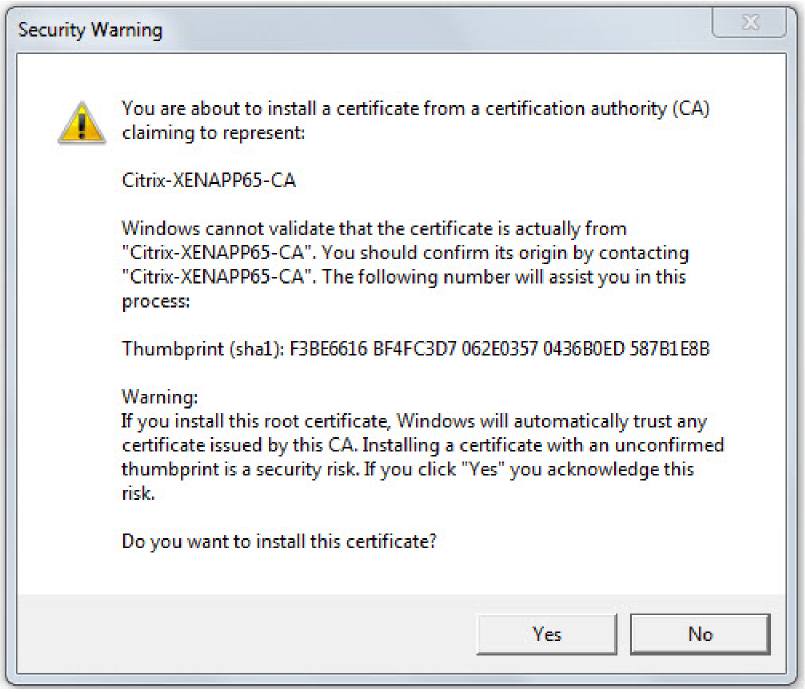
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certifica
Content	Certificate

Figure 2.139: Finishing the import

8. The following warning message will appear. Click **Yes** in Figure 2.140 to proceed with the import.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

Citrix-XENAPP65-CA

Windows cannot validate that the certificate is actually from "Citrix-XENAPP65-CA". You should confirm its origin by contacting "Citrix-XENAPP65-CA". The following number will assist you in this process:

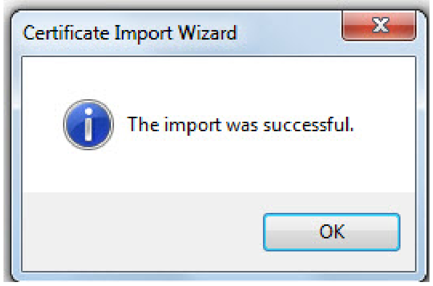
Thumbprint (sha1): F3BE6616 BF4FC3D7 062E0357 0436B0ED 587B1E8B

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Figure 2.140: A warning message that appears when importing a certificate issued by an internal CA

9. If import is successful, the following message will appear. Click **OK**.



Certificate Import Wizard

The import was successful.

Figure 2.141: A message box informing you that the certificate has been successfully imported

You will now be able to access the eG manager without a glitch!

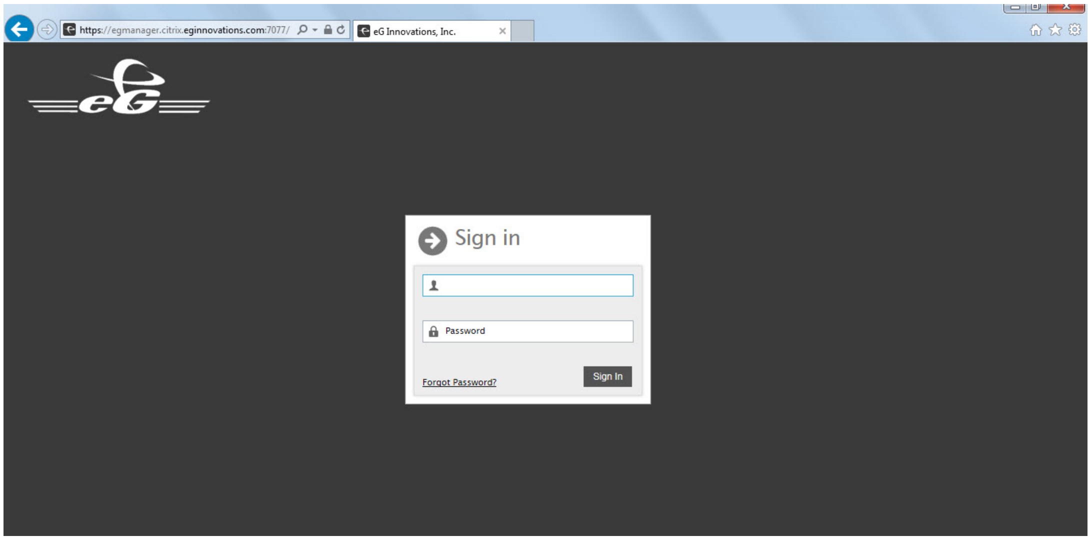


Figure 2.142: The login screen of the eG manager, without the ‘Certificate error’

How to convert a certificate from the p7b format to a PEM format?

Digital certificates issued by Microsoft are in a format (p7b) that cannot be used by Tomcat. Therefore, if you have obtained a valid certificate using Microsoft Active Directory Certificate Services as the CA, then, before attempting to import that certificate into a keystore file (i.e., before getting to the 2.8.0.9), you will have to convert the digital certificate in p7b (PKCS#7) format to PEM format on Windows. To achieve this, follow the steps below:

1. Login to the eG manager host.
2. In Windows Explorer, search for the certificate file with the extension **.p7b**.
3. Once you find it, double-click on it. This will open the **Certificates** window (see Figure 2.143).

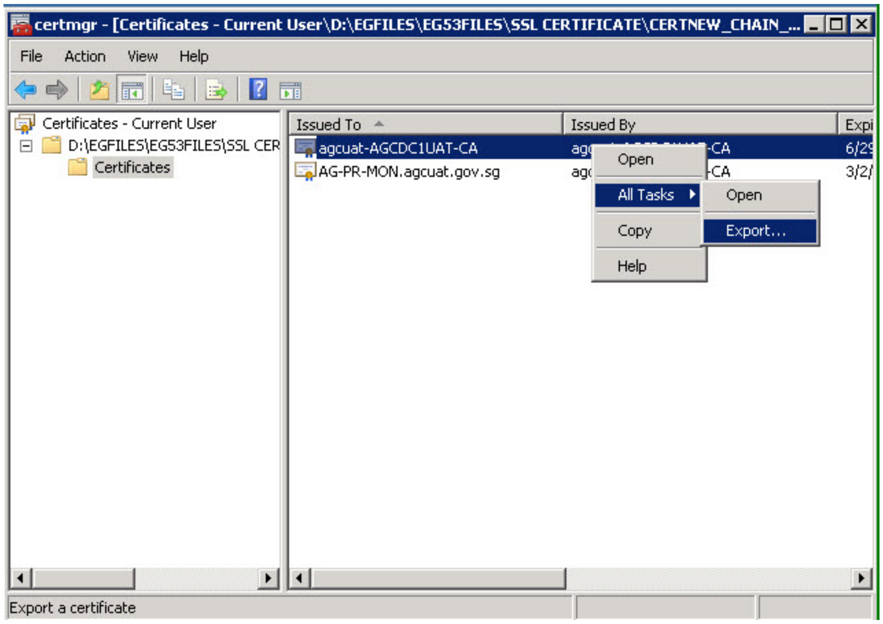


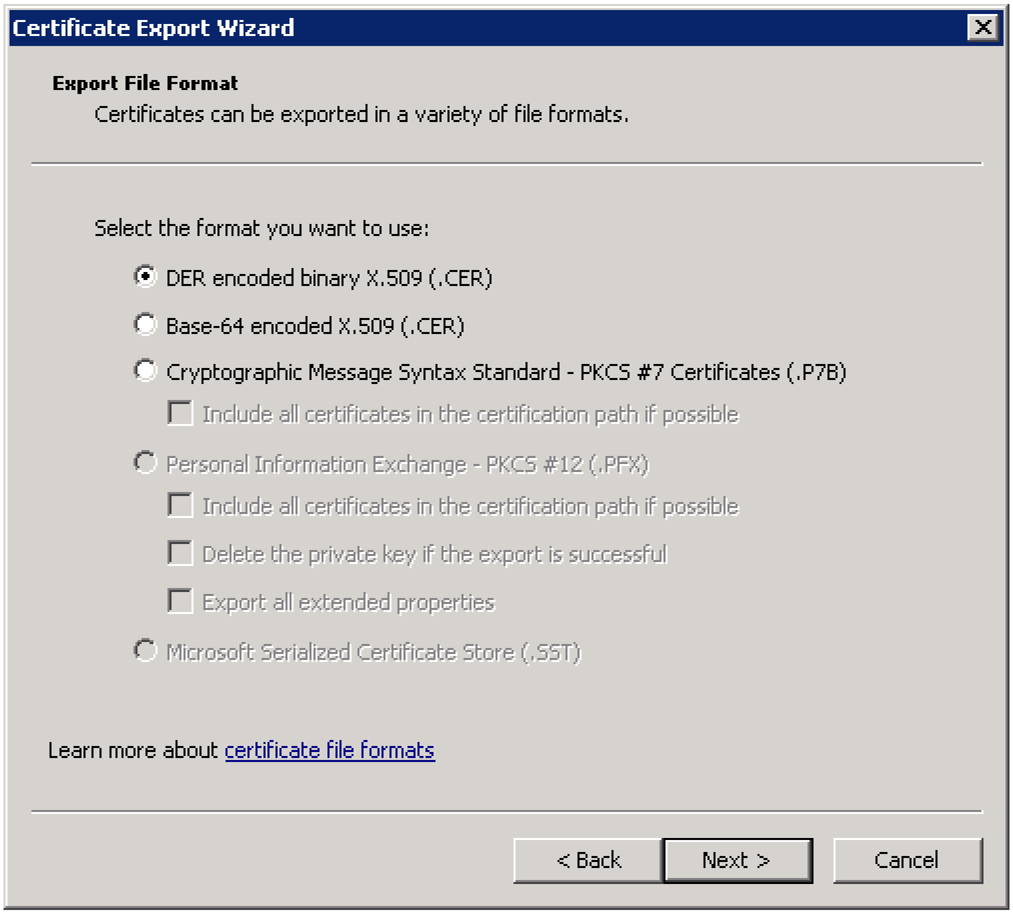
Figure 2.143: The Certificates window

4. In the left panel of the **Certificates** window, you will find a tree-structure with a list of certificate files available on the eG manager host for the current user. Expand the SSL Certificate file node and then click on the **Certificates** sub-node within. The right panel will then display the certificates.

5. From the certificates list in the right panel, select the certificate that needs to converted into the PEM format, right-click on it, and follow the *All Tasks* -> *Export* menu sequence in the shortcut menu that appears (see Figure 2.143).

6. A wizard will appear. Click **Next** in the wizard to proceed.

7. Figure 2.144 will then appear. Select the **DER encoded binary X.509 (.CER)** option in Figure 2.144 and click the **Next** button.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Figure 2.144: Converting the certificate into PEM format

8. You will now be prompted for a **File name**. Provide a name for the converted digital certificate, and click **Next**.

2.11 Configuring Double-byte Support

I have enabled double-byte support for my eG manager. My admin and monitor user interfaces now display double-byte characters. However, I am unable to save any of the reports that eG Reporter provides as PDF documents. What could be the problem?

- If you are working with an eG manager that is double-byte enabled, then you can save the reports that are generated by that manager as PDF documents only if the instructions given below are followed. Until then, eG Enterprise will **not allow you to save any report as a PDF**.
- Download the font file **Code2000.ttf** from the web. In fact, there are many web sites that provide downloads of this file. The site that we recommend is http://www.code2000.net/code20000_page.htm
- Copy the downloaded font file to the <EG_INSTALL_DIR>\lib directory.

- Next, move to the <EG_INSTALL_DIR>\lib directory, and issue the following command:

  jar -cvf font.jar CODE2000.TTF

- Finally, check whether the **font.jar** is created in the <EG_INSTALL_DIR>\lib directory.

Note:

If your eG manager is double-byte enabled, but the **Language** preference that you have set in the **USER PROFILE** page is **English**, then, you do not have to follow the steps discussed above to ensure that reports are saved as PDF documents. However, while using a double-byte enabled eG manager, if you have chosen to view data in a **Language** other than **English**, then reports cannot be saved as PDF documents until the above-mentioned steps are followed.

Chapter 3: eG Agent Installation

The eG agents monitor the environment by running periodic **tests**and use different approaches for testing the target environments. Based on the monitoring approach employed and where they are installed, agents are classified as follows:

Internal Agents

Internal Agents are installed on the same machines that they monitor and have the ability to run many tests. This will be the most common method of monitoring and is suitable for monitoring applications, servers, operating systems, etc. A single agent on a server can monitor any number of applications and also different types of applications (for example, web servers, middleware, messaging applications, enterprise applications, databases, etc.) running on it. Because of its multiple application support and one-agent-fits-all approach, this agent is also called a Universal Monitoring Agent.

Remote Agents

Remote Agents are proxies for internal agents in the sense that they perform similar tasks – just that they are deployed outside the target system they are intended to monitor. These agents connect remotely to the target systems using protocols such as JMX, SSH, SMI-S, web services APIs (e.g., virtual platforms), etc. for monitoring. This forms an agentless monitoring approach for servers and devices. Remote agents are typically used in cases where it is not recommended to install an internal agent – for example, on a VMware hypervisor where any software installation on the console operating system is to be avoided; or a storage device, where it is not possible to deploy an agent. For more details on agentless monitoring using remote agents, refer to the topic.

External Agents

External Agents are mainly used for black box monitoring of network devices, servers, and applications. Typical functions include tracking network availability and responsiveness via PING tests and application availability and responsiveness by making TCP port connections. These agents also make protocol level requests for protocols such as HTTP, SMTP, FTP and others to report service availability and responsiveness. These same agents can be used to monitor network switches, routers, firewalls, printers and so on using SNMP. This also forms an agentless monitoring approach.

For making measurements, eG agents support various mechanisms. The Simple Network Management Protocol (SNMP) continues to be the standard for monitoring network elements (routers, load balancers, WAP gateways, etc.). Besides monitoring network elements, eG agents also manage systems and applications. SNMP is rarely supported at the application layer. Hence, for monitoring applications, eG agents support various other mechanisms:

1. **Emulated transactions:** By emulating typical transactions from clients to different applications, eG agents monitor various aspects of the server. For example, to measure the health of a web server, eG Enterprise uses an HttpTest that emulates user accesses to the web server. Depending on whether and when a response is received or not, as well as based on the status code returned by the server in the Hyper Text Transport Protocol (HTTP) response returned by the server, the eG agent assesses the availability of the web server and the response time for the request.
2. **SNMP data collection:** To monitor the various network elements and any other application components that support SNMP, eG agents support SNMP-based monitoring.
3. **OS-specific instrumentation:** Server operating systems already collect a host of statistics regarding the health of the server and processes executing on it. For example, CPU, memory, and disk space utilizations, network traffic statistics, process-related measures can all be collected using operating system specific hooks. eG agents use these hooks to collect and report a variety of statistics of interest.
4. **Application specific adapters:** For monitoring specific applications, an eG agent uses custom adapters. One example of a custom adapter is the **web adapter**. The key motivation for the web adapter technology is that even today log files produced by web servers continue to be the predominant mode of monitoring web servers. Logging has several drawbacks. Since each and every request received by the web server is recorded in the logs, each request produces a disk access that can be an expensive operation. Moreover, large web sites that get millions of hits a day can produce logs that are several terabytes in size. Processing these log files is extremely expensive (in terms of CPU and memory overheads on the server). Consequently, most web site administrators are forced to process their logs in off-line mode. The eG web adapter is designed to enable web site administrators to collect statistics regarding user accesses in real-time, without the need for explicit logging of requests by the web server. The web adapter is a layer that fits between the TCP/IP stack and the web server itself. It can be thought off as a passive probe that watches the requests received by the server and the responses produced by the server. By applying a fast, pattern-matching algorithm on the packets that flow by, the web adapter collects a variety of statistics regarding web sites and the transactions executed by users at these sites.

eG agents have been pre-programmed to execute specific tests for web servers, SSL servers, LDAP servers, DNS server, Database servers, and application servers. For components that are not included in the core eG Enterprise system, the eG professional services team provides customization services that include studying the behavior of a component, designing, and implementing tests for the component, and integrating the new component into the eG management framework.

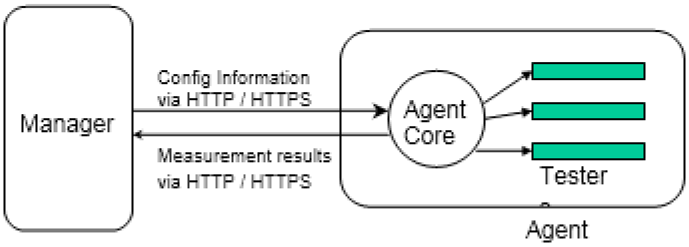

Manager
Config Information via HTTP / HTTPS
Measurement results via HTTP / HTTPS
Agent Core
Tester
s
Agent

Figure 3.1: The manager-agent communication in the eG architecture

All manager-agent communication happens over the HTTP / HTTPS protocol. The agent uses **tester threads**, each of which is responsible for a specific test. The main functions of the agent core are:

- To read configuration information from the manager and determine what tests are to be executed on a host.
- To periodically refresh the configuration information from the manager and determine if any of the testers needs to be stopped or restarted, or whether the configuration information for any of the tests needs to be changed.
- To read the threshold information from the manager and use it to determine whether the state of each measurement is normal or not
- To provide alarms to the manager in the event that the state of any measurement changes
- To upload measurement results back to the manager for permanent storage.

Figure 3.2 depicts the typical deployment architecture of eG Enterprise. The eG manager is installed on a server called the eG server. By default, an external agent is also hosted on this system. Internal agents are installed on all the other servers being monitored in this environment. The configuration of external agents can be modified to suit the target environment. For example, in Figure 3.2, an external agent is located within each customer's network (in the case of a service provider servicing multiple customers) or within each network domain (in the case of a corporate Intranet that comprises of different independent domains).

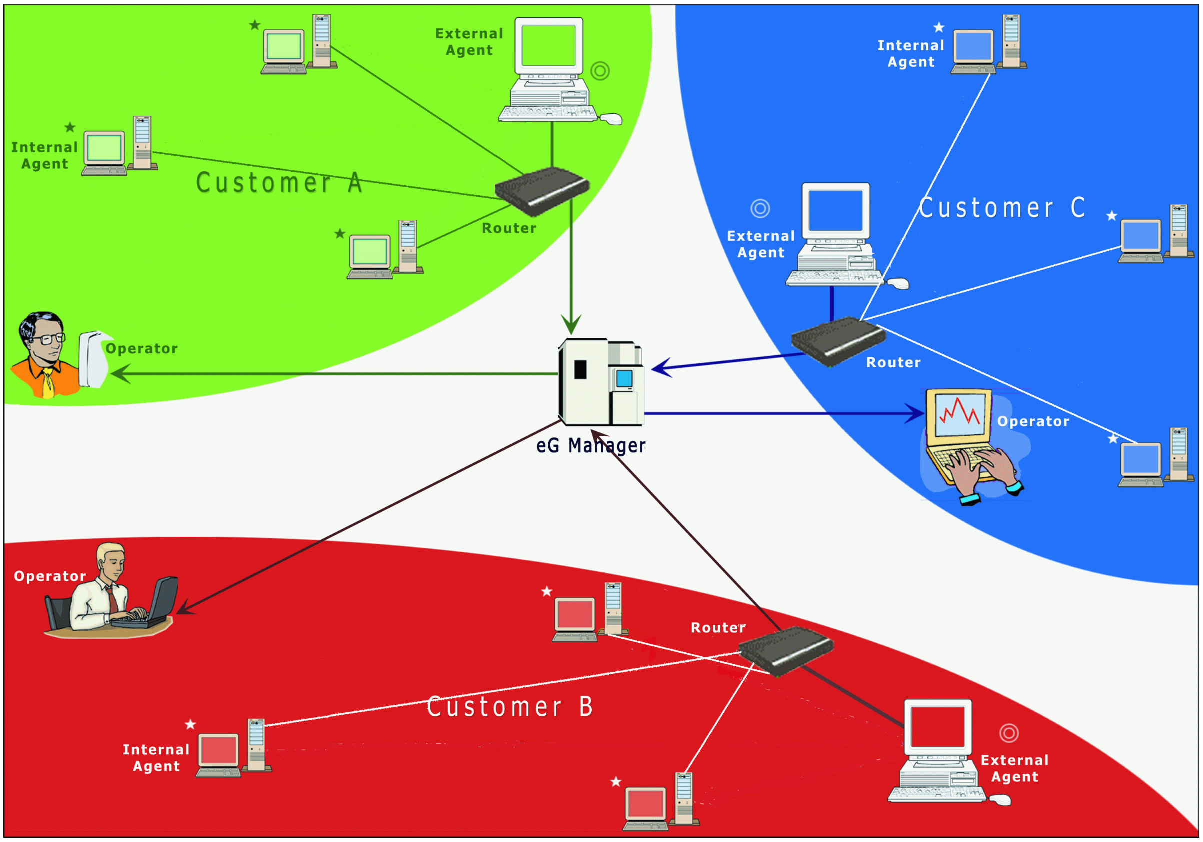


Figure 3.2: A typical deployment architecture of eG Enterprise

3.1 Pre-requisites for Installing eG Agent

A set of pre-requsites should be fulfilled before you start deploying the eG agent. The requirements will vary based on the platform on which the eG agent is being installed. These requirements are discussed in the following sections.

3.1.1 For Windows Platforms

For the eG agent to function effectively, the system on which the agent is being installed should support:

- Windows 2008 server (OR) Windows Vista (OR) Windows 7 (OR) Windows 8 (OR) Windows 2012 (OR) Windows 10 (OR) Windows 2016 (OR) Windows 2019
- 512 MB RAM with at least 1 GB of disk space free for installing the agent

Note:

- On Windows systems, the user account used to run the eG Agent on a system has to be a part of the local administrator group of that system. The two basic privileges that the user running the eG agent should have are “allow log on locally” and “log on as a service”. If the proper privileges are not provided to the user running the eG agent service, the eG agent will stop after running for a while.

- Before deploying the web adapter to monitor an IIS web server, check whether any other ISAPI filters pre-exist. If so, ensure compatibility of the filters before deployment.

3.1.2 For Unix Platform

For the eG agent to function effectively, the system on which the agent is being installed should support:

- Solaris 7 (or higher), Red Hat Enterprise Linux v3 (or higher), AIX 4.3.3 (or higher), HP-UX 10 (or higher), FreeBSD 5.4, Tru64 5.1, openSUSE v11 (or above), CentOS v5.2 (or above), Fedora Linux, Oracle Linux v6.x (or higher), Ubuntu, Debian
- 512 MB RAM and at least 1 GB of disk space for installing the agent

Note:

The eG agent software has to be installed from a super-user account.

As in the case of the manager, the procedure for installing an agent varies depending on the operating system environment used. Instructions for installing the agent on Solaris, Linux, AIX and HPUX operating systems are provided in the following sections.

3.2 eG Agent on Windows

The procedure for installing and configuring an eG agent on Windows varies based on whether the agent is installed for an Enterprise deployment of the eG manager or a SaaS deployment. To know how to install the eG agent in the different deployment scenarios, use Section **3.2.1** topic in this section.

3.2.1 Installing and Configuring the eG Agent on Windows

There are two approaches to installing an eG agent on Windows:

- The eG agent software for Windows is available in the eG web site as a set of **self-extracting setup programs (*.exe)** - one for every flavor/version of Windows that eG supports. You can **download** the **exe** that corresponds to the target Windows host **from the eG web site**, and **manually run the executable** on that host to install the eG agent. This approach is ideal if you want to deploy eG for a single organization - i.e., for the Enterprise deployment of eG.

- The eG agent software for Windows is provided as a set of **packaged applications -** one for every flavor/version of Windows that eG supports. You can **download** the **agent package** that corresponds to the target Windows host **from the eG manager console**, extract the contents of the package to any folder in the target host, and **silently run setup on each host** to install the agent. If you are **deploying eG Enterprise for SaaS**, then it is **mandatory that your tenants use this approach** to install the eG agents in their environment.

Both these approaches are discussed in this section.

3.2.1.1 Installing Windows Agents for an Enterprise Deployment of the eG Manager

An Enterprise deployment of the eG manager is typically used to monitor only a single organization's IT infrastructure. In this case, it is recommended that the procedure detailed in this section be used to install eG agents on Windows hosts.

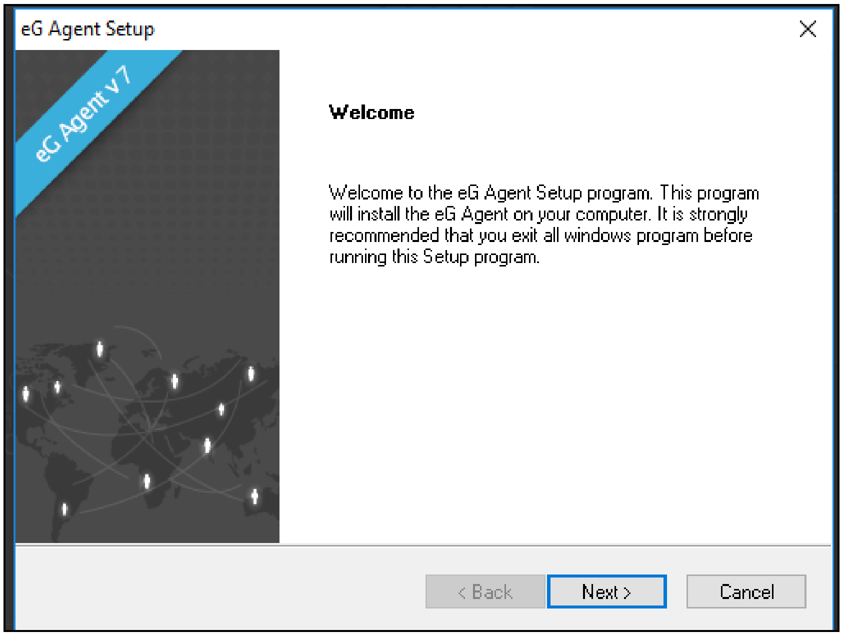
Before installing the eG agent on Windows, choose from the following self-extracting programs, based on what flavor/version of Windows is in use:

- **eGAgent_win2008.exe**, if you are installing on a 32-bit Windows 2008 / Windows Vista/ Windows 7 host
- **eGAgent_ win2008_ x64.exe**, if you are installing on a 64-bit Windows 2008/Windows Vista/Windows 7 host
- **eGAgent_win2012.exe** , if you are installing on a 32-bit Windows 8 / Windows 2012 host
- **eGAgent_win2012_x64.exe**, if you are installing on a 64-bit Windows 8 / Windows 2012 host
- **eGAgent_win2016_x64.exe**, if you are installing on a Windows 2016 / Windows 10 host
- **eGAgent_win2019_x64.exe**, if you are installing on a Windows 2019 host

Note:

Before installing an eG agent on a Windows 2008 host, make sure that the VC 2008 (or above) runtime engine exists on that host. If not, then download and install the same. For use on a 32-bit Windows 2008 host, you need to download the 32-bit VC 2008 (or above) runtime engine from the URL, *http://www.microsoft.com/download/en/details.aspx?id=29*. Prior to installing the eG agent on a 64-bit Windows 2008 host, download and install the 64-bit VC 2008 (or above) runtime engine from the URL, *http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=15336*.

1. To start the installation process, download the corresponding **exe**from the eG web site to any folder in the target Windows host. The steps for downloading are detailed in the *eG Quick Installation Guide*. Then, run the downloaded exe. The Welcome screen (see Figure 3.3) of the eG agent Setup program appears. Clicking on the **Next >** button at the bottom of this screen takes the user to the next step of the setup.

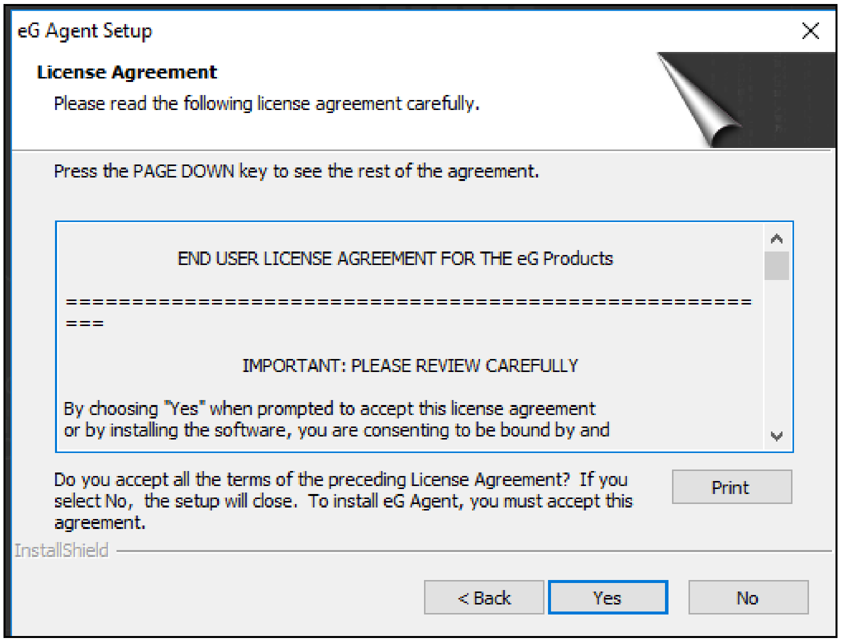


Welcome

Welcome to the eG Agent Setup program. This program will install the eG Agent on your computer. It is strongly recommended that you exit all windows program before running this Setup program.

Figure 3.3: Welcome screen of the eG agent setup program

2. Now, the user can view the eG license agreement (see Figure 3.4). Also, the setup program seeks the confirmation of the user regarding his/her acceptance of the terms and conditions of the license agreement. It is mandatory that the user must accept the license agreement to proceed with the setup. The user now needs to go through the license agreement thoroughly and click the **Yes** button at the bottom of the screen to accept and proceed with the setup process.



eG Agent Setup

License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

END USER LICENSE AGREEMENT FOR THE eG Products

==
===

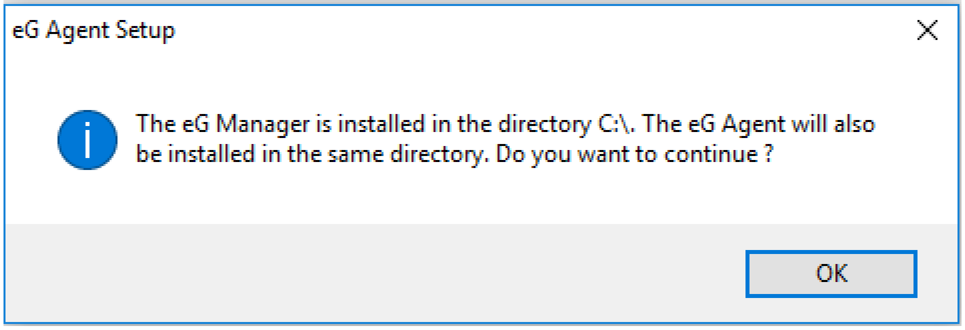
IMPORTANT: PLEASE REVIEW CAREFULLY

By choosing "Yes" when prompted to accept this license agreement
or by installing the software, you are consenting to be bound by and

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install eG Agent, you must accept this agreement.

Figure 3.4: License agreement for the eG agent

3. If an eG manager resides on the host where the agent is being installed, then setup will automatically install the agent in the same location as the manager. In this case, a message to that effect will appear, as depicted by Figure 3.5. Click the **OK** button in Figure 3.5 to continue with the installation.



eG Agent Setup

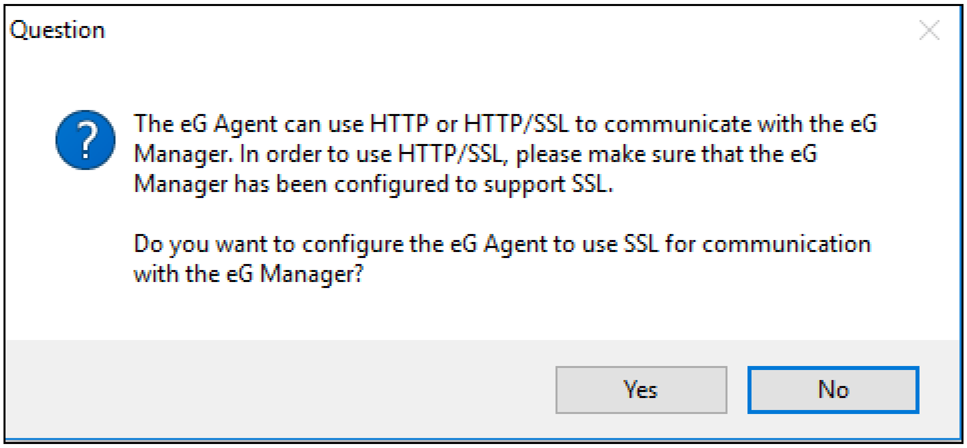
The eG Manager is installed in the directory C:\. The eG Agent will also be installed in the same directory. Do you want to continue ?

Figure 3.5: Installing the eG agent in the same directory as the eG manager

On the other hand, if an eG manager does not pre-exist on the eG agent's host, then you will be prompted to specify the directory in which the eG agent needs to be installed. After specifying the directory, click the **Next** button to continue with the installation.

4. Soon after the agent install directory is specified, a message box will appear requesting you to indicate whether the eG agent is to use SSL for communicating with the manager (see Figure

3.6). Click on the **Yes** button to confirm SSL support for the agent. If the eG manager is not SSL-enabled or if you do not want the agent to communicate with the manager over SSL, then click the **No** button.

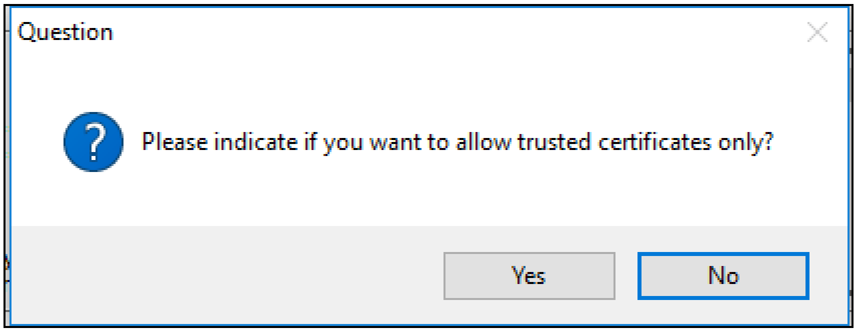

Question

The eG Agent can use HTTP or HTTP/SSL to communicate with the eG Manager. In order to use HTTP/SSL, please make sure that the eG Manager has been configured to support SSL.

Do you want to configure the eG Agent to use SSL for communication with the eG Manager?

Figure 3.6: A message box requesting the user's confirmation to enable SSL support for the eG agent

5. If the **Yes** button is clicked at step 4, then Figure 3.7 will appear requesting your confirmation to allow trusted certificates only. Click on the **Yes** button if the agent is expected to communicate only with a manager that has a trusted SSL certificate. If you click on the **No** button, the agent accepts any certificate provided by the manager at the time when the SSL connection is established.


Question

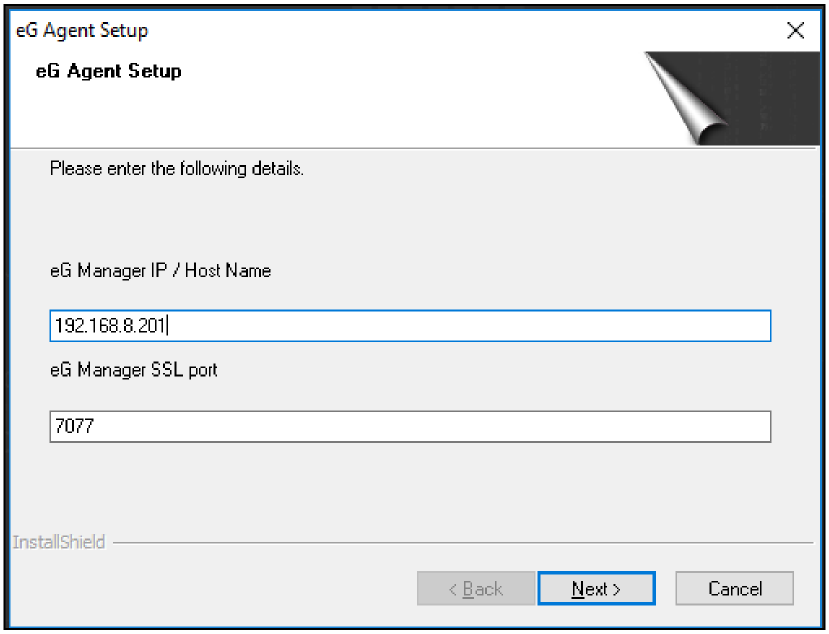
Please indicate if you want to allow trusted certificates only?

Figure 3.7: A message box requesting your confirmation to allow only trusted certificates

Note:

If you have chosen to allow only trusted certificates only, then ensure that the IP/hostname provided in Figure 3.8 matches that of the certificate. Then, follow the procedure detailed in **Enabling the eG Agent to Allow Trusted Certificates** topic once the agent installation is complete.

6. Clicking on either button (in Figure 3.7) will reveal Figure 3.8 using which the manager IP/hostname and the SSL port will have to be specified.


eG Agent Setup

eG Agent Setup

Please enter the following details.

eG Manager IP / Host Name

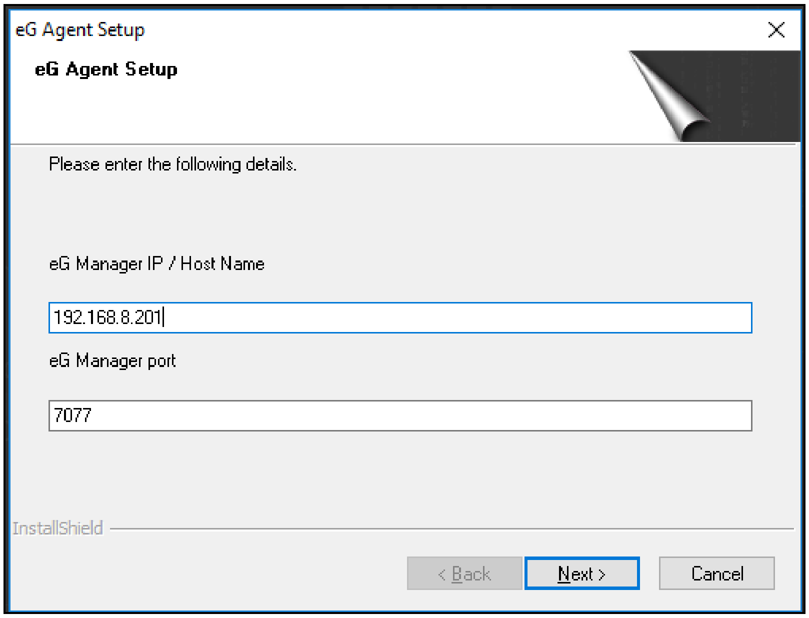
192.168.8.201

eG Manager SSL port

7077

Figure 3.8: Specifying the IP/hostname and SSL port of the eG manager

7. However, if you click on the **No** button in the message box that appears at step 4, then you will jump straight to this step, where you will have to configure the IP/hostname and port (not SSL port) of the eG manager that the agent should communicate with (see Figure 3.9). 7077 is the default port. The hostname should be used if DNS is enabled in the target environment. Otherwise, the IP address should be used.



eG Agent Setup

eG Agent Setup

Please enter the following details.

eG Manager IP / Host Name

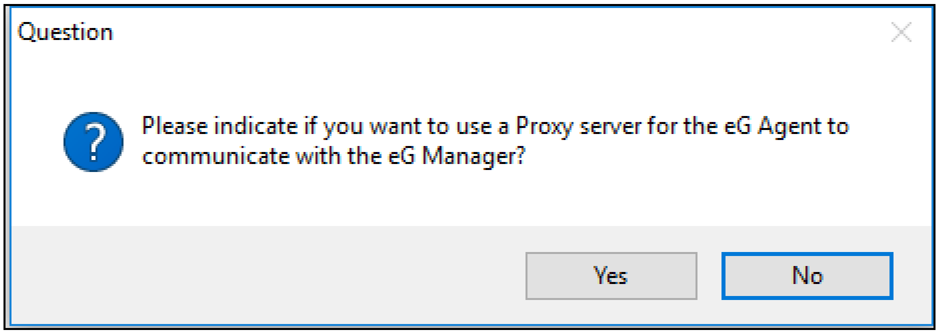
192.168.8.201

eG Manager port

7077

Figure 3.9: Hostname and port number of the eG manager to which the agent communicates

8. The setup process requires to know if the user needs a proxy for the eG manager - agent communication. The same has to be indicated via the dialog box depicted by Figure 3.10. The default option is **No**. If you want the eG agent to communicate with the eG manager via proxy, then click the **Yes** button in Figure 3.10.

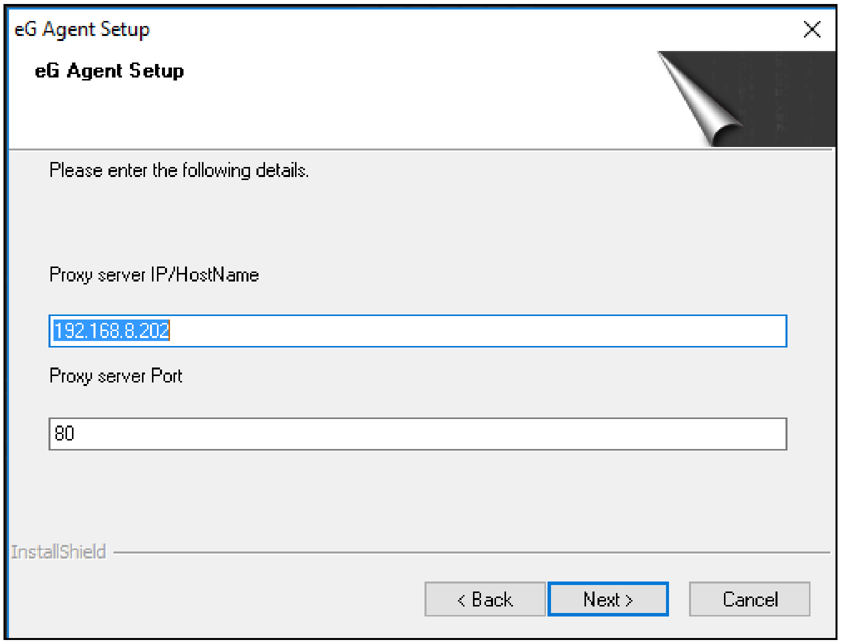


Question

Please indicate if you want to use a Proxy server for the eG Agent to communicate with the eG Manager?

Figure 3.10: Setup enquiring if the user wants to use a proxy server for the eG manager - agent communication

9. If the user chooses to use a proxy, he/she has to provide the name of the proxy server followed by the port number of the proxy server in Figure 3.11. The default port number of a proxy server is 80. However, if the user chooses not to use a proxy server, he/she will be taken to step 12 of this setup.


eG Agent Setup

eG Agent Setup

Please enter the following details.

Proxy server IP/HostName

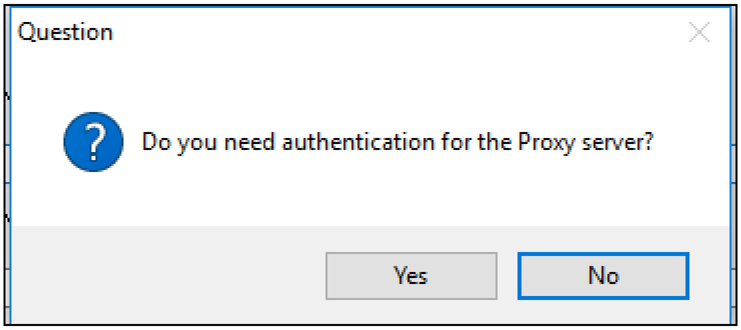
192.168.8.202

Proxy server Port

80

Figure 3.11: Specifying the proxy server that the agent may need to use to communicate with the eG manager

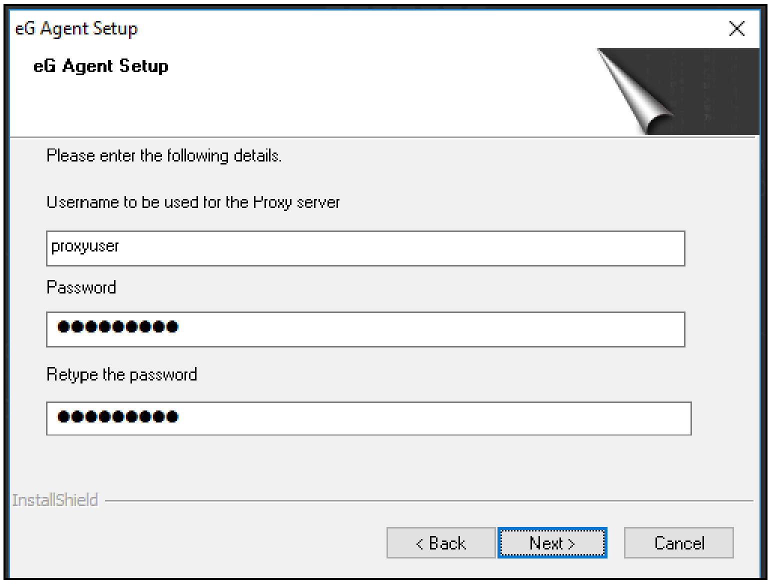
10. Some proxy servers may be setup to validate incoming requests based on the user name and password specified before forwarding the requests to other web servers. To support such cases, the setup process enquires as to whether authentication is required by the proxy server (see Figure 3.12). The default option is **No**. Click **Yes** if the proxy server requires authentication.


Question

Do you need authentication for the Proxy server?

Figure 3.12: Setup seeking the confirmation regarding authentication of the proxy server

11. If authentication is required, the eG agent setup allows the user to enter the user name and password that is used for all communications from the agent to the manager via a proxy server as in Figure 3.13.



eG Agent Setup

eG Agent Setup

Please enter the following details.

Username to be used for the Proxy server

proxyuser

Password

●●●●●●●●●

Retype the password

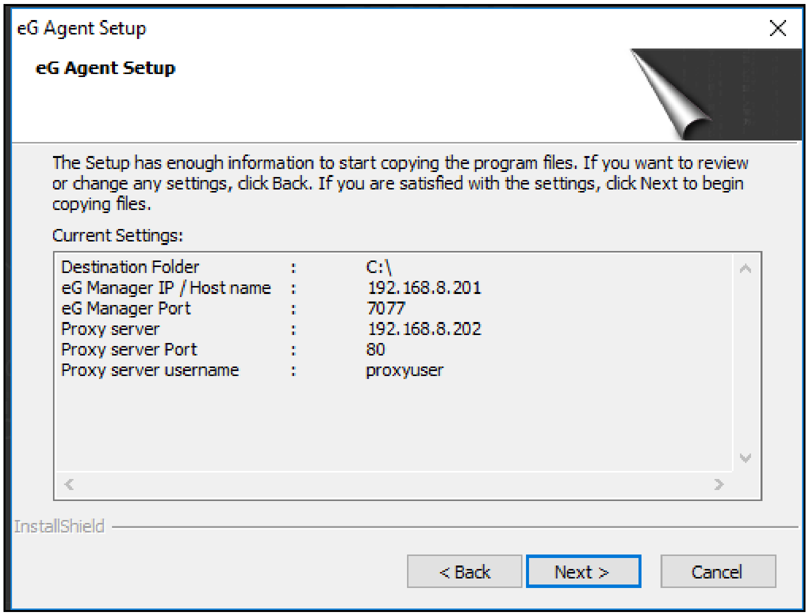
●●●●●●●●●

Figure 3.13: Username and password to be used for communication via a proxy server

Note:

If the eG agent is configured to communicate with the eG manager via a proxy server, then, whenever the eG agent attempts to remotely monitor an application by connecting to it via HTTP/HTTPS, it may automatically use the proxy server to establish this connection; this in tun may cause problems while monitoring those applications. To avoid this, before configuring the eG agent-manager communication via a proxy, make sure that the agent will be able to connect to remote applications also via the same proxy.

12. The next step displays all the details that have been provided so far by the user as in Figure 3.14.



eG Agent Setup

eG Agent Setup

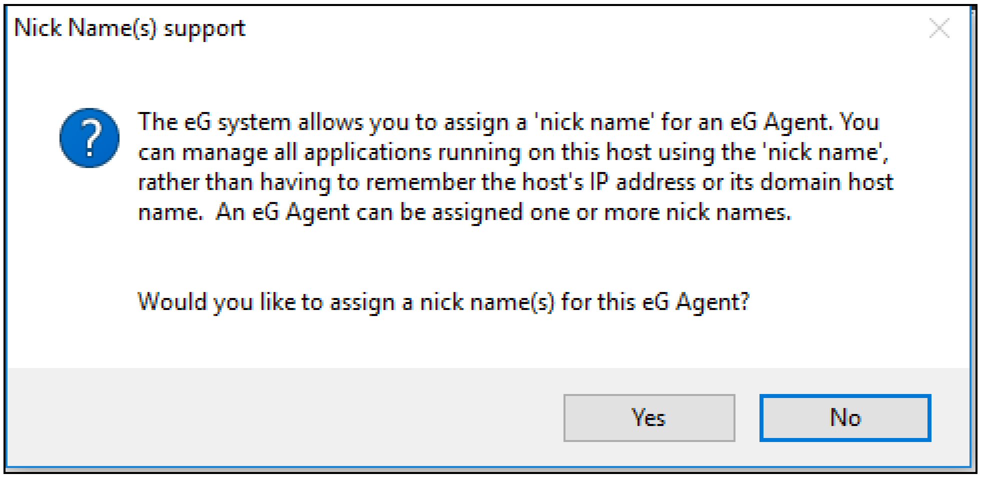
The Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
Destination Folder          :        C:\
eG Manager IP / Host name   :        192.168.8.201
eG Manager Port             :        7077
Proxy server                :        192.168.8.202
Proxy server Port           :        80
Proxy server username       :        proxyuser
```

Figure 3.14: Information specified by the user at the various stages of the setup process

13. Next, the user has to decide whether to assign a nick name for the eG agent. In many environments, servers and routers may not be assigned host names. Furthermore, the host names may not be easy to remember or recall. It is not easy to refer to servers and network devices using their IP addresses. To make it easy for administrators/operators to refer to the monitored servers/devices, the eG manager and agents can identify these devices using "nick names". A nick name is a logical, easy to understand name assigned to a server/device. Nick names can be assigned to a server when installing the agent. The nick name assigned to a server when installing an agent must also be specified in the eG admin interface when adding an application on that server. Figure 3.15 provides the user the option of specifying a nick name.



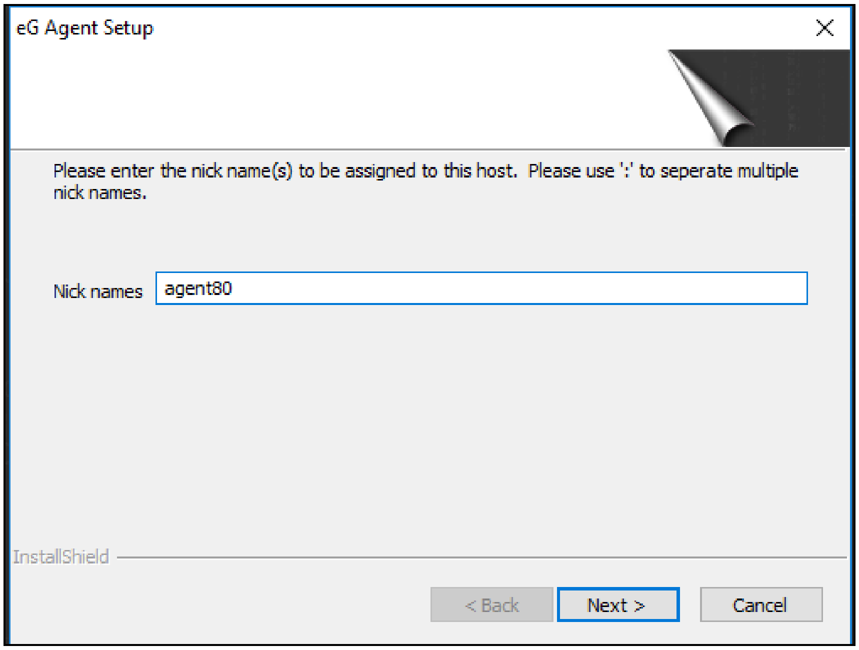
Nick Name(s) support

The eG system allows you to assign a 'nick name' for an eG Agent. You can manage all applications running on this host using the 'nick name', rather than having to remember the host's IP address or its domain host name. An eG Agent can be assigned one or more nick names.

Would you like to assign a nick name(s) for this eG Agent?

Figure 3.15: Setup requesting the user's confirmation to assign a nick name for the eG agent

14. Clicking on the **Yes** button in Figure 3.15 will then require the user to specify the nick name (see Figure 3.16).



Please enter the nick name(s) to be assigned to this host. Please use ':' to seperate multiple nick names.

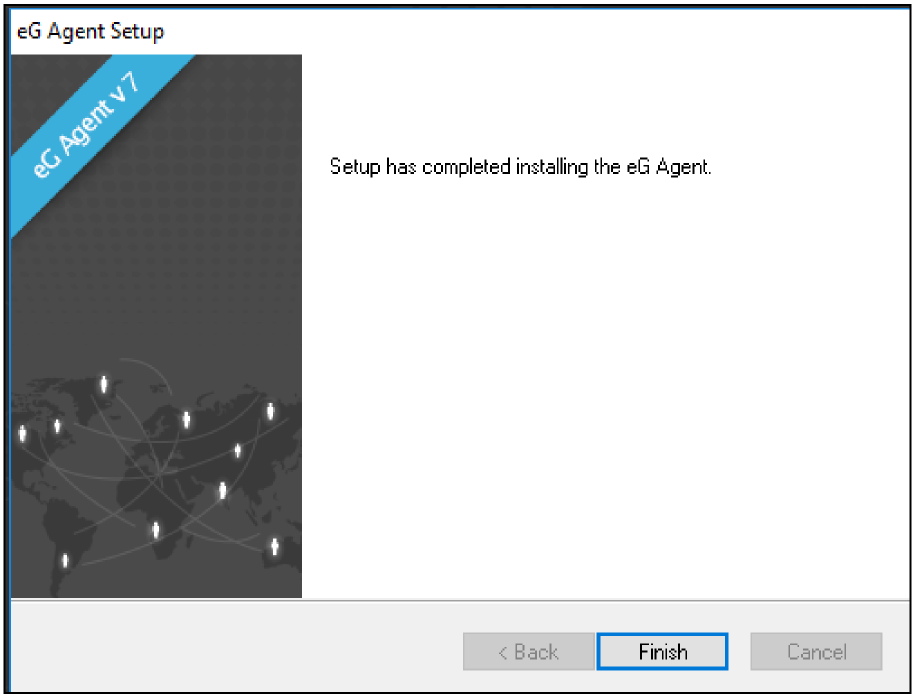
Nick names: agent80

Figure 3.16: Assigning a nick name for the eG agent's host

Note:

Once a nick name is specified for a host, the user has the option of managing applications running on the host by using the nick name/ IP address. While providing multiple nick names, ensure that they are separated by a ':'. Also, ensure that a nick name does not contain any white spaces, and that all nick names are in lower case.

15. If the configuration process succeeds, the following screen will be displayed (see Figure 3.17). Clicking on the **Finish** button will exit the Setup.



Setup has completed installing the eG Agent.

Figure 3.17: The completion of the eG agent setup

3.2.1.2 Installing Windows Agents for a SaaS Deployment of the eG Manager

As stated earlier, where eG Enterprise needs to support multiple tenants - eg., MSP environments with multiple customers, enterprises with multiple departments/domains - the individual tenants should use only this approach to deploy the eG agent on the Windows hosts in their specific environments.

A key pre-requisite of this approach is that the eG manager should already be deployed and running.

To enable a tenant to install eG agents, the administrator should first make sure that the agent packages that correspond to the tenant's environment are accessible to the tenant from the eG manager console. For that, the administrator should do the following:

1. Login to the system hosting the eG manager.
2. From a browser, connect to the URL: https://www.eginnovations.com/eval712/AgentPackages
3. In this location, you will find a set of zip files. Each zip file is an agent package that corresponds to every operating system on which an eG agent can be installed.
4. Download the agent packages / zip files that correspond to the hosts in your tenant's

environment, to any folder on the eG manager host. The Windows-specific packages are as follows:

- **Windows_2008.zip** for 32-bit Windows 2008 / Windows Vista/ Windows 7 hosts
- **Windows_2008_x64.zip** for 64-bit Windows 2008 / Windows Vista/ Windows 7 hosts
- **Windows_2012.zip** for 32-bit Windows 8 / Windows 2012 hosts
- **Windows_2012_x64.zip** for 64-bit Windows 8 / Windows 2012 hosts
- **Windows_2016_x64.zip** for Windows 2016 / Windows 10 hosts
- **Windows_2019_x64.zip** for Windows 2019 hosts

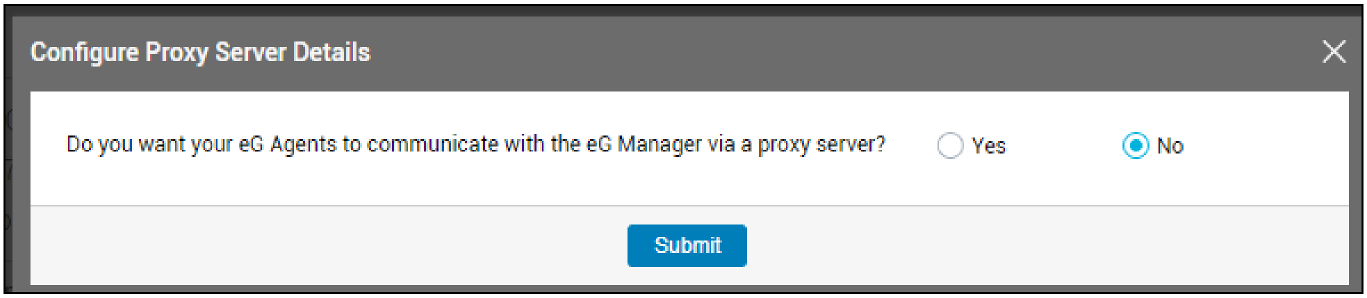
5. Copy the downloaded packages to the <EG_ MANAGER_ INSTALL_ DIR>\agents\Universal\Latest folder.

The tenant can now proceed to install the eG agent using the procedure discussed hereunder:

Note:

Before installing an eG agent on a Windows 2008 host, make sure that the VC 2008 (or above) runtime engine exists on that host. If not, then download and install the same. For use on a 32-bit Windows 2008 host, you need to download the 32-bit VC 2008 (or above) runtime engine from the URL, *http://www.microsoft.com/download/en/details.aspx?id=29*. Prior to installing the eG agent on a 64-bit Windows 2008 host, download and install the 64-bit VC 2008 (or above) runtime engine from the URL, *http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=15336*.

1. Using a browser, connect to the URL of the eG management console.
2. Login to the eG management console using the credentials you used (corporate email ID and password) to register with eG Enterprise for SaaS.
3. Click the ⬇ icon in the top, right corner of the page that appears to download eG agents.
4. Doing so will invoke Figure 3.18, where you need to indicate if the eG agent you are downloading should communicate with the eG manager via a proxy server. If not, then pick the **No** option. If a proxy server is to be used for agent-manager communication, then select the **Yes** option.

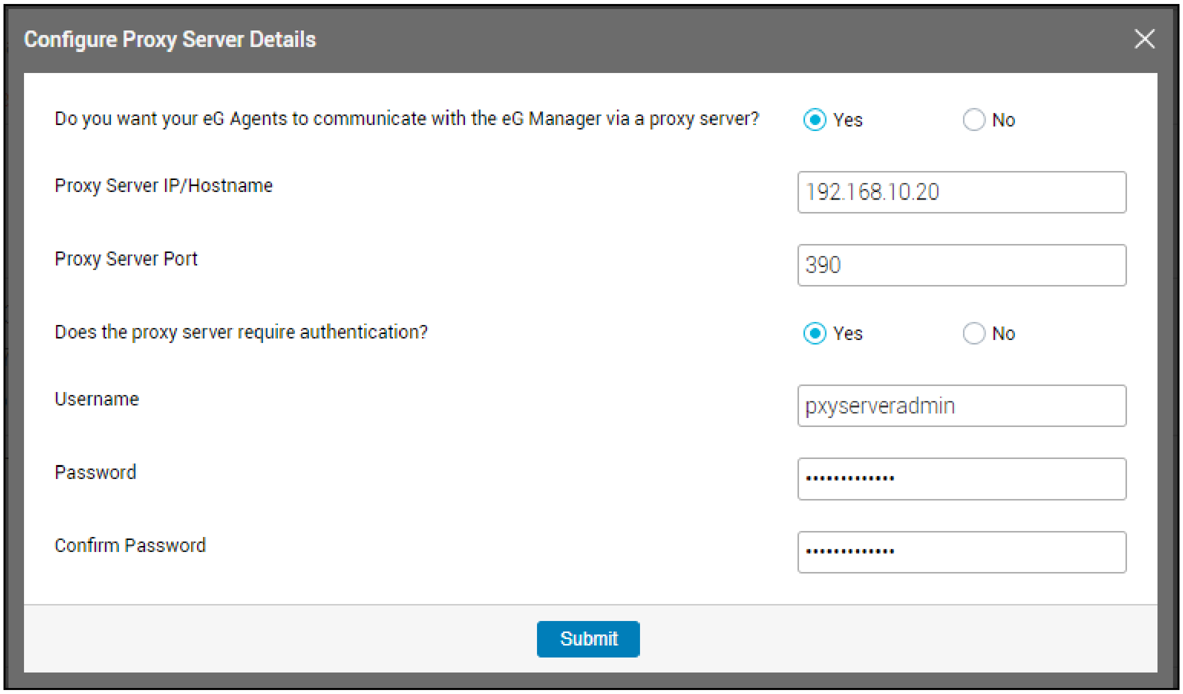


Configure Proxy Server Details

Do you want your eG Agents to communicate with the eG Manager via a proxy server? ○ Yes ● No

Figure 3.18: Indicating whether/not the eG agent being downloaded should communicate with the eG manager

5. If the **Yes** option is chosen in Figure 3.18, then Figure 3.19 will appear. Here, you need to provide the details of the proxy server used for agent-manager communication.



Configure Proxy Server Details

Do you want your eG Agents to communicate with the eG Manager via a proxy server? ● Yes ○ No

Proxy Server IP/Hostname: 192.168.10.20

Proxy Server Port: 390

Does the proxy server require authentication? ● Yes ○ No

Username: pxyserveradmin

Password: •••••••••••••

Confirm Password: •••••••••••••

Figure 3.19: Configuring agent-manager communication via a proxy server

6. Specify the following in Figure 3.19:

- **Proxy Server IP/Hostname**: Mention the IP address/hostname of the proxy server used for agent-manager communication.
- **Proxy Server Port**: Specify the port number at which the proxy server listens.
- **Does the proxy server require authentication?**: Indicate whether/not the proxy server requires authentication. Select the **No** option if authentication is required, and **Yes** if it is.

- **Username, Password, and Confirm Password**: If the proxy server requires authentication, then provide the credentials of a valid proxy server user against the **Username** and **Password** text boxes. Confirm the password by retyping it in the **Confirm Password** text box.
- Finally, click the **Submit** button to confirm the proxy server specifications and proceed with the downloading of the eG agent.

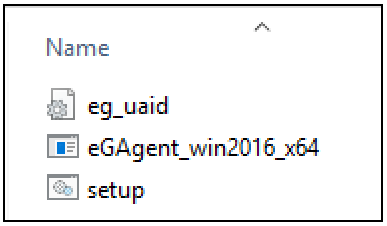
7. Figure 3.20 will appear. By default, Figure 3.20 lists the 'internal agent packages' that have been uploaded to the eG manager - i.e., agent packages to be used for monitoring components in an agent-based manner. If you want to deploy a remote agent, click the **agentless monitoring** link in Figure 3.20. Likewise, to deploy an external agent, click the **external monitoring** link in the page.

Figure 3.20: eG's internal agent packages available for download from the eG manager console

Note:

Though the eG management console lists the packages meant for agent-less, agent-based, and external monitoring in separate pages, the procedure to download and install these packages remains the same across monitoring approaches.

8. To download an agent package for Windows, click on the package that corresponds to the version/flavor of Windows that the target Windows host is using. For instance, to install an agent on a Windows 2016 server, download the Windows_2016_x64.zip file by clicking on it.
9. If the host to which you have downloaded the package is the target Windows host for agent installation, then login to that Windows host. On the other hand, if you want to install the eG agent on a host different from the one on which the package has been downloaded, then first copy the agent package to any location on the target Windows host. Then, login to that host.
10. Open the folder to which the zip file has been copied/downloaded, and extract the contents of the file. The extracted contents will be as depicted by Figure 3.21.



Name

eg_uaid

eGAgent_win2016_x64

setup

Figure 3.21: The contents extracted from the agent package zip file

11. As is evident from Figure 3.21, the following files are extracted:

    - **eGAgent_<winflavor>_<win_bitrate>**: This is the eG agent installable (exe) that corresponds to the version/flavor/bit rate of the target Windows host.
    - **setup.bat**: This is the batch file that drives the silent installation of the eG agent. Running setup invokes the eG agent executable and silently installs the agent on the target host.
    - **eg_uaid**: In a multi-tenant setup, once a tenant - eg., a user representing a customer / a department / a domain - registers with eG Enterprise to use its monitoring services, eG automatically generates a unique UAID and assigns the same to that tenant. If that tenant later logs into the eG management console using the registered credentials (email ID and password) and downloads the agents, each agent so downloaded is automatically tagged with that UAID. The downloaded agents, once installed and configured, will automatically start discovering applications on their respective hosts. eG Enterprise auto-manages the discovered applications and auto-assigns them to the user who has the same UAID as the eG agent that discovered these applications. The eg_uaid file contains the UAID of the tenant who downloaded agent packages from the eG management console; this is the same UAID that will be assigned to each agent installed by that tenant.

12. Next, to install the eG agent on a Windows host silently, open Windows explorer and go to the folder to which the contents of the zip file have been extracted.

13. Right-click on the **setup.bat** file in that folder, and click the **Run as administrator** option in the shortcut menu that pops up.

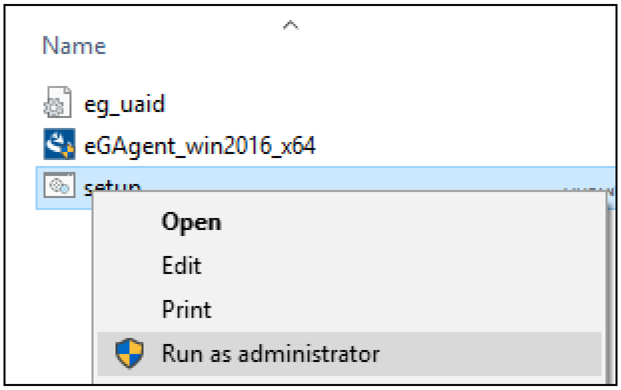


Figure 3.22: Running the setup.bat file as administrator

14. This will automatically install an eG agent on the target Windows host. This eG agent will automatically report metrics to the eG manager from which the agent package was downloaded. Also, the hostname of such an agent is automatically set as its nick name.

In a multi-tenant setup, a hostname may not be unique across tenant environments. To avoid nick name duplication, eG Enterprise automatically employs the following algorithm when assigning nick names:

- At the time of setting the hostname of an agent host as its nick name, eG first checks if that hostname has already been assigned to any existing agent.
- If it finds that the hostname has already been taken, then it will attempt to assign the FQDN - the fully qualified domain name - of the agent host as the nick name.
- In the process, if eG finds that the FQDN is also in use, then it will break-down the FQDN into smaller strings, and try to assign each of these strings, one after another, to the agent.
- If all these FQDN strings have already been assigned to other agents, then the eG agent will suffix the hostname of the agent host with the number 0, and try to assign this as the nick name of the eG agent. For instance, if the hostname of the eG agent host is winpc, then the nick name assigned to that agent will be winpc0.
- If this nick name is also taken, then eG will increment the number 0, which suffixes the hostname, by 1, and will try to assign the resultant string to the eG agent,. This way, eG will keep incrementing the number suffix until an unused string is found. Such a string will finally be assigned to the agent as its nick name.

  In a SaaS deployment, if a tenant manually adds components to be monitored by an eG agent, then that agent's nick name should only be added as the nick name of each of those components.

Note:

If you are downloading an agent for installation on an imaging system (e.g. for Citrix Provisioning services), or on a snapshot (for Citrix Machine Creation Services), or on a VM template for virtual servers, then, make sure you first enable the **Installation on a golden image / VM template** flag in Figure 3.20 and then proceed with the downloading. If this is done, then after the agent so downloaded is installed, setup will stop that agent. Also, setup will auto-delete the eg_nick.ini file of that agent, so that no nick name is assigned to that agent.

On the other hand, if you download and install an agent on an imaging system / snapshot / VM template WITHOUT ENABLING the **Installation on a golden image / VM template** flag in Figure 3.20, then the installation will automatically start the agent and assign the hostname of the system as the nick name automatically. In such a case, you need to do the following:

- On the snapshot / golden image / master VM, open the eg_nick.ini file in the <EG_AGENT_INSTALL_DIR>\agent\config directory.

- Check to see if the Nick parameter in that file is set to any value. If this parameter has no value, it implies that no nick name was set for the eG agent on that snapshot / golden image / master VM. On the other hand, if the Nick parameter has a value, it indicates that a nick name was set for the eG agent. In this case, make sure that you delete the eg_nick.ini file on the snapshot / golden image / master VM before you proceed further.
- Also, stop the eG agent.

Note:

- It is not necessary to reboot a server after installing the eG agent on Windows.
- If certain supported Microsoft operating systems and applications are to be monitored in an agentless manner, then, in order to enable the eG remote agent to collect measurements from these applications using Perfmon counters, the following are required:
  - A remote agent can monitor a Windows environment only if it is installed with a domain administrator's privileges.
  - NetBIOS should be enabled on the target host.
  - PerfMon should have at least READ access to the **Perflib\LanguageID** subkey on the remote computer (which allows external access to PerfMon). The Perflib\LanguageID subkey is located in the following Registry path: HKEY_ LOCAL_ MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Perflib\LanguageID. The LanguageID is a numeric code for the spoken language of the installed operating system. A computer with a LanguageID of 009 (the English LanguageID) has the following **Perflib\Language** subkey: **HKEY_ LOCAL_ MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Perflib\009**.
  - The Disk Performance Statistics Driver (diskperf) should exist on the target computer; allow READ access explicitly to the user account for the following registry key and all subkeys: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Diskperf**.

Note:

- The monitored computer should be able to connect to IPC$. The following registry entry enables connecting to IPC$:
  - Hive: **HKEY_LOCAL_MACHINE\SYSTEM**
  - Key: **CurrentControlSet\Services\LanmanServer\Parameters**
  - Name: **AutoShareWks**

  - Type: **REG_DWORD**
  - Value: **1**

- At least READ access should be granted to the following registry subkey (allowing it to remotely connect to the Windows registry): **HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg**. This permission determines who can remotely connect to a registry. If this subkey does not exist, all users can remotely connect to the registry. To remotely connect to a registry, a user must have at least READ access to the winreg subkey on the target computer.
- At least READ access should be granted to the following registry keys on the remote computer:
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Perflib
- To monitor Windows 2000 and Windows XP, the user name must have access granted by the following group policies:
  - Profile single process
  - Profile system performance

  Both group policies are security settings that you can set from the **Local Policies** => **User Rights** option in the **Administrative Tools** of the **Control Panel**.
- To monitor Windows XP, if the systemroot is on an NTFS partition, the user name must have at least READ access to the following two files:
  - %SystemRoot%\System32\Perfc009.dat
  - %SystemRoot%\System32\Perfh009.dat

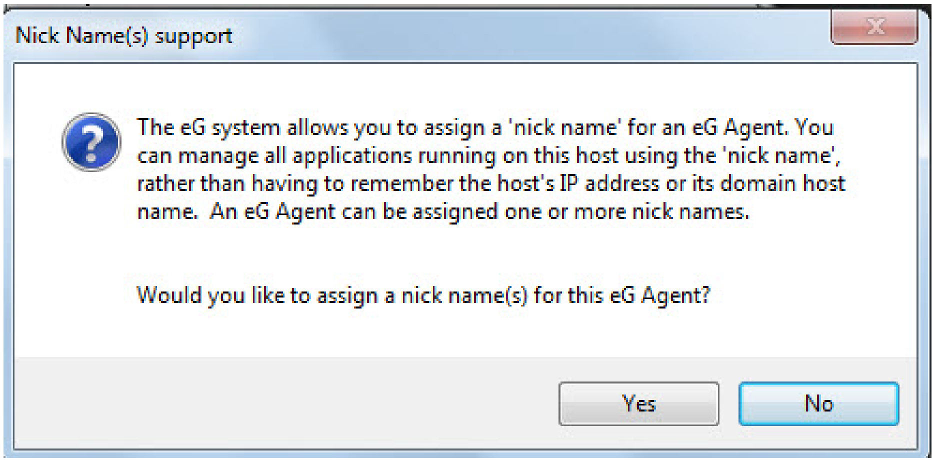
3.3 Installing an eG Agent on a Citrix PVS Gold Image

A Golden Image is a template for a virtual machine (VM), virtual desktop, server or hard disk drive. A Golden Image may also be referred to as a clone image, master image or base image.

When preparing a golden image of a Citrix Xenpp server using Citrix PVS, you can install the eG agent as part of the golden image, so that every Windows VM / virtual desktop that is created from that image automatically includes a fully functional eG agent.

For this purpose, all you need to do is install the eG agent on the new Windows VM to be used as the golden image for PVS. The steps for installation are the same as that of any regular Windows agent. Refer Section **3.2.1** for the detailed installation and configuration steps.

Typically, when installing and configuring any eG agent, setup will request you to confirm whether/not you want to assign a nick name for that agent (see Figure 1).



Nick Name(s) support

The eG system allows you to assign a 'nick name' for an eG Agent. You can manage all applications running on this host using the 'nick name', rather than having to remember the host's IP address or its domain host name. An eG Agent can be assigned one or more nick names.

Would you like to assign a nick name(s) for this eG Agent?

Figure 3.23: Setup requesting the user's confirmation to assign a nick name for the eG agent

When configuring an eG agent on a golden image for PVS, make sure that you do not assign any nick name for the agent. To this effect, click the **No** button at this prompt.

3.3.1 Silent Mode Installation of the eG Agent on Windows

To install an eG agent on Windows in the silent mode, the following broad steps need to be followed:

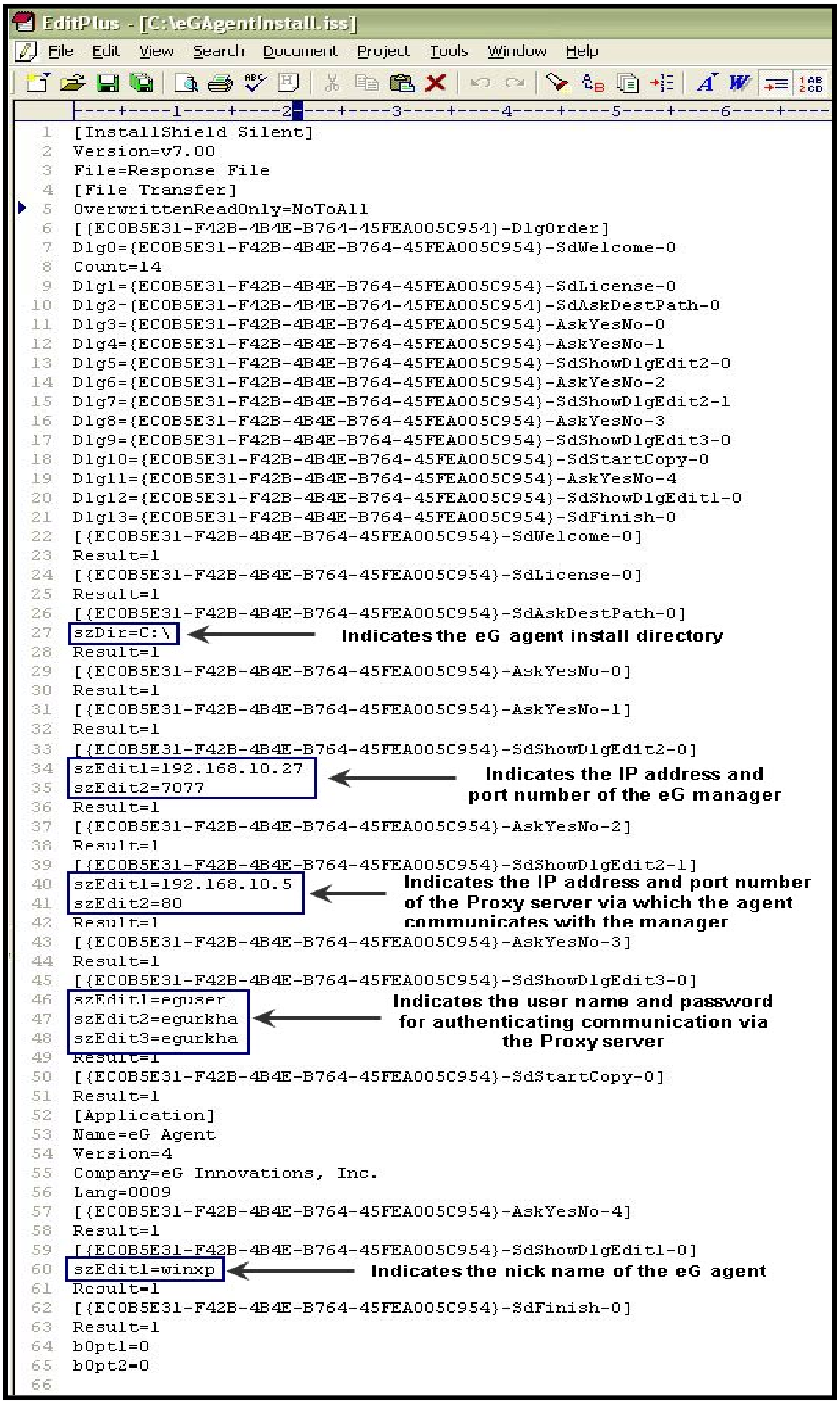
- Create the silent mode script for the agent installation;
- Use the script along with the eG agent executable to install agents on other hosts

Each of these steps has been explained in-depth in the sections below.

3.3.1.1 Creating the Silent Mode Script for Agent Installation

The first step towards installing the eG agent in the silent mode is to create the silent mode script for an agent installation. The script file will carry the extension **.iss**, and will contain the inputs provided by the administrator while installing the eG agent in the normal mode. Before attempting script creation, ensure that the **eGAgent_<OS>.exe** is available on the local host. Then, to create the script, do the following:

1. From the command prompt, switch to the directory in which the **eGAgent_<OS>.exe** resides.
2. Next, issue the following command: **eGAgent_<OS>.exe -a -r /f1"<Full path to the script file >"**. For example, to create a script file named **eGAgent_<OS>.iss** in the **c:\script** directory, the command should be: **eGAgent_<OS>.exe -a -r /f1"c:\script\eGAgent.iss"**.
3. The *Normal mode* agent installation will then begin. The inputs supplied during the normal mode will automatically be saved in the **iss** file that was created in step 2. Refer to the Section **3.2.1** topic for the detailed procedure for installing an eG agent on Windows in the normal mode.
4. Figure 3.24 depicts a sample script file and explains its key components.


EditPlus - [C:\eGAgentInstall.iss]
File Edit View Search Document Project Tools Window Help

```
[InstallShield Silent]
Version=v7.00
File=Response File
[File Transfer]
OverwrittenReadOnly=NoToAll
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-DlgOrder]
Dlg0={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdWelcome-0
Count=14
Dlg1={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdLicense-0
Dlg2={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdAskDestPath-0
Dlg3={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-0
Dlg4={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-1
Dlg5={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdShowDlgEdit2-0
Dlg6={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-2
Dlg7={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdShowDlgEdit2-1
Dlg8={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-3
Dlg9={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdShowDlgEdit3-0
Dlg10={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdStartCopy-0
Dlg11={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-4
Dlg12={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdShowDlgEdit1-0
Dlg13={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdFinish-0
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdWelcome-0]
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdLicense-0]
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdAskDestPath-0]
szDir=C:\
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-0]
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-1]
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdShowDlgEdit2-0]
szEdit1=192.168.10.27
szEdit2=7077
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-2]
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdShowDlgEdit2-1]
szEdit1=192.168.10.5
szEdit2=80
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-3]
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdShowDlgEdit3-0]
szEdit1=eguser
szEdit2=egurkha
szEdit3=egurkha
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdStartCopy-0]
Result=1
[Application]
Name=eG Agent
Version=4
Company=eG Innovations, Inc.
Lang=0009
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-4]
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdShowDlgEdit1-0]
szEdit1=winxp
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdFinish-0]
Result=1
bOpt1=0
bOpt2=0
```

Indicates the eG agent install directory

Indicates the IP address and port number of the eG manager

Indicates the IP address and port number of the Proxy server via which the agent communicates with the manager

Indicates the user name and password for authenticating communication via the Proxy server

Indicates the nick name of the eG agent

Figure 3.24: Contents of the script file

3.3.1.2 Using the Silent Mode Script to Perform Subsequent Agent Installations

Once the silent mode script is created, you can use this script to perform subsequent agent installations. Before attempting to *reuse* a script file, you might have to decide on the following:

a. Whether the target script file can be used as is;

b. Whether the target script file can be used after minor changes;

c. Whether a new script file is to be generated

This decision is typically based on the configuration you desire for the eG agent that you are about to install. Moreover, the process of installation may slightly vary depending upon this decision. The sections that follow discuss each decision and how it impacts the silent mode installation process.

3.3.1.2.1 Silent Mode Installation of an eG Agent without any Changes to the Script File

Sometimes, for some reason, you might just want to 'reinstall' an eG agent on a host where a script file pre-exists; the configuration of the old agent and the intended configuration of the new agent may be the same. In this case therefore, you can opt for (a) above - i.e., proceed to use a script file, without any changes, for agent installation in the silent mode. The procedure to reinstall an eG agent in the silent mode has been discussed below:

1. Uninstall the eG agent on the host (if it already exists).
2. Ensure that the **eGAgent_<OS>.exe** is present on the host, go to the command prompt, and then switch to the directory containing the agent executable.
3. From that directory, execute the following command to install the eG agent in the silent mode: **eGAgent_<OS>.exe -a -s /f1"<Full path to the script file containing the inputs for the installation>"**. In other words, to extract installation inputs from the **eGAgent.iss** file that was created in our example above, the command will be: **eGAgent_ <OS>.exe -a -s /f1"c:\script\eGAgent.iss"**.
4. The eG agent installation will then begin and proceed in the silent mode. Setup will extract the required inputs from the **iss** file specified in step 3 above and perform the installation automatically, requiring no user intervention of any kind.

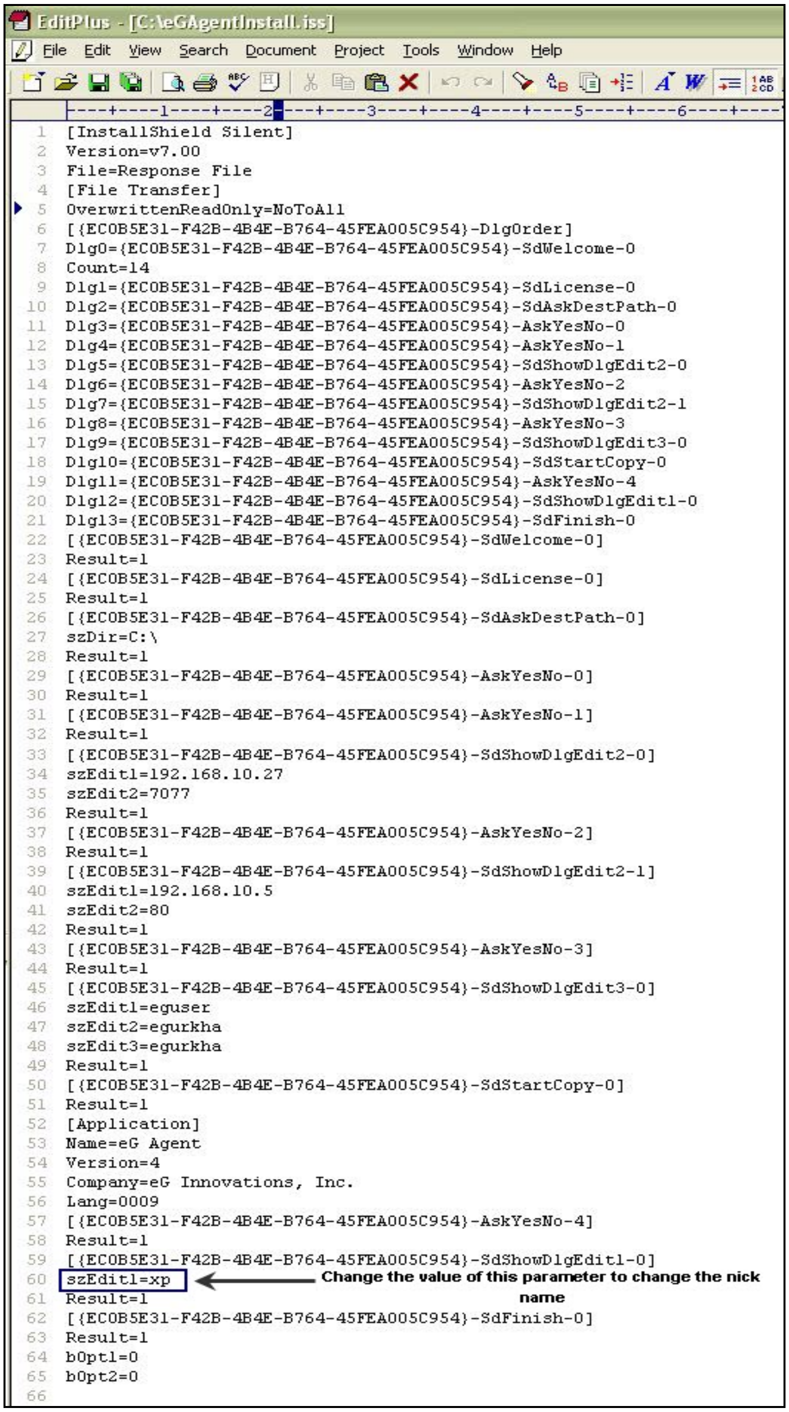
3.3.1.2.2 Silent Mode Installation of an eG Agent after making Minor Changes to the Script File

Note that all the eG agents deployed in a target environment will not possess the same configuration - at least, the nick name will be different for each agent. Since the **.iss** file holds a particular agent's configuration, you cannot use the same script file, as is, for installing eG agents on multiple hosts. In such cases, besides the mandatory nick name change, a few/more minor changes to the script file may become necessary. The other changes that qualify as 'minor' changes have been listed below:

- The manager IP and/or port
- The agent install directory
- The Proxy server IP and/or port
- The user name and/or password for authenticating the Proxy server communication

To make these changes to a script file and then use it to install an agent in the silent mode, follow the steps given below:

1. Copy the script file to the target host.
2. Open the script file in an Editor.
3. Change the values of the required configuration parameters. For instance, to assign a different nick name to the new agent, search the script file for the parameter, **szEdit1**; then, change the value of the last occurrence of this parameter to change the nick name.



```
[InstallShield Silent]
Version=v7.00
File=Response File
[File Transfer]
OverwrittenReadOnly=NoToAll
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-DlgOrder]
Dlg0={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdWelcome-0
Count=14
Dlg1={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdLicense-0
Dlg2={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdAskDestPath-0
Dlg3={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-0
Dlg4={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-1
Dlg5={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdShowDlgEdit2-0
Dlg6={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-2
Dlg7={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdShowDlgEdit2-1
Dlg8={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-3
Dlg9={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdShowDlgEdit3-0
Dlg10={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdStartCopy-0
Dlg11={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-4
Dlg12={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdShowDlgEdit1-0
Dlg13={EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdFinish-0
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdWelcome-0]
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdLicense-0]
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdAskDestPath-0]
szDir=C:\
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-0]
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-1]
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdShowDlgEdit2-0]
szEdit1=192.168.10.27
szEdit2=7077
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-2]
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdShowDlgEdit2-1]
szEdit1=192.168.10.5
szEdit2=80
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-3]
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdShowDlgEdit3-0]
szEdit1=eguser
szEdit2=egurkha
szEdit3=egurkha
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdStartCopy-0]
Result=1
[Application]
Name=eG Agent
Version=4
Company=eG Innovations, Inc.
Lang=0009
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-AskYesNo-4]
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdShowDlgEdit1-0]
szEdit1=xp
Result=1
[{EC0B5E31-F42B-4B4E-B764-45FEA005C954}-SdFinish-0]
Result=1
bOpt1=0
bOpt2=0
```

Change the value of this parameter to change the nick name

Figure 3.25: Changing the nick name of an eG agent

4. Finally, save the file.

5. Once this is done, you can proceed to use the updated script file to install the eG agent on a host. The procedure for installation is the same as discussed in Section **3.3.1.2.1**.

3.3.1.2.3 Silent Mode Installation of an eG Agent Using a Script File that is Newly Generated

Sometimes, the configuration you desire for the agent to be installed could be vastly different from the script file contents. This is possible in the following cases:

- If an SSL-enabled agent is to be installed, but the script file is for a non-SSL agent, or vice-versa;
- If the agent to be installed needs to communicate via a Proxy server, but the script file does not consist of a Proxy server configuration, or vice-versa;
- If the agent to be installed communicates via a Proxy server with authentication, but the script file does not consist of any authentication information, or vice-versa;

In these cases, it is recommended that you generate a new script file that suits your specific purpose, using the procedure discussed in Section **3.3.1.1** , and then use it to install the eG agent. The procedure for installation is the same as discussed in Section **3.3.1.2.1** above.

3.3.1.3 Uninstalling the eG Agent on Windows in the Silent Mode

Like installation, agent uninstallation might also need to be performed simultaneously, on multiple agent hosts, with little to no human interference. To achieve this, follow the steps below:

1. First, ensure that an eG agent is operational on the target host.
2. Next, make sure that the **eGAgent_<OS>.exe** is available on the local host.
3. Then, from the command prompt, switch to the directory in which the **eGAgent_<OS>.exe** resides.
4. Next, issue the following command to create a script file for the uninstallation:

   eGAgent_<OS>.exe –a –r /f1"<Full path to the script file >"

5. For example, to create a script file named **eGAgent_<OS>.iss** in the **c:\script** directory, the command should be: **eGAgent_<OS>.exe –a –r /f1"c:\script\eGAgent.iss"**.
6. The *Normal mode* agent uninstallation will then begin. The inputs supplied during the normal mode will automatically be saved in the **iss** file that was created in step 4. Refer to the Section **3.3.10** topic for the detailed procedure for uninstalling an eG agent on Windows in the normal mode.
7. Once the script is created, you can use the same script to uninstall agents in the silent mode, from multiple hosts. For this, do the following:

- Ensure that the script file to be used for the silent mode uninstallation process is also copied to the host.
- Next, go to the command prompt, and then switch to the directory containing the agent executable.
- From that directory, execute the following command to install the eG agent in the silent mode: **eGAgent_<OS>.exe –a –s /f1"<Full path to the script file containing the inputs for the installation>"**. In other words, to extract installation inputs from the **eGAgent.iss** file that was created in our example above (see step 4), the command will be: **eGAgent_<OS>.exe -a –s /f1"c:\script\eGAgent.iss"**.
- The eG agent uninstallation will then begin and proceed in the silent mode. Setup will extract the required inputs from the **iss** file and perform the uninstallation automatically, requiring no user intervention of any kind.

3.3.2 Enabling the eG Agent to Allow Trusted Certificates

If you have configured the eG agent (during agent setup) to allow trusted SSL certificates alone, you need to follow the broad steps below to ensure the same:

- Extract the certificate from the **keystore** file and export it to a **certificate** file. The steps for achieving this are explained in the Section **3.3.2.1** topic.
- Import the SSL certificate into the JRE of the eG agent. The details on this are discussed in the Section **3.3.2.2** topic. The key limitation of this approach is that, whenever the JRE is upgraded, the SSL certificates in its trust store get overwritten. This can disrupt eG agent- manager communication post the JRE upgrade. To avoid this, it is recommended that you import the SSL certificate into the Windows trust store, and not the JRE's trust store. The procedure for importing an SSL certificate into the Windows trust store of the eG agent host has been discussed in detail in Section **3.3.2.3**.

3.3.2.1 Extracting the SSL Certificate to a Certificate File

To achieve this, do the following

1. Login to the eG manager.
2. Set the **JAVA_HOME** environment variable to point to the Java installation directory.
3. Then, go to the command prompt.
4. Execute the following command:

cd %JAVA_HOME%\bin

keytool -export -alias ***egitlab1*** *-keystore* ***<filename>.keystore*** *–storepass* ***mykey*** *-keypass* ***mykey*** *-file* ***C:\tmp\eGCert.cer***

The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

- **-alias** : the alias name of the certificate being extracted; **make sure that you provide the same alias name that you provided while generating the keystore file** (see Section **2.8.0.2** or Section **2.8.0.6**). If you are extracting the SSL certificate from the default keystore that is bundled with the eG manager, then first determine the alias name using which the keystore file was created. For this, from the <eg_Install_dir>\java\jdk\bin directory, run the following command:

  keytool –list –v –keystore egmanager.bin

  This command will prompt for the keystore passphrase. Type *eginnovations* and press **Enter**. This will provide the details of the default keystore. From these details, you can infer the **Aliasname**.

- **-keypass** : the password used to protect the key that was generated; make sure that you provide the same password that you provided while generating the keystore file (see Section **2.8.0.2** or Section **2.8.0.6**). Also, note that **-storepass** and **-keypass** should be the same. If you are extracting the SSL certificate from the default keystore that is bundled with the eG manager, then the **–storepass** and **–keypass** should be *eginnovations*.
- **-keystore** : Provide the name of the *keystore* file in which the key has been stored; **specify the same file name that you used to store the key** (see Section **2.8.0.2** or Section **2.8.0.6**).
- **-file** : Specify the full path to and the name of the certificate file (**.cer**) to which the certificate has to be exported

5. Once the **keytool** command successfully executes, the certificate file will be created.
6. Finally, copy the certificate file from the eG manager to any location (say, *C:\tmp*) on the eG agent host.

3.3.2.2 Importing the SSL Certificate into the JRE of the eG Agent

To achieve this, do the following:

1. Login to the eG agent host.
2. Open the command prompt and set the path to <EG_INSTALL_DIR>\jre\bin;%path%, using the command:

   set path=<EG_INSTALL_DIR>\jre\bin;%path%

3. Then, using the **keytool** command, import the manager certificate to the JRE of the eG agent. A sample command has been given below:

   keytool -import -file C:\tmp\eGCert.cer -alias egcert -keystore <EG_ INSTALL_ DIR>\jre\lib\security\cacerts

   The parameters expected by this command are:

   - **-alias** : an alias name for the certificate being imported; make sure that you provide the same alias name that you provided while generating the keystore file (see Section **2.8.0.2** or Section **2.8.0.6**, depending upon whether the certificate is a self-signed certificate or a certificate obtained from a valid certificate authority). If you are extracting the SSL certificate from the default keystore that is bundled with the eG manager, then first determine the alias name using which the keystore file was created. For this, from the <EG_INSTALL_ DIR>\java\jdk\bin directory, run the following command:

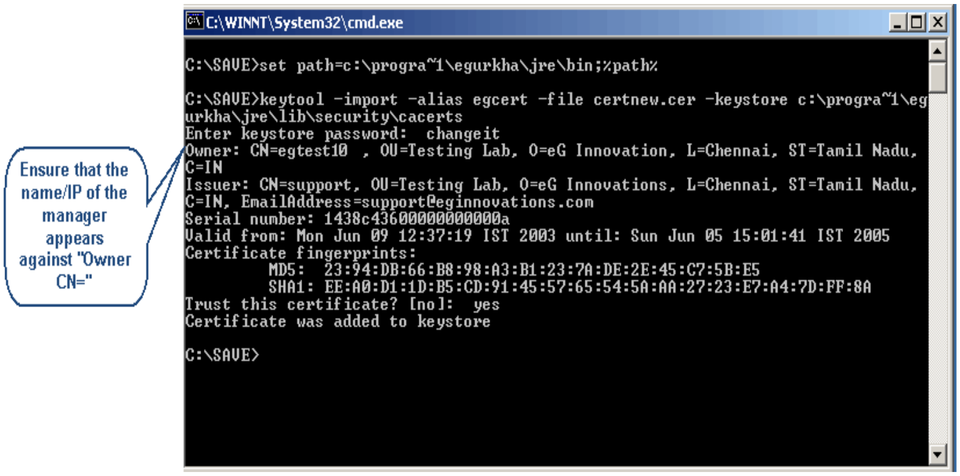
     keytool –list –v –keystore egmanager.bin

     This command will prompt for the keystore passphrase. Type *eginnovations* and press **Enter**. This will provide the details of the default keystore. From these details, you can infer the **Aliasname**.

   - **-file** : the full path to the **.cer** file that was created in the Section **3.3.2.1**.
   - **-keystore** : the keystore file that the JVM used by the agent checks for trusted certificates; specify the same file name that you used to store the key (see Section **2.8.0.2** or Section **2.8.0.6**, depending upon whether the certificate is a self-signed certificate or a certificate obtained from a valid certificate authority). For the default certificate bundled with the eG manager, the **–keystore** should be *egmanager.bin*.
   - This command, upon execution, will request for the keystore password. Provide the same keystore password you provided when generating the keystore file (see Section **2.8.0.2** or Section **2.8.0.6**, as the case may be). For the default certificate bundled with the eG manager, the password should be *eginnovations*.

4. Finally, the command will request your confirmation to make the imported certificate a trusted one. Enter **yes** to trust the certificate.

5. If the processing was successful, then a message stating that the *"Certificate was added to keystore"* will appear. Figure 3.26 depicts the processing explained above.



```
C:\SAVE>set path=c:\progra~1\egurkha\jre\bin;%path%

C:\SAVE>keytool -import -alias egcert -file certnew.cer -keystore c:\progra~1\eg
urkha\jre\lib\security\cacerts
Enter keystore password:  changeit
Owner: CN=egtest10  , OU=Testing Lab, O=eG Innovation, L=Chennai, ST=Tamil Nadu,
C=IN
Issuer: CN=support, OU=Testing Lab, O=eG Innovations, L=Chennai, ST=Tamil Nadu,
C=IN, EmailAddress=support@eginnovations.com
Serial number: 1438c43600000000000a
Valid from: Mon Jun 09 12:37:19 IST 2003 until: Sun Jun 05 15:01:41 IST 2005
Certificate fingerprints:
         MD5:  23:94:DB:66:B8:98:A3:B1:23:7A:DE:2E:45:C7:5B:E5
         SHA1: EE:A0:D1:1D:B5:CD:91:45:57:65:54:5A:AA:27:23:E7:A4:7D:FF:8A
Trust this certificate? [no]:  yes
Certificate was added to keystore

C:\SAVE>
```

Ensure that the name/IP of the manager appears against "Owner CN="

Figure 3.26: The process of importing and trusting the manager certificate

6. Now, start the agent.

3.3.2.3 Importing SSL Certificate into the Windows Trust Store of the eG Agent Host

To import the eG manager's SSL certificate into the Windows Trust Store of the eG agent host, follow the steps discussed below:

1. Login to the eG agent host.

2. Using Windows Explorer, navigate to the folder containing the SSL certificate file of the eG manager.

3. Right-click on the certificate file within that folder and select the Install Certificate option from the shortcut menu that pops out (see Figure 3.27).

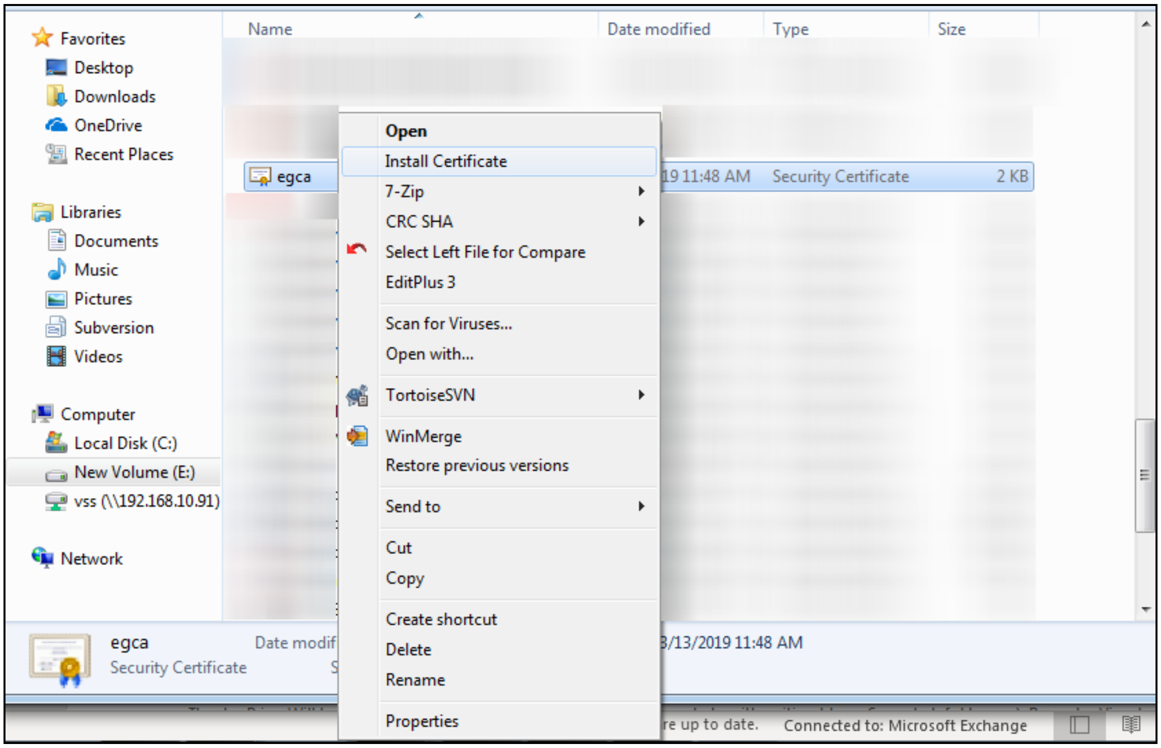
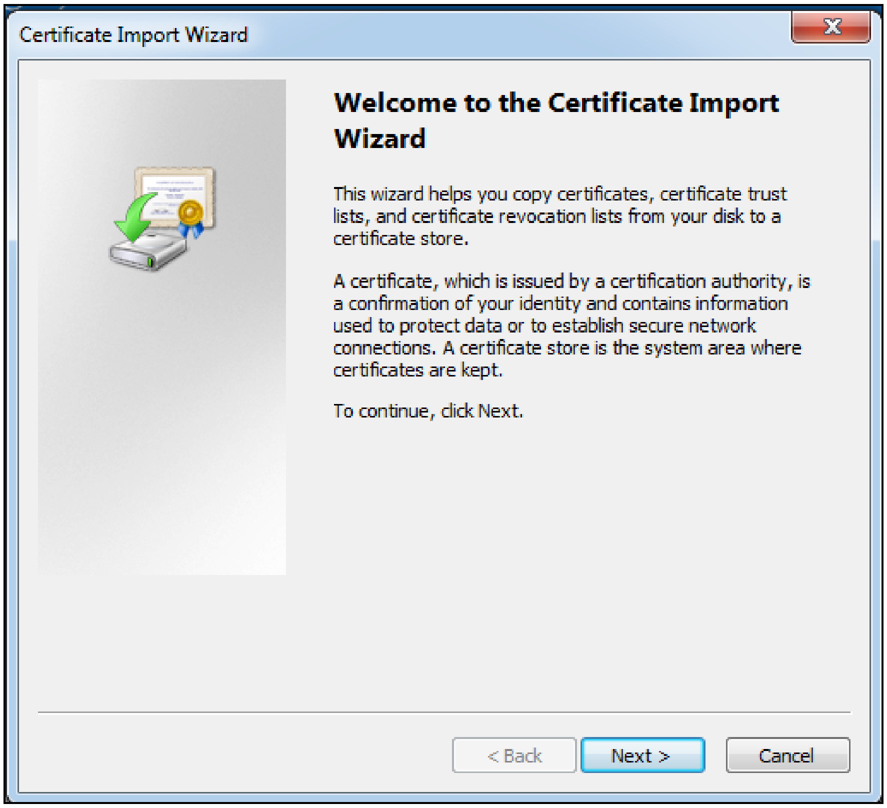


Figure 3.27: Selecting to install the eG manager's SSL certificate into the eG agent host's Windows trust store

4. Figure 3.28 will then appear. Click the Next button in Figure 3.28 to proceed with the installation.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

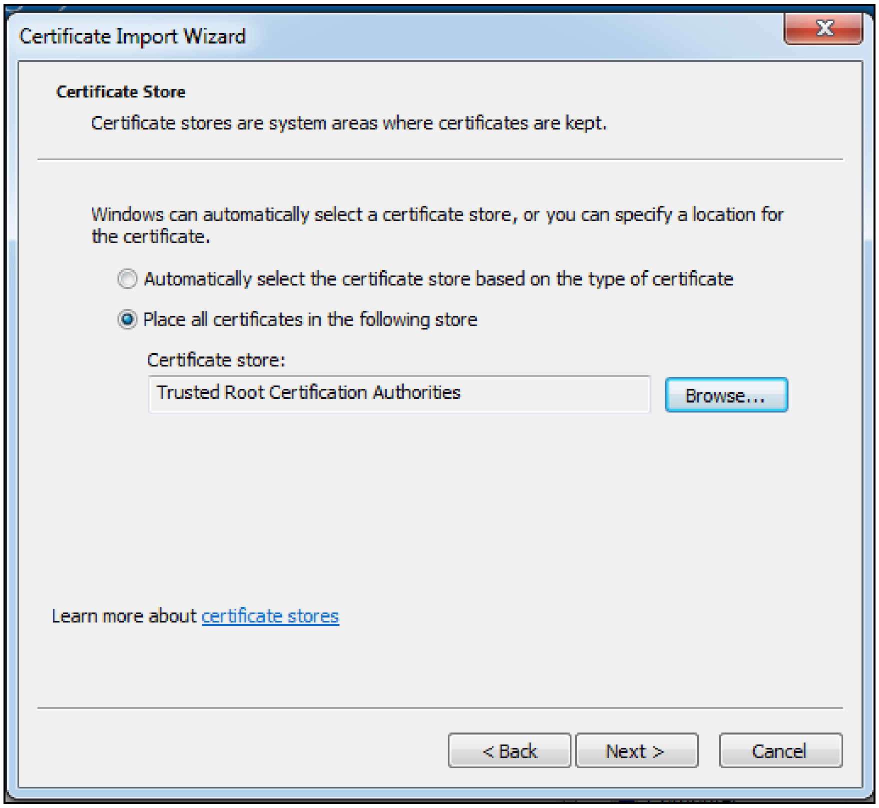
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Figure 3.28: The Welcome screen of the SSL certificate installation wizard

5. When Figure 3.29 appears, select the **Place all certificate files in the following store** option and click the **Browse** button alongside to browse for the Windows trust store. Select the **Trusted Root Certification Authorities** option from the list that appears. Upon selection, the chosen option will appear in Figure 3.29 as the **Certificate store**. Then, click the **Next** button in Figure 3.29 to move to the next step of the installation.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

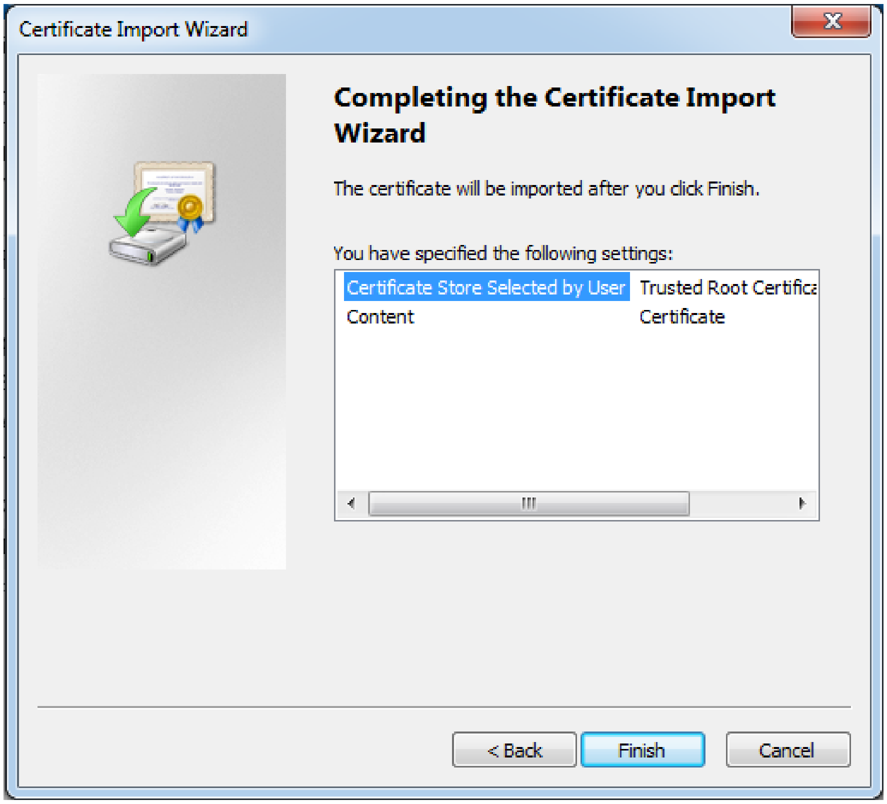
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Figure 3.29: Choosing to place all certificate files in the Windows trust store

6. When Figure 3.30 appears, click **Finish** to end the installation.



Certificate Import Wizard

Completing the Certificate Import Wizard

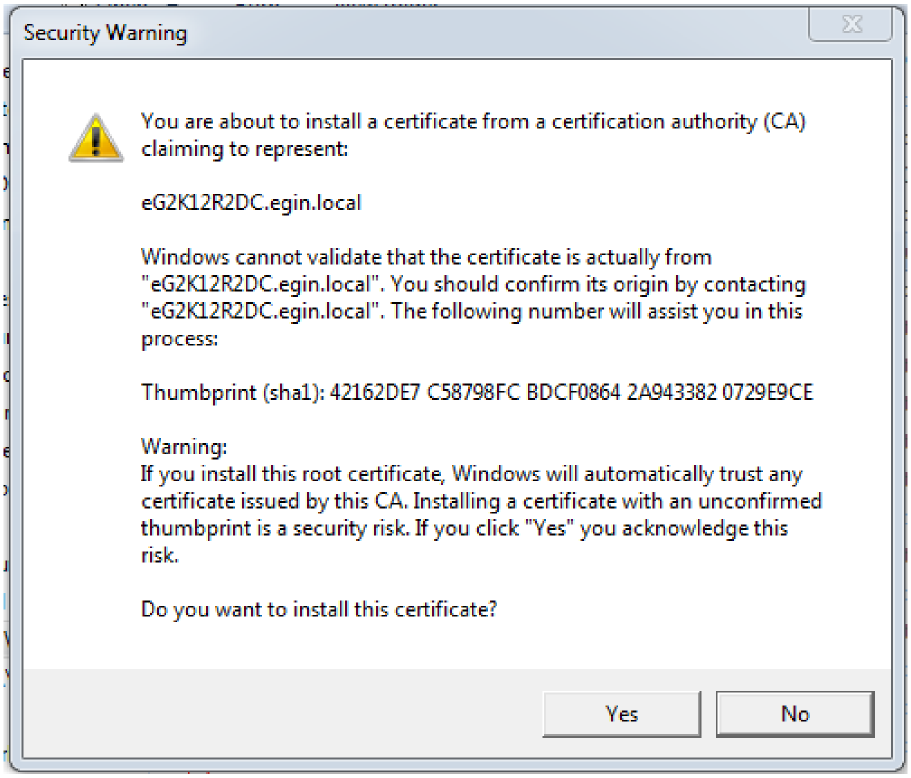
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certifica
Content	Certificate

Figure 3.30: Clicking the Finish button to end the certificate installation process

7. If the SSL certificate being installed is a self-signed certificate or is signed by an internal certificate authority, then Figure 3.31 will appear. Figure 3.31 requests you to confirm the addition of a certificate issued by a non-certified authority to the Windows trust store. Click **Yes** to confirm the addition and to exit the installation wizard.



You are about to install a certificate from a certification authority (CA) claiming to represent:

eG2K12R2DC.egin.local

Windows cannot validate that the certificate is actually from "eG2K12R2DC.egin.local". You should confirm its origin by contacting "eG2K12R2DC.egin.local". The following number will assist you in this process:

Thumbprint (sha1): 42162DE7 C58798FC BDCF0864 2A943382 0729E9CE

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Figure 3.31: A message requesting your confirmation to install a self-signed certificate or a certificate from an internal CA to the Windows trust store

3.3.3 Starting the eG Agent

The eG agent requires 'administrator' privileges to start:

In Windows 2008/Windows 7 systems therefore, follow the Start -> Programs -> eG Monitoring Suite -> eG Agent menu sequence, right-click on the **Start Agent** menu option, and pick the **Run as administrator** option (see Figure 3.32).

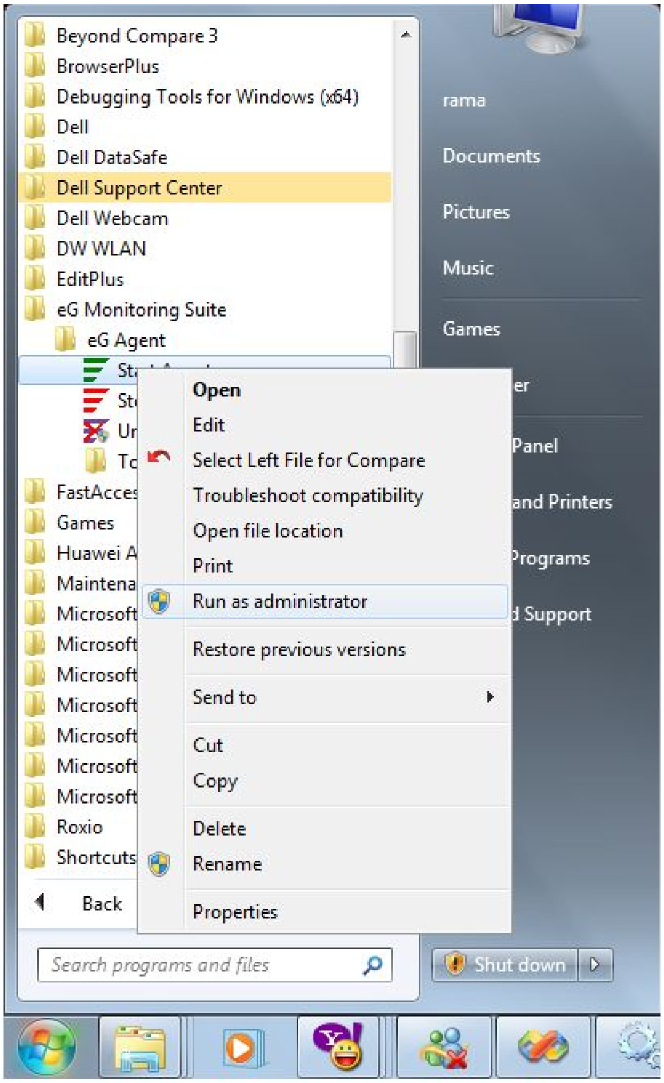


Figure 3.32: Starting an eG agent on Windows 2008

In case of Windows Vista, click on **Start Search** on the task bar of the agent host, right-click on **Command Prompt**, and then select the **Run as administrator** option, as depicted by Figure 3.33. This implies that the command that is issued at the command prompt soon after, will be executed with administrator privileges.

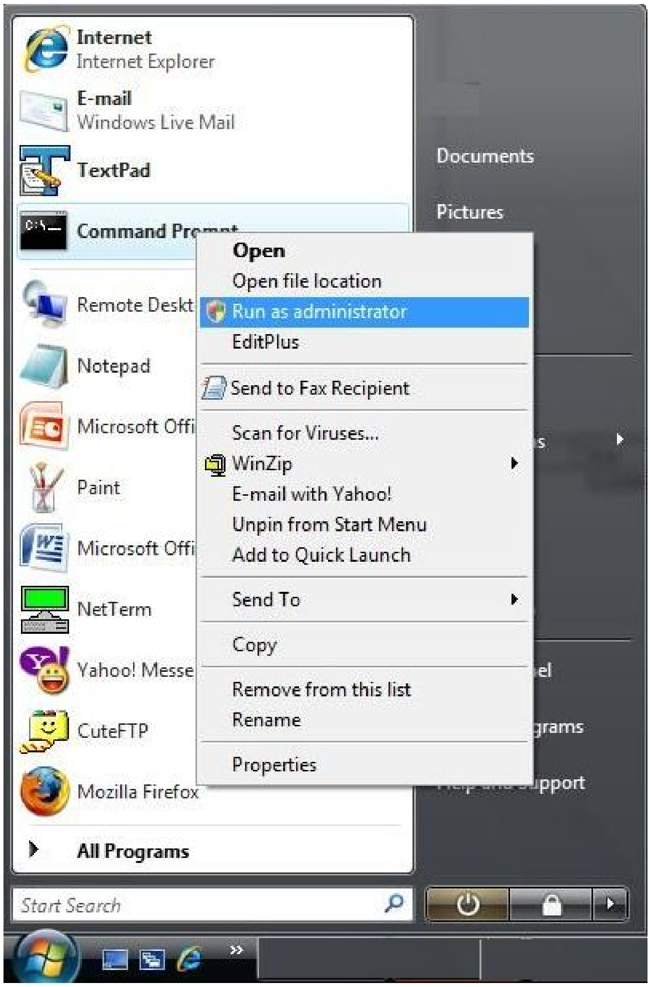
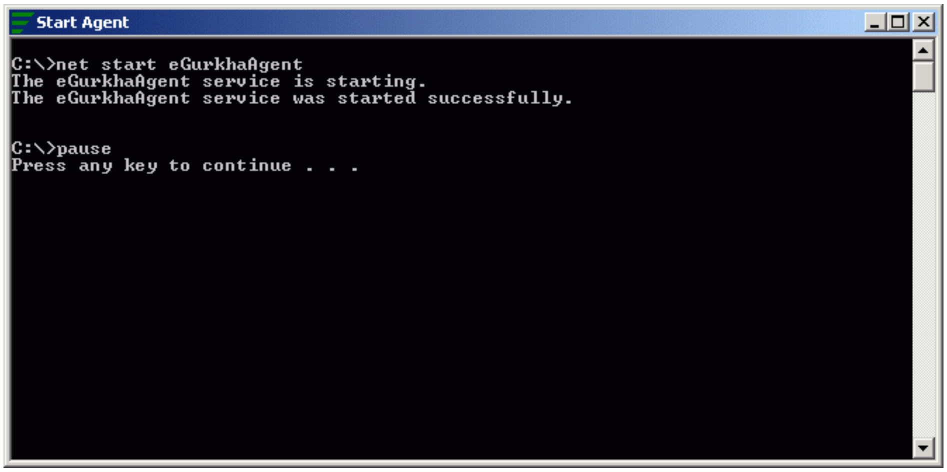


Figure 3.33: Starting the eG agent on Windows Vista

Then, at the command prompt, switch to the <EG_AGENT_INSTALL_DIR>\bin directory and execute the **start_agent** command.

If the agent starts successfully, the following message appears



```
C:\>net start eGurkhaAgent
The eGurkhaAgent service is starting.
The eGurkhaAgent service was started successfully.

C:\>pause
Press any key to continue . . .
```

Figure 3.34: Message indicating that the agent has started successfully.

3.3.3.1 Starting the eG Agent on a Windows 2008/7/Vista System with Italian Locale

Before starting the eG agent deployed on a Windows 2008/7/Vista system with **Italian** language support, you need to ensure that the language settings of the user who is currently logged into that Windows system are copied to the *Local System*, *Local Service*, and *Network Service* accounts (i.e., the **system accounts**). For this purpose, follow the steps discussed below on a Windows 2008/7/Vista system that supports the **Italian** language:

1. Go to the **Pennello di controllo** (the **Control Panel** in English) window and double-click on the **Paese e lingua** (**Region and Language** in English) option therein (as indicated by Figure 3.35).

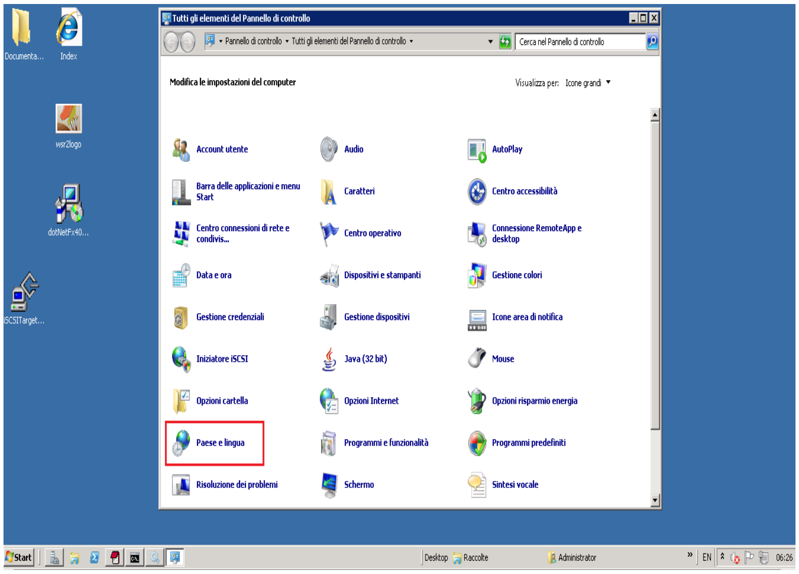
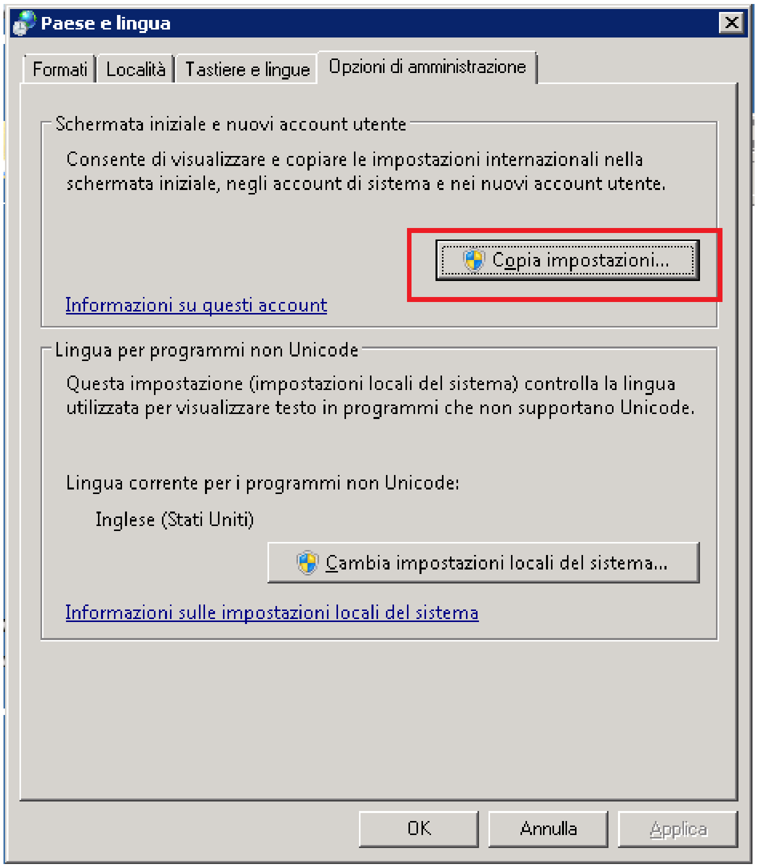


Figure 3.35: The Control Panel

2. Figure 3.36 will then appear. Click on the **Opzioni di amminsrazione** tab page (**Administrative** tab page in English) and click the **Copia impostazioni** (**Copy Settings in English**) button therein.



Schermata iniziale e nuovi account utente

Consente di visualizzare e copiare le impostazioni internazionali nella schermata iniziale, negli account di sistema e nei nuovi account utente.

Lingua per programmi non Unicode

Questa impostazione (impostazioni locali del sistema) controlla la lingua utilizzata per visualizzare testo in programmi che non supportano Unicode.

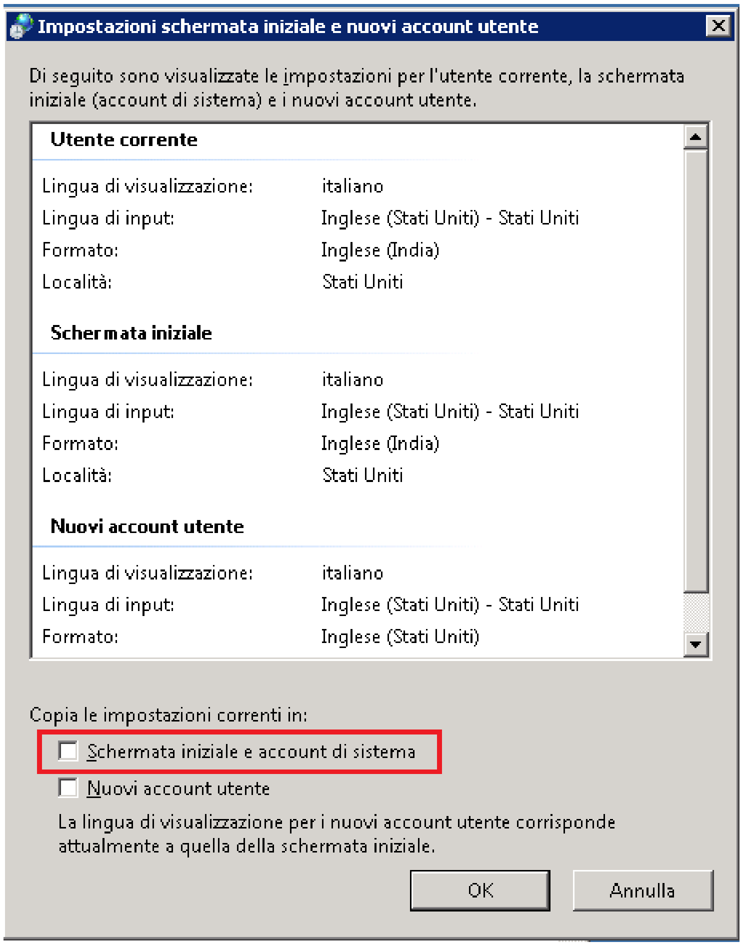
Lingua corrente per i programmi non Unicode:

Inglese (Stati Uniti)

Cambia impostazioni locali del sistema...
Informazioni sulle impostazioni locali del sistema
OK
Annulla
Applica

Figure 3.36: The Administrative tab page

3. When Figure 3.37 appears, select the **Schermata iniziale e account di sistema** check box (i.e., the **Welcome screen and system accounts** check box in English) therein and click the **OK** button to copy the current user's settings to the system accounts.


Impostazioni schermata iniziale e nuovi account utente

Di seguito sono visualizzate le impostazioni per l'utente corrente, la schermata iniziale (account di sistema) e i nuovi account utente.

Utente corrente

Lingua di visualizzazione:	italiano
Lingua di input:	Inglese (Stati Uniti) - Stati Uniti
Formato:	Inglese (India)
Località:	Stati Uniti

Schermata iniziale

Lingua di visualizzazione:	italiano
Lingua di input:	Inglese (Stati Uniti) - Stati Uniti
Formato:	Inglese (India)
Località:	Stati Uniti

Nuovi account utente

Lingua di visualizzazione:	italiano
Lingua di input:	Inglese (Stati Uniti) - Stati Uniti
Formato:	Inglese (Stati Uniti)

Copia le impostazioni correnti in:

☐ Schermata iniziale e account di sistema

☐ Nuovi account utente

La lingua di visualizzazione per i nuovi account utente corrisponde attualmente a quella della schermata iniziale.

Figure 3.37: Copying the current user’s settings to the system accounts

3.3.4 The eG Agent Services

The following services are started when the eG agent is installed. The services are:

- eGurkhaAgent (core agent process)
- eGAgentMon (agent recovery process)

If the status corresponding to the eGurkhaAgent service shows “Started”, then it implies that the agent has been started successfully.

3.3.5 Troubleshooting the Failure of the eG Agent

If the eG agent is failed to start, first check the <EG_HOME_DIR>\agent\logs\error_log file to find out the reasons due to which the agent failed to start. In Windows environments, executing the eG agent in the **debugon** mode automatically triggers error logging. The steps involved in this process are detailed below:

1. Stop the eG agent.
2. Run the **debugon.bat** file in the <EG_AGENT_INSTALL_DIR>\lib directory by double-clicking on it.
3. Finally, restart the eG agent.
4. Upon restarting, the following files will be automatically created in the <EG_AGENT_INSTALL_DIR>\agent\logs directory:

   - The **agentout.log** file, which records details of the tests run and measures reported by the agent to the manager
   - The **agenterr.log** and **error_log** files to which the runtime errors encountered by the eG agent are logged
   - The **agentupgrade.log** file which provides the agent upgrade status.

5. The errors (if any) will be logged in the **error_log** file that will be automatically created in the <EG_AGENT_INSTALL_DIR>\agent\logs directory.

You can ‘switch off’ error logging if so required, by running the **debugoff.bat** file in the <EG_AGENT_INSTALL_DIR>\lib directory.

3.3.6 Overheads of the eG Agent on Windows

The resource utilization of an eG agent is dependent on various factors including:

- the number of components that are being monitored by the eG agent;
- the specific component types to be monitored;
- the frequency of monitoring;
- whether the agent is monitoring applications in an agent-based or an agentless manner;

For an **internal** agent monitoring a single application on the server at a 5 minute frequency, the agent typically consumes 0.1-0.3% of CPU. Network traffic generated by the agent is about 0.05 – 0.2 kbps. The size of the agent on disk is about 1 GB. When the agent is started, its memory footprint will be about 10-15 MB additional to that of the Java Virtual Machine. In total, the eG agent process consumes 128 MB of memory.

For an agent that monitors multiple applications on a server, or for an agent that monitors components in an agentless/external manner, the CPU, memory, and network bandwidth usage will be higher.

3.3.7 Increasing the Memory of the eG Agent

The eG agent runs as a Java process. If an eG agent has been deployed on the same host as the eG manager, then 1/4th of the total system memory is the maximum heap memory that can be allocated. For a stand-alone eG agent on the other hand, a maximum of 512 MB of heap memory can be allocated, if it's a 64-bit agent, and 256 MB, if it's a 32-bit agent.

If a large number of components are to be monitored, you may have to allocate more heap memory to the eG agent. In such a case, follow the steps below for a Windows agent:

1. Login to the eG agent host.
2. Edit the **debugon.bat** or **debugoff.bat** file in the <EG_INSTALL_DIR>\lib directory.
3. Look for the entry *-Xmx* in the file. If you do not find it, then, insert an entry of the following format:

   Xmx<Memory_allocation_to_the _eG_agent>M

   For instance, if you want to allocate 8 GB of memory to the eG agent, your –Xmx specification should be as follows:

   Xmx8192M

   On the other hand, if you find the entry in the **debugoff.bat** or **debugon.bat** file (as the case may be), then simply alter the <*Memory_allocation_to_the _eG_agent*> to suit your specific needs.

4. Finally, save the file, and run the **debugoff.bat** or **debugon.bat** file (as the case may be).

3.3.8 Configuring High Availability for the eG Agent

eG Enterprise uses external and remote agents to monitor the environment, for example VMware infrastructure, where it is not possible to install an eG agent. In such cases, the eG agent is deployed on an external host, and is remotely connected to the target system to collect its performance metrics. These agents can be a single point of failures

You can configure two agents within a Windows cluster setup, so that when one agent fails, the other agent takes over from the first and performs all the monitoring tasks originally assigned to the first. This way, there will not be a single point of failure of the eG agent.

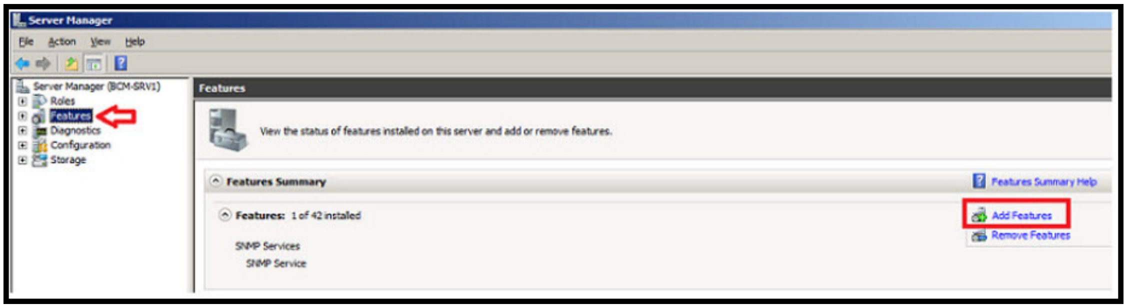
In order to configure a fail-proof agent, follow the broad steps listed below:

1. Prepare two machines with identical specifications. Name them as Node 1 and Node 2.
2. Install Windows 2008 R2 Enterprise Edition on both the machines.
3. Both nodes in the cluster must be in the same Active Directory domain, as a best practice. Both the clustered nodes should have the same domain role. The recommended role is *member server*.
4. The File Share Server should also be in the same Active Directory domain as the clustered nodes.
5. Install an eG agent each on Node 1 and Node 2.
6. Then, proceed to create the Windows cluster. Follow the steps detailed in Section **3.3.8.1** for this purpose.
7. Next, create a Windows file share from a File share server. This file share will be used as a third vote in the **Node and File Share Majority** quorum mode that is to be set for the cluster. The steps to achieve this have been detailed in Section **3.3.8.2**.
8. Configure cluster quorum settings using the procedure discussed in Section **3.3.8.3**.
9. Add eG agent service as a cluster resource, as outlined in Section **3.3.8.4**.

3.3.8.1 Creating a Windows Cluster

To achieve this, follow the steps discussed below:

1. Install the **Failover Clustering** feature on both nodes of the cluster. For this, first, do the following on Node 1:
2. If you recently installed Windows Server 2008 R2 on the server and the **Initial Configuration Tasks** interface is displayed, look for the **Customize This Server** option, and click the **Add features** option under it.
3. If **Initial Configuration Tasks** is not displayed, add the feature through **Server Manager**. If Server Manager is already running, click **Features** (see Figure 3.38). Then, under **Features Summary**, click **Add Features**.



View the status of features installed on this server and add or remove features.

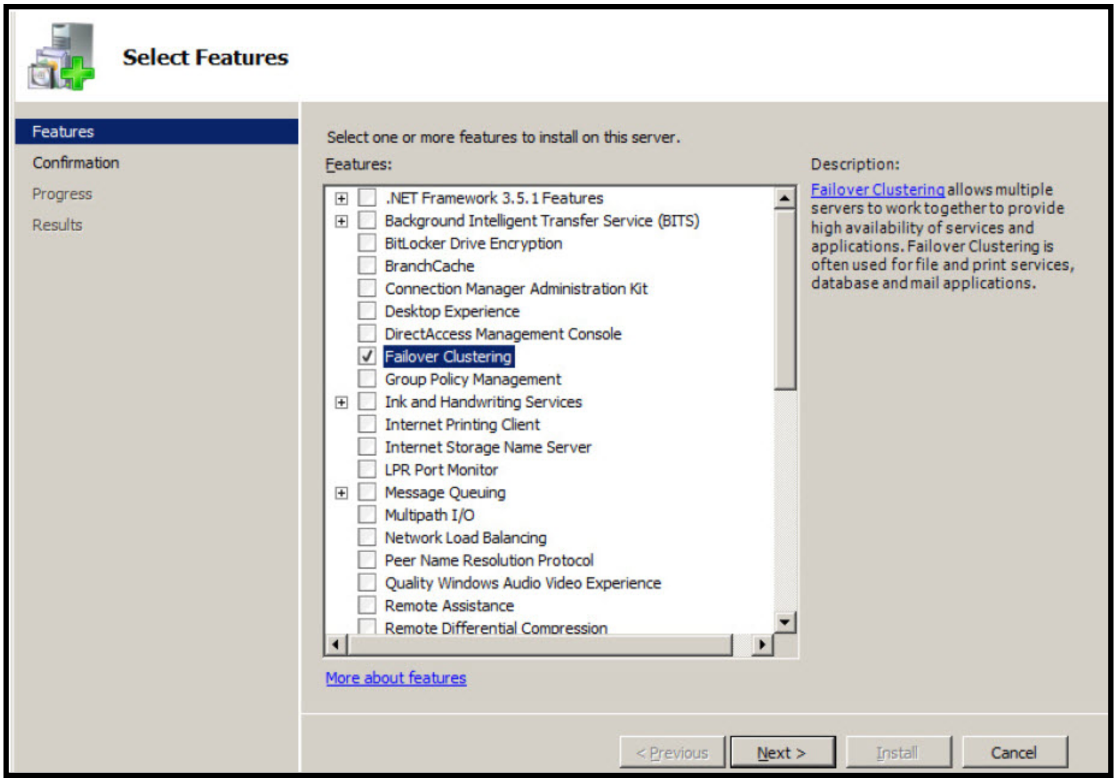
Features: 1 of 42 installed

SNMP Services
SNMP Service

Figure 3.38: Clicking the Add Features option in the Server Manager

4. If Server Manager is not running, click **Start**, click **Administrative Tools**, click **Server Manager**, and then, if prompted for permission to continue, click **Continue**. Then, under **Features Summary**, click **Add Features**.

5. In the **Add Features Wizard**, click **Failover Clustering** and then click **Install** (see Figure 3.39).



Select one or more features to install on this server.

Features:

- □ .NET Framework 3.5.1 Features
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BranchCache
- □ Connection Manager Administration Kit
- □ Desktop Experience
- □ DirectAccess Management Console
- ☑ Failover Clustering
- □ Group Policy Management
- □ Ink and Handwriting Services
- □ Internet Printing Client
- □ Internet Storage Name Server
- □ LPR Port Monitor
- □ Message Queuing
- □ Multipath I/O
- □ Network Load Balancing
- □ Peer Name Resolution Protocol
- □ Quality Windows Audio Video Experience
- □ Remote Assistance
- □ Remote Differential Compression

Description:

Failover Clustering allows multiple servers to work together to provide high availability of services and applications. Failover Clustering is often used for file and print services, database and mail applications.

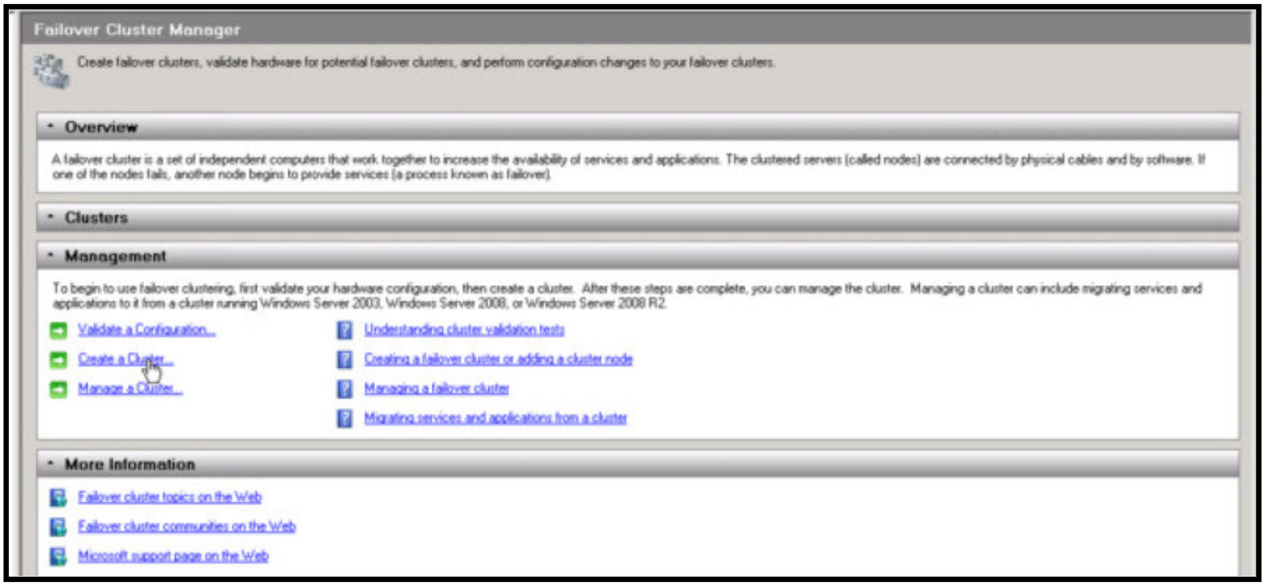
Figure 3.39: Installing the Failover Clustering feature

When installation completes, close the wizard.

6. Now, repeat the process on each of the nodes that you want to include in the cluster.

7. Once this is done, you are ready to create your cluster. For this, first launch the **Failover Cluster**

Manager by following the Start -> Administrative Tools -> Failover Cluster Management menu sequence (see Figure 3.40). Then, click on the **Create a Cluster** link therein (see Figure 3.40).



Failover Cluster Manager

Create failover clusters, validate hardware for potential failover clusters, and perform configuration changes to your failover clusters.

Overview

A failover cluster is a set of independent computers that work together to increase the availability of services and applications. The clustered servers (called nodes) are connected by physical cables and by software. If one of the nodes fails, another node begins to provide services (a process known as failover).

Clusters

Management

To begin to use failover clustering, first validate your hardware configuration, then create a cluster. After these steps are complete, you can manage the cluster. Managing a cluster can include migrating services and applications to it from a cluster running Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2.

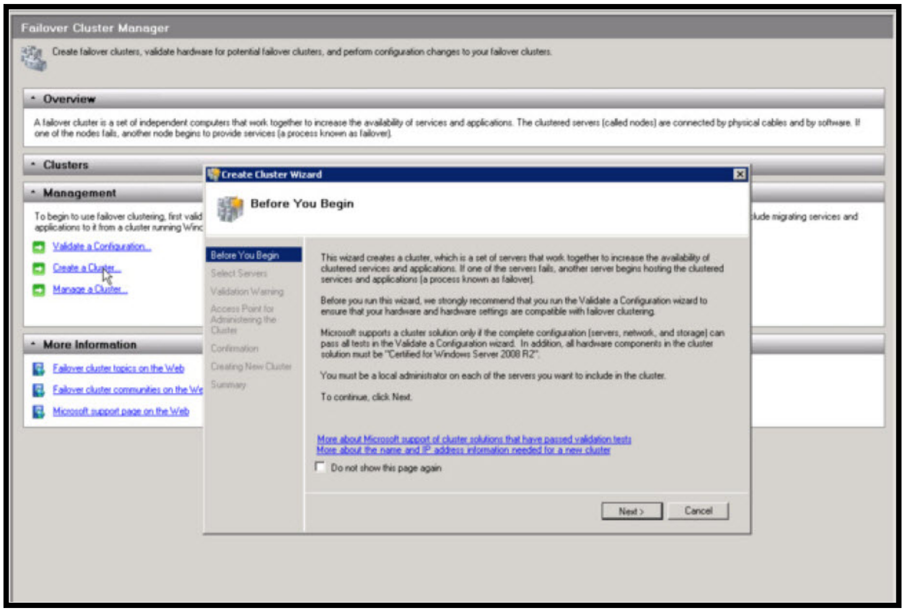
Validate a Configuration...
Create a Cluster...
Manage a Cluster...
Understanding cluster validation tests
Creating a failover cluster or adding a cluster node
Managing a failover cluster
Migrating services and applications from a cluster

More Information

Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web

Figure 3.40: Creating a failover cluster

8. When Figure 3.41 appears, click on the **Next** button to proceed.



Create Cluster Wizard

Before You Begin

This wizard creates a cluster, which is a set of servers that work together to increase the availability of clustered services and applications. If one of the servers fails, another server begins hosting the clustered services and applications (a process known as failover).

Before you run this wizard, we strongly recommend that you run the Validate a Configuration wizard to ensure that your hardware and hardware settings are compatible with failover clustering.

Microsoft supports a cluster solution only if the complete configuration (servers, network, and storage) can pass all tests in the Validate a Configuration wizard. In addition, all hardware components in the cluster solution must be "Certified for Windows Server 2008 R2".

You must be a local administrator on each of the servers you want to include in the cluster.

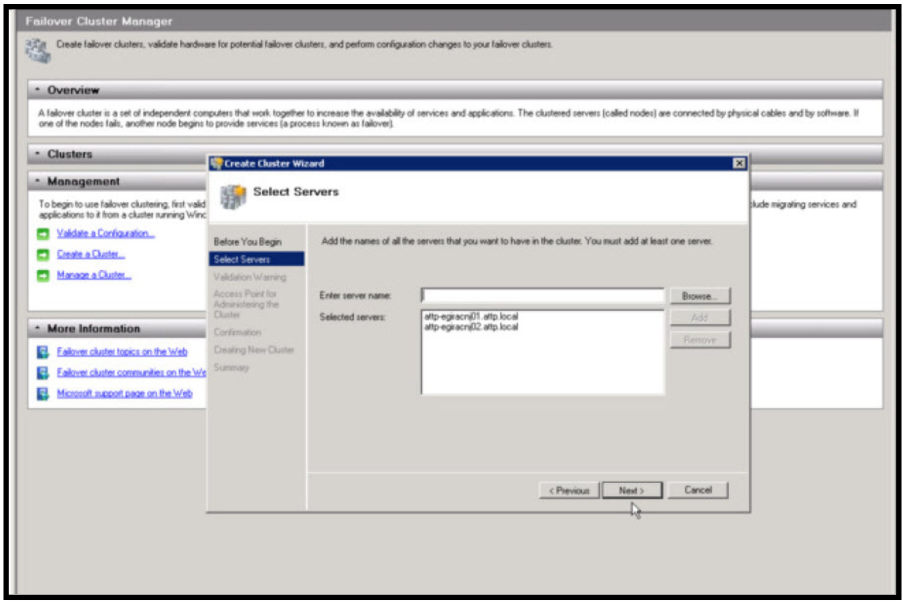
To continue, click Next.

More about Microsoft support of cluster solutions that have passed validation tests
More about the name and IP address information needed for a new cluster
□ Do not show this page again
Next >
Cancel

Figure 3.41: The Welcome screen of the Create Cluster Wizard

9. Using Figure 3.42 that appears next, add Node 1 and Node 2 to the cluster. For that, first enter

the server name of Node 1 in the **Enter server name** text box of Figure 3.42 and click the **Add** button. Likewise, specify the server name of Node 2 in the **Enter server name** text box and click the **Add** button again. Then, click on **Next** to proceed.



Failover Cluster Manager

Create failover clusters, validate hardware for potential failover clusters, and perform configuration changes to your failover clusters.

A failover cluster is a set of independent computers that work together to increase the availability of services and applications. The clustered servers (called nodes) are connected by physical cables and by software. If one of the nodes fails, another node begins to provide services (a process known as failover).

Create Cluster Wizard

Select Servers

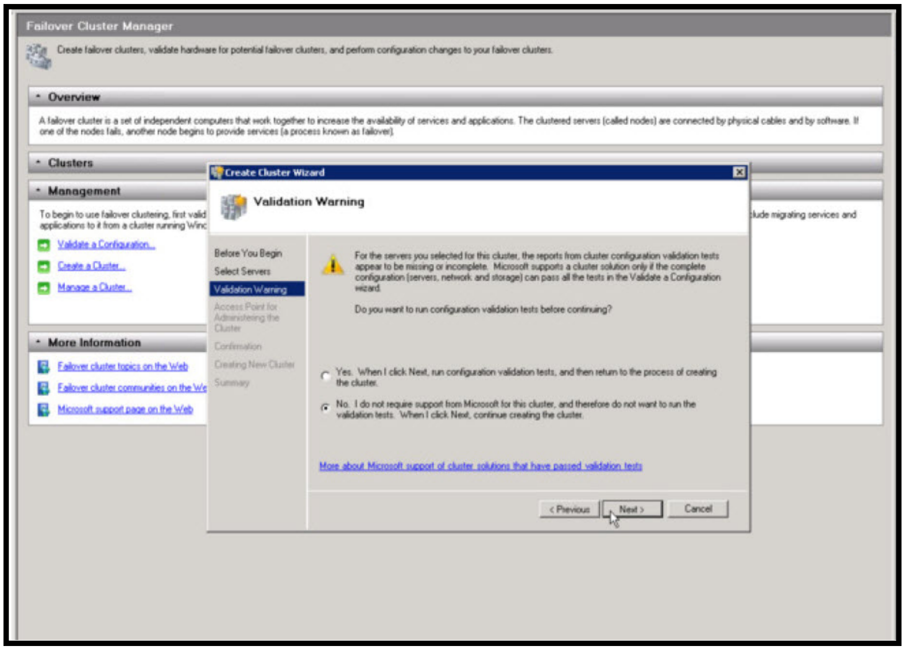
Add the names of all the servers that you want to have in the cluster. You must add at least one server.

Enter server name:

Selected servers: altp-egiracnj01.altp.local
altp-egiracnj02.altp.local

Figure 3.42: Adding nodes to a cluster

10. Skip the validation tests by clicking the **Next** button in Figure 3.43.



Create Cluster Wizard

Validation Warning

For the servers you selected for this cluster, the reports from cluster configuration validation tests appear to be missing or incomplete. Microsoft supports a cluster solution only if the complete configuration (servers, network and storage) can pass all the tests in the Validate a Configuration wizard.

Do you want to run configuration validation tests before continuing?

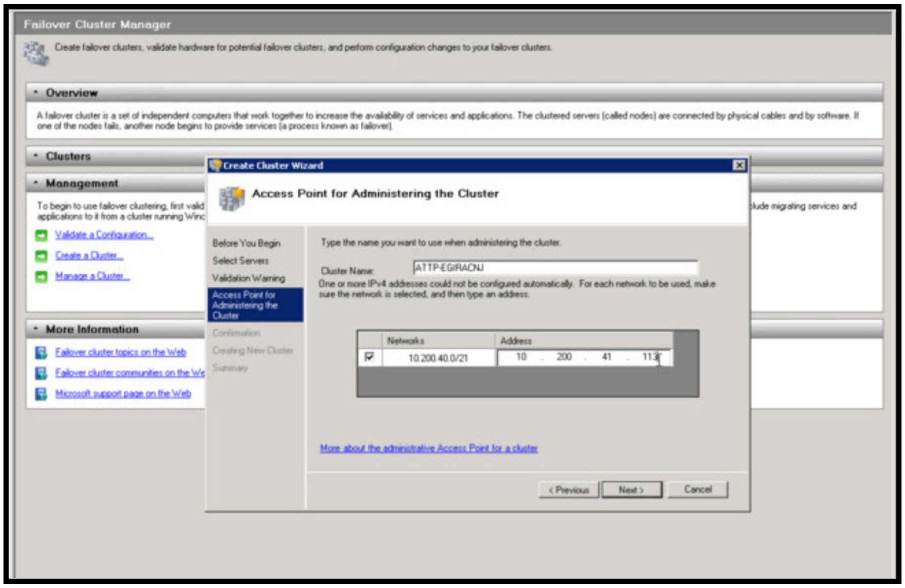
○ Yes. When I click Next, run configuration validation tests, and then return to the process of creating the cluster.

● No. I do not require support from Microsoft for this cluster, and therefore do not want to run the validation tests. When I click Next, continue creating the cluster.

More about Microsoft support of cluster solutions that have passed validation tests

Figure 3.43: Skipping the validation tests

11. Next, provide a name for the cluster and specify its IP address, as depicted by Figure 3.44 below. Then, click the **Next** button.



Create failover clusters, validate hardware for potential failover clusters, and perform configuration changes to your failover clusters.

A failover cluster is a set of independent computers that work together to increase the availability of services and applications. The clustered servers (called nodes) are connected by physical cables and by software. If one of the nodes fails, another node begins to provide services (a process known as failover).

To begin to use failover clustering, first valid[...] applications to it from a cluster running Winc[...] lude migrating services and

Access Point for Administering the Cluster

Type the name you want to use when administering the cluster.

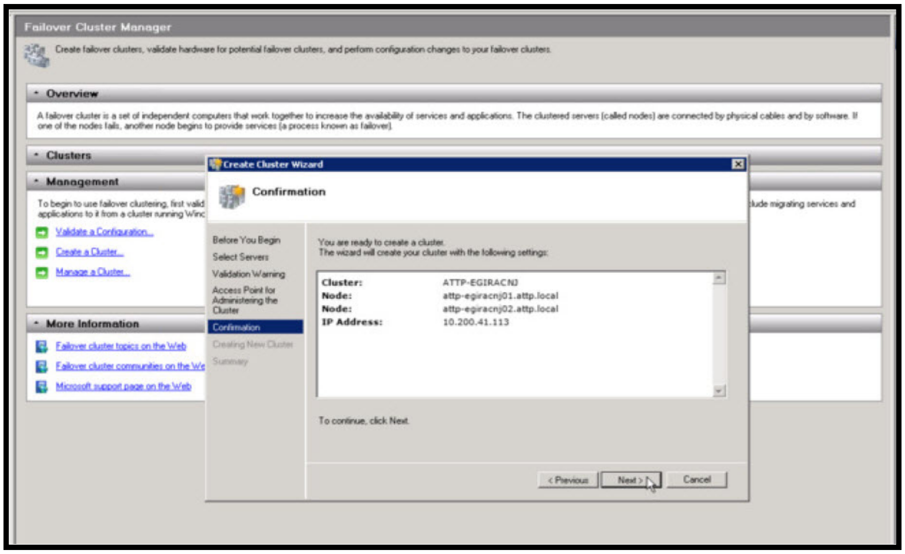
Cluster Name: ATTP-EGIRACNJ

One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.

	Networks	Address
☑	10.200.40.0/21	10 . 200 . 41 . 113

Figure 3.44: Specifying the name and IP address of the cluster

12. A brief summary of the cluster configuration will then appear, as shown by Figure 3.45. Click **Next** therein to confirm and proceed.



Confirmation

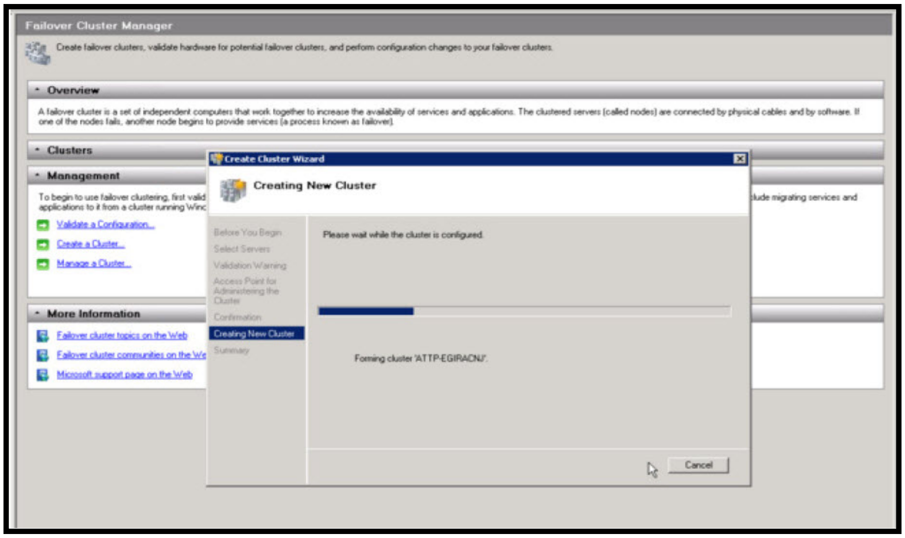
You are ready to create a cluster.
The wizard will create your cluster with the following settings:

Cluster: ATTP-EGIRACNJ
Node: attp-egiracnj01.attp.local
Node: attp-egiracnj02.attp.local
IP Address: 10.200.41.113

To continue, click Next.

Figure 3.45: Confirming the cluster configuration

13. Cluster creation will then begin (see Figure 3.46).



Create failover clusters, validate hardware for potential failover clusters, and perform configuration changes to your failover clusters.

A failover cluster is a set of independent computers that work together to increase the availability of services and applications. The clustered servers (called nodes) are connected by physical cables and by software. If one of the nodes fails, another node begins to provide services (a process known as failover).

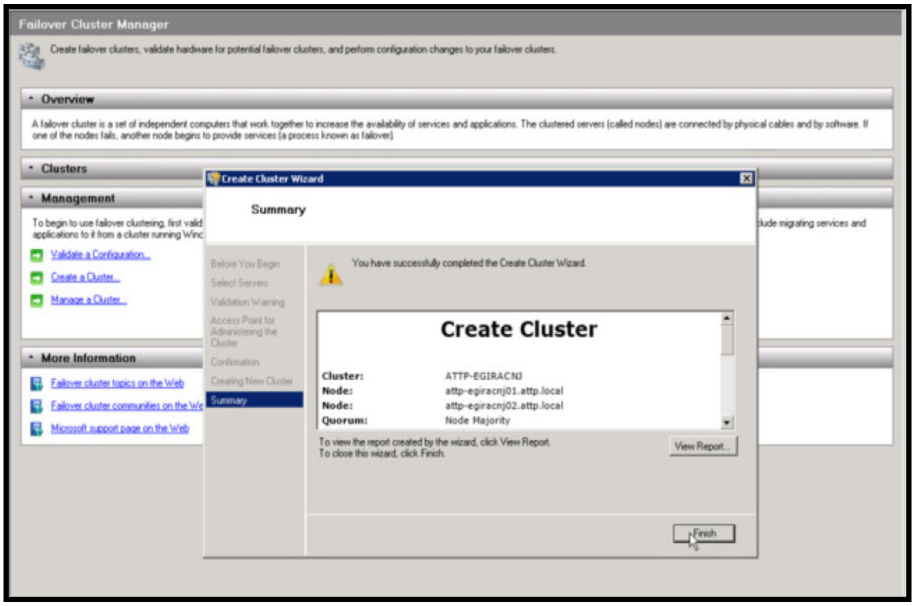
To begin to use failover clustering, first valid ... lude migrating services and applications to it from a cluster running Winc

Please wait while the cluster is configured.

Forming cluster 'ATTP-EGIRACNJ'.

Figure 3.46: Cluster creation in progress

14. Once cluster creation completes, Figure 3.47 will appear. Click the **Finish** button therein to end the cluster creation process.



Create failover clusters, validate hardware for potential failover clusters, and perform configuration changes to your failover clusters.

A failover cluster is a set of independent computers that work together to increase the availability of services and applications. The clustered servers (called nodes) are connected by physical cables and by software. If one of the nodes fails, another node begins to provide services (a process known as failover).

To begin to use failover clustering, first valid ... lude migrating services and applications to it from a cluster running Winc

You have successfully completed the Create Cluster Wizard.

Create Cluster

Cluster:	ATTP-EGIRACNJ
Node:	attp-egiracnj01.attp.local
Node:	attp-egiracnj02.attp.local
Quorum:	Node Majority

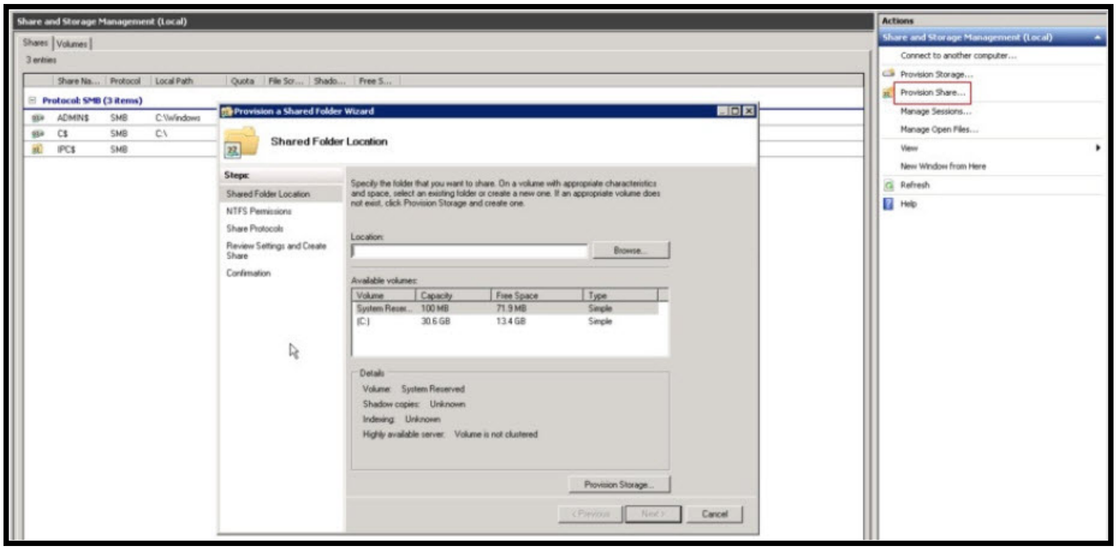
To view the report created by the wizard, click View Report.
To close this wizard, click Finish.

Figure 3.47: Completion of cluster creation

3.3.8.2 Creating a Windows File Share

Now that the cluster has been created, proceed to create a Windows File Share for the cluster. This is required in order to set a quorum for the cluster. The quorum for a cluster is the number of elements that must be online for that cluster to continue running. In effect, each element can cast one “vote” to determine whether the cluster continues running. The voting elements are nodes or, in some cases, a disk witness or file share witness. Where a file share witness (FSW) is a voting element, you will have to create a Windows file share. The procedure for this is as follows:

1. Launch the Share and Storage Management tool on the File Share server by following the Start -> Administrative Tools -> Share and Storage Management menu sequence. Once in the Share and Storage Management console, click on the **Provision Share** option in the right panel of the console, as indicated by Figure 3.48.



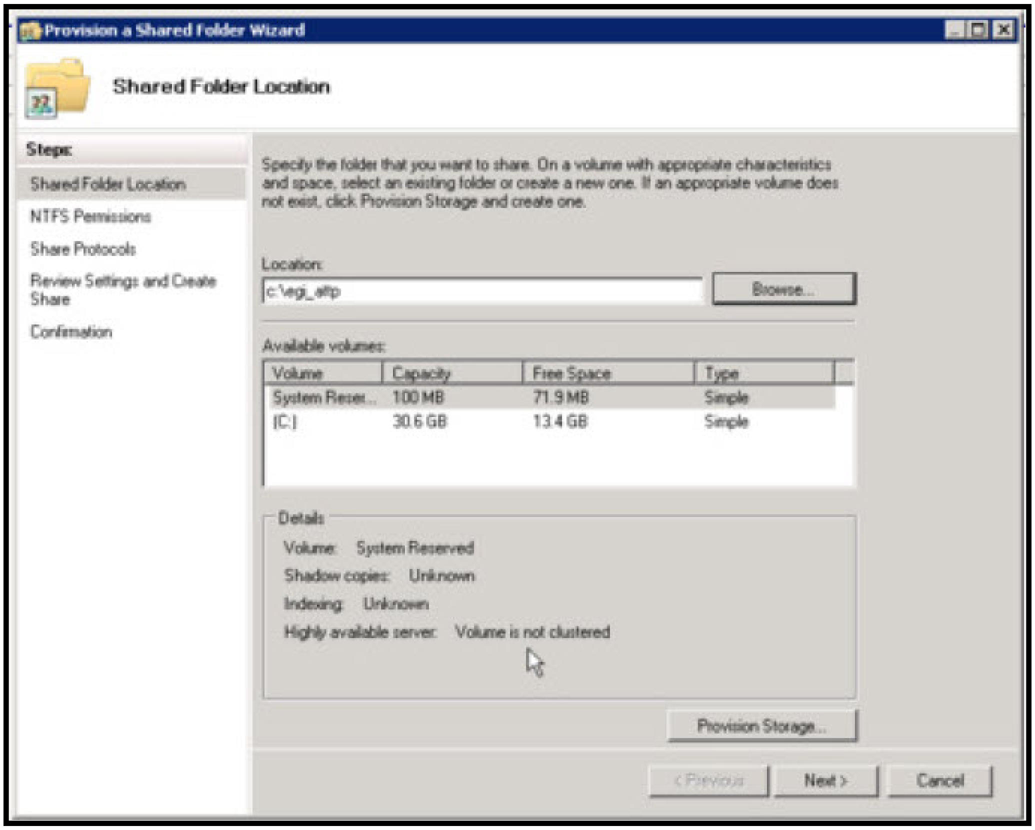
Specify the folder that you want to share. On a volume with appropriate characteristics and space, select an existing folder or create a new one. If an appropriate volume does not exist, click Provision Storage and create one.

Volume	Capacity	Free Space	Type
System Reser...	100 MB	71.9 MB	Simple
(C:)	30.6 GB	13.4 GB	Simple

Volume: System Reserved
Shadow copies: Unknown
Indexing: Unknown
Highly available server: Volume is not clustered

Figure 3.48: Selecting the Provision Share option

2. In the **Location** text box of Figure 3.49 that appears, specify the folder you want to share from the local machine, and click the **Next** button to proceed.



Specify the folder that you want to share. On a volume with appropriate characteristics and space, select an existing folder or create a new one. If an appropriate volume does not exist, click Provision Storage and create one.

Location: c:\egi_sftp

Available volumes:

Volume	Capacity	Free Space	Type
System Reser...	100 MB	71.9 MB	Simple
(C:)	30.6 GB	13.4 GB	Simple

Details

Volume: System Reserved

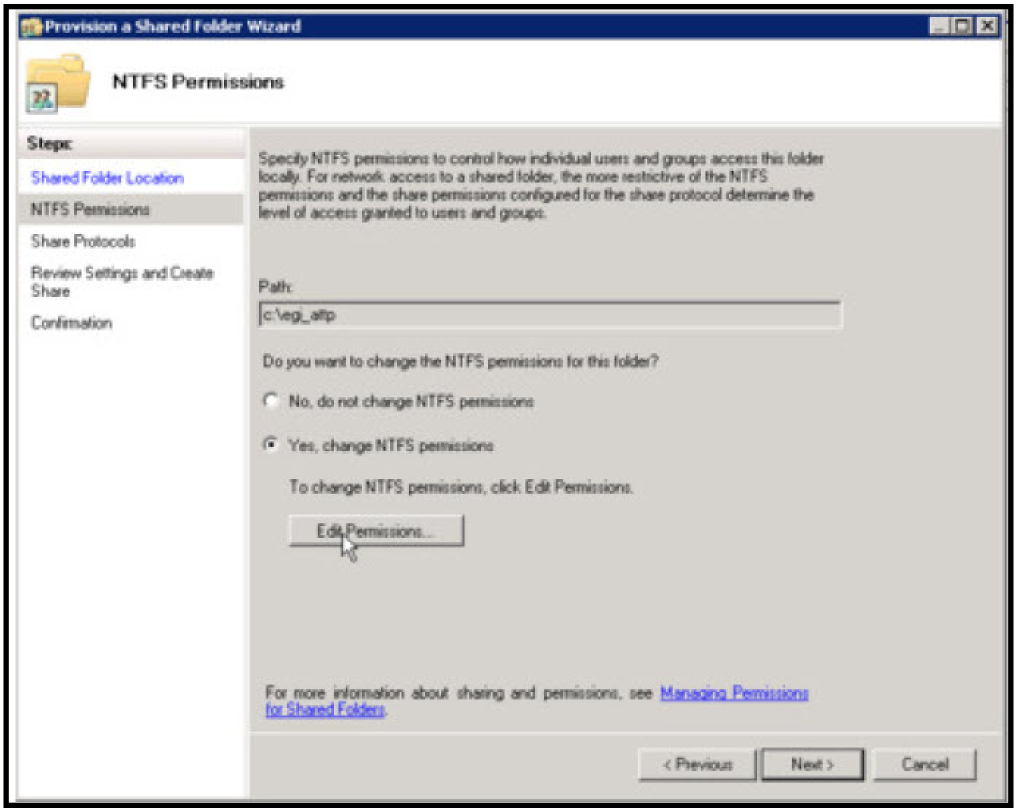
Shadow copies: Unknown

Indexing: Unknown

Highly available server: Volume is not clustered

Figure 3.49: Selecting the folder to share

3. In the NTFS Permissions dialog box that appears next (see Figure 3.50), choose to change the NTFS permissions of the specified folder, by picking the **Yes, change NTFS permissions** option. Then, click the **Edit Permissions** button.



Specify NTFS permissions to control how individual users and groups access this folder locally. For network access to a shared folder, the more restrictive of the NTFS permissions and the share permissions configured for the share protocol determine the level of access granted to users and groups.

Path:
c:\egi_attp

Do you want to change the NTFS permissions for this folder?

○ No, do not change NTFS permissions

● Yes, change NTFS permissions

To change NTFS permissions, click Edit Permissions.

For more information about sharing and permissions, see Managing Permissions for Shared Folders.

Figure 3.50: Choosing to change the NTFS permissions of the specified folder

4. Doing so invokes Figure 3.51. Click the **Add** button in Figure 3.51.

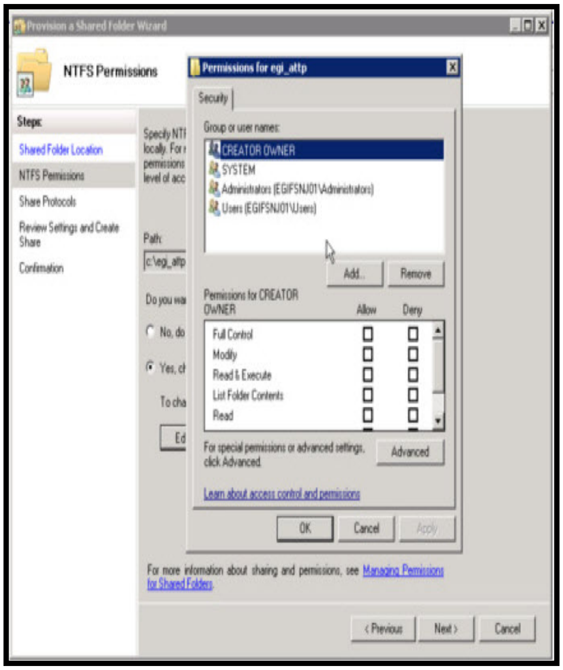

Provision a Shared Folder Wizard
NTFS Permissions
Steps:
Shared Folder Location
NTFS Permissions
Share Protocols
Review Settings and Create Share
Confirmation
Specify NTI locally. For permissions level of acc
Path:
c:\egi_attp
Do you wa
No, do
Yes, cl
To cha
Ed
Permissions for egi_attp
Security
Group or user names:
CREATOR OWNER
SYSTEM
Administrators (EGIFSNJ01\Administrators)
Users (EGIFSNJ01\Users)
Add...
Remove
Permissions for CREATOR OWNER
Allow
Deny
Full Control
Modify
Read & Execute
List Folder Contents
Read
For special permissions or advanced settings, click Advanced.
Advanced
Learn about access control and permissions
OK
Cancel
Apply
For more information about sharing and permissions, see Managing Permissions for Shared Folders.
< Previous
Next >
Cancel

Figure 3.51: Adding a user/group

5. Figure 3.52 will then appear. Click the **Object Types** button in Figure 3.52 , select the **Computers** check box in the window that pops up, and click the **OK** button in that window to return to Figure 3.52.

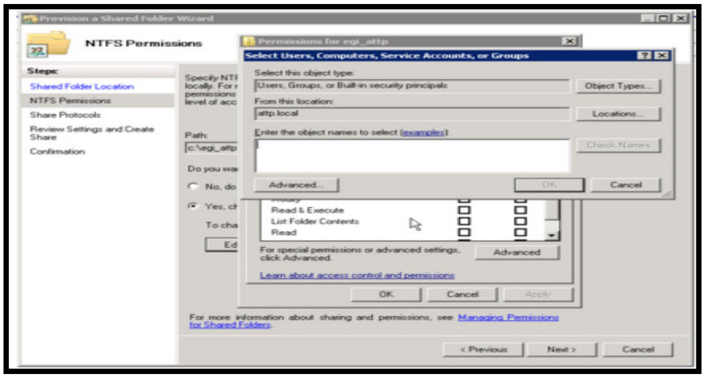
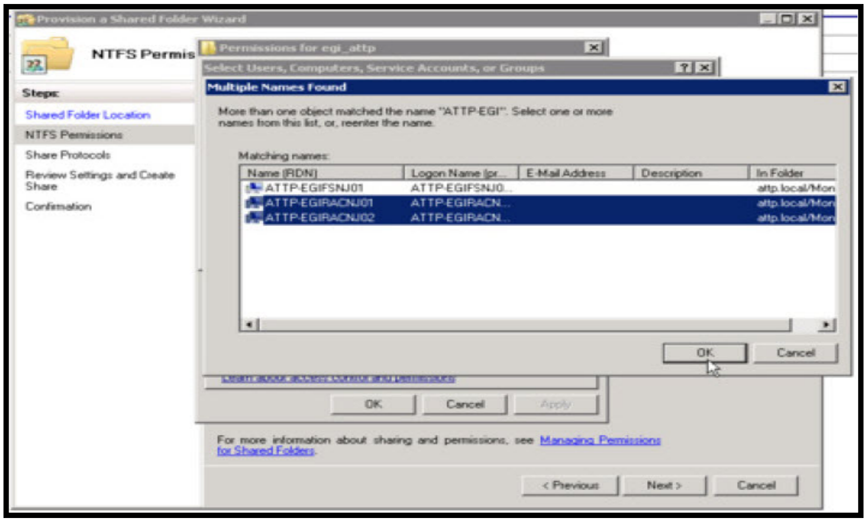

Provision a Shared Folder Wizard
NTFS Permissions
Steps:
Shared Folder Location
NTFS Permissions
Share Protocols
Review Settings and Create Share
Confirmation
Specify NTI locally. For permissions level of acc
Path:
c:\egi_attp
Do you wa
No, do
Yes, cl
To cha
Ed
Permissions for egi_attp
Select Users, Computers, Service Accounts, or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
attp.local
Locations...
Enter the object names to select (examples):
Check Names
Advanced...
OK
Cancel
Read & Execute
List Folder Contents
Read
For special permissions or advanced settings, click Advanced.
Advanced
Learn about access control and permissions
OK
Cancel
Apply
For more information about sharing and permissions, see Managing Permissions for Shared Folders.
< Previous
Next >
Cancel

Figure 3.52: Clicking the Object Types button

6. Now, in the **Enter the object names to select** text area of Figure 3.52, type the name of the cluster you created using the procedure detailed in the Section **3.3.8.1** topic, and click the **Check Names** button. Figure 3.53 will then appear, listing all objects that match the cluster name that you specified.



More than one object matched the name "ATTP-EGI". Select one or more names from this list, or, reenter the name.

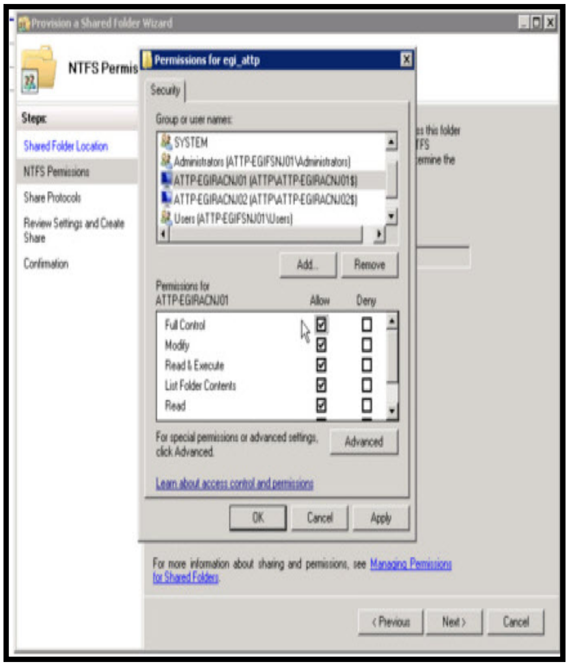
Matching names:

Name (RDN)	Logon Name (pr...	E-Mail Address	Description	In Folder
ATTP-EGIFSNJ01	ATTP-EGIFSNJ0...			attp.local/Mon
ATTP-EGIRACNJ01	ATTP-EGIRACN...			attp.local/Mon
ATTP-EGIRACNJ02	ATTP-EGIRACN...			attp.local/Mon

For more information about sharing and permissions, see Managing Permissions for Shared Folders.

Figure 3.53: A window displaying all objects with names that match the specified cluster name

7. Select the name of the cluster you created from Figure 3.53 and click the **OK** button therein. 3.3.8.2 will then appear. From the **Group of user names** list of 3.3.8.2, select the cluster name. Then, select the **Allow** check box against **Full Control** permission in the **Permissions for …** list and click the **OK** button.



Group or user names:

- SYSTEM
- Administrators (ATTP-EGIFSNJ01\Administrators)
- ATTP-EGIRACNJ01 (ATTP\ATTP-EGIRACNJ01$)
- ATTP-EGIRACNJ02 (ATTP\ATTP-EGIRACNJ02$)
- Users (ATTP-EGIFSNJ01\Users)

Permissions for ATTP-EGIRACNJ01	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□

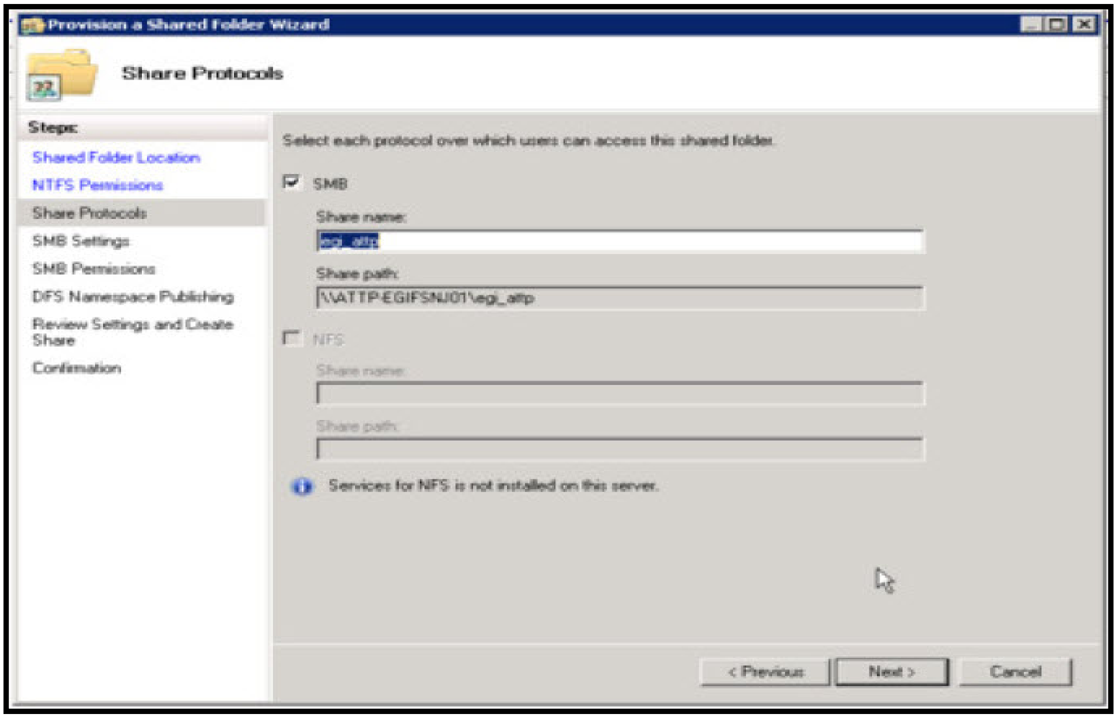
For special permissions or advanced settings, click Advanced.

For more information about sharing and permissions, see Managing Permissions for Shared Folders.

Figure 3.54: Granting Full Control to cluster

8. This will lead you straight to **Share Protocols** section of the **Provision a Shared Folder**

wizard. Click the **Next** button in this section to accept the default settings and move on.



Select each protocol over which users can access this shared folder.

☑ SMB

Share name: egi_attp

Share path: \\ATTP-EGIFSNJ01\egi_attp

□ NFS

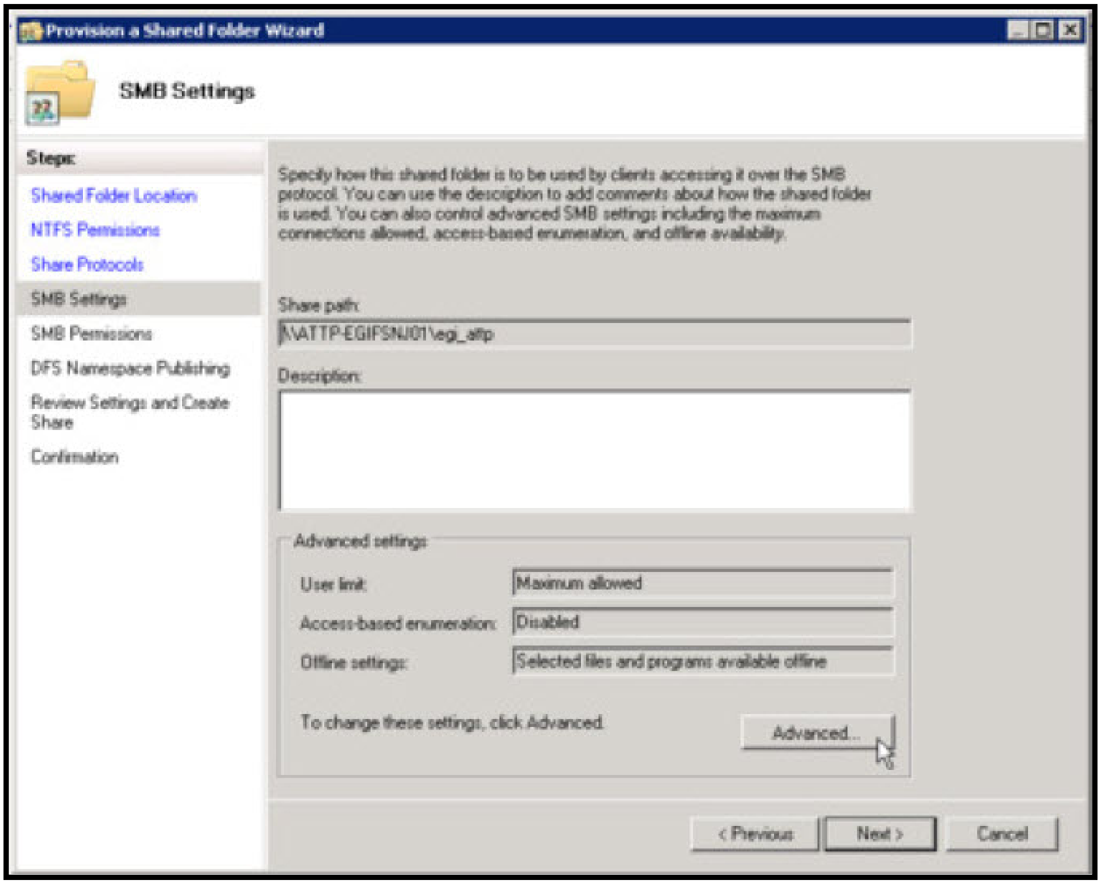
Share name:

Share path:

Services for NFS is not installed on this server.

Figure 3.55: Accepting the default settings of the Share Protocols section

9. This will take you to the **SMB Settings** section (see Figure 3.56). Here again, click the **Next** button to proceed.



Specify how this shared folder is to be used by clients accessing it over the SMB protocol. You can use the description to add comments about how the shared folder is used. You can also control advanced SMB settings including the maximum connections allowed, access-based enumeration, and offline availability.

Share path:
\\ATTP-EGIFSNJ01\egi_attp

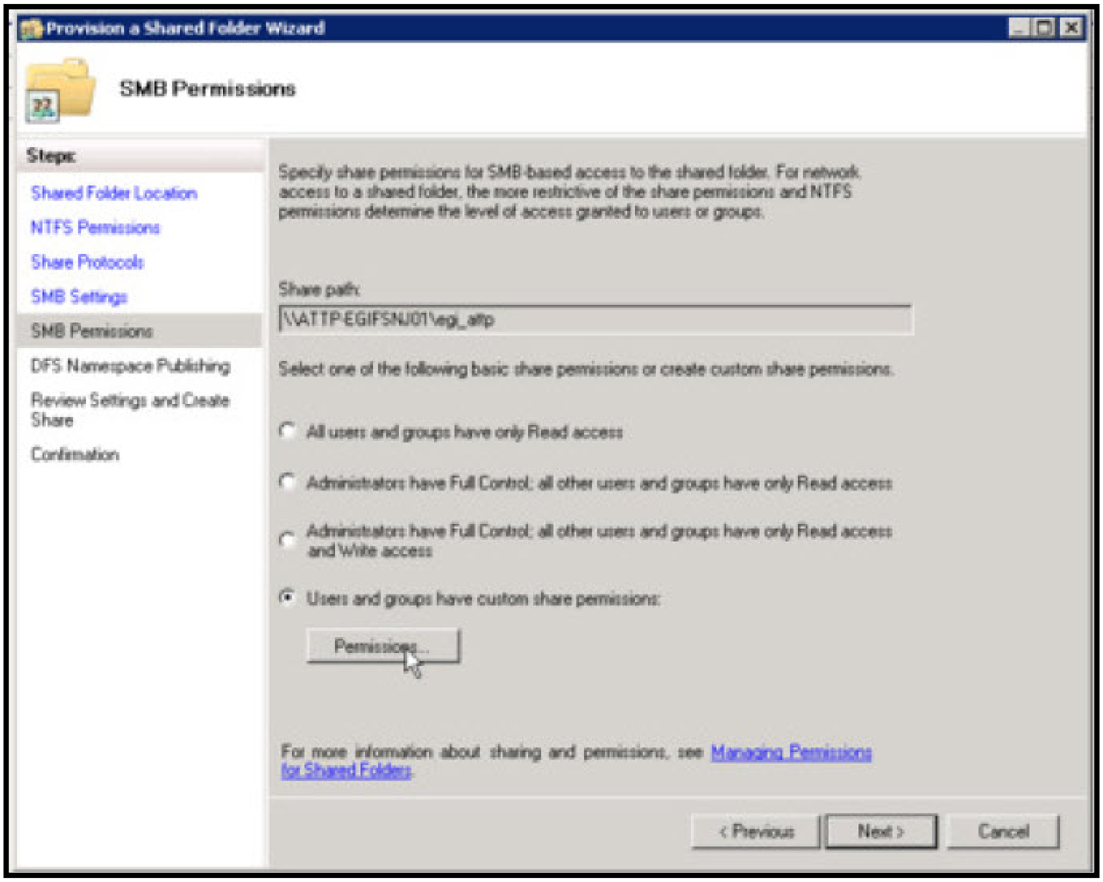
Description:

Advanced settings
User limit: Maximum allowed
Access-based enumeration: Disabled
Offline settings: Selected files and programs available offline

To change these settings, click Advanced.

Figure 3.56: Accepting the default settings of the SMB Settings section

10. In the **SMB Permissions** section that appears next, select the **Users and groups have custom share permissions** option (see Figure 3.57). Then, click the **Permissions** button in Figure 3.57.



Specify share permissions for SMB-based access to the shared folder. For network access to a shared folder, the more restrictive of the share permissions and NTFS permissions determine the level of access granted to users or groups.

Share path:
\\ATTP-EGIFSNJ01\egi_attp

Select one of the following basic share permissions or create custom share permissions.

○ All users and groups have only Read access

○ Administrators have Full Control; all other users and groups have only Read access

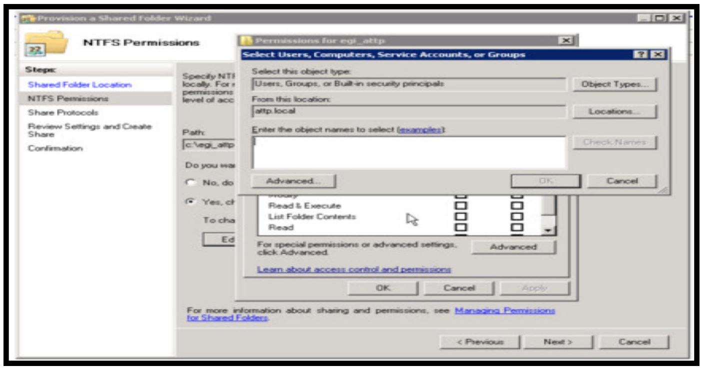
○ Administrators have Full Control; all other users and groups have only Read access and Write access

● Users and groups have custom share permissions:

For more information about sharing and permissions, see Managing Permissions for Shared Folders.

Figure 3.57: Configuring SMP Permissions

11. When Figure 3.58 appears, click the **Object Types** button in Figure 3.58, select the **Computers** check box in the window that pops up, and click the **OK** button in that window to return to Figure 3.58.



Select this object type:
Users, Groups, or Built-in security principals

From this location:
attp.local

Enter the object names to select (examples):

For special permissions or advanced settings, click Advanced.

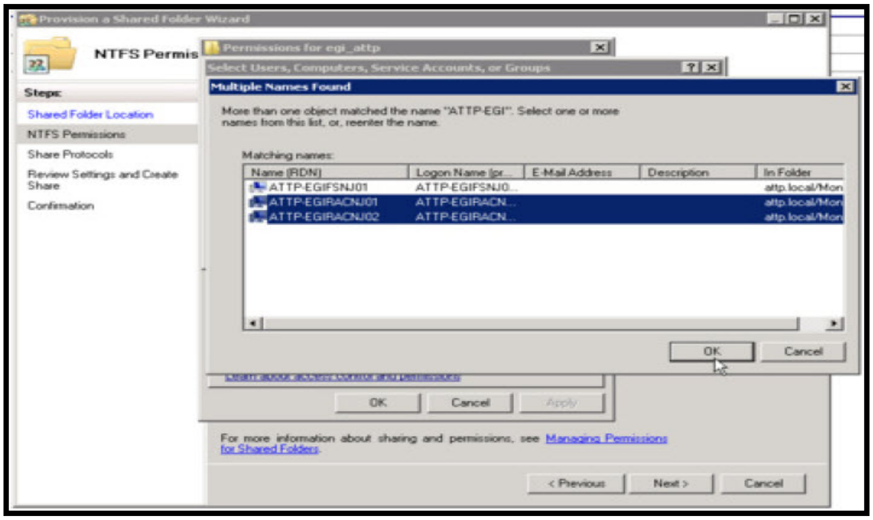
Learn about access control and permissions

For more information about sharing and permissions, see Managing Permissions for Shared Folders.

Figure 3.58: Clicking the Object Types button

12. Now, in the **Enter the object names to select** text area of Figure 3.58, type the name of the

cluster you created using the procedure detailed in Section 3.23.1, and click the **Check Names** button. Figure 3.59 will then appear, listing all objects that match the cluster name that you specified.



More than one object matched the name "ATTP-EGI". Select one or more names from this list, or, reenter the name.

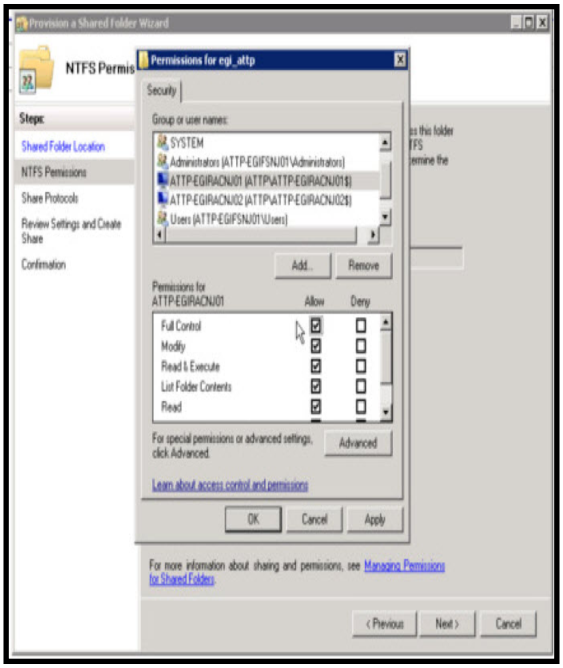
Matching names:

Name (RDN)	Logon Name (pr...	E-Mail Address	Description	In Folder
ATTP-EGIFSNJ01	ATTP-EGIFSNJ0...			attp.local/Mon
ATTP-EGIRACNJ01	ATTP-EGIRACN...			attp.local/Mon
ATTP-EGIRACNJ02	ATTP-EGIRACN...			attp.local/Mon

For more information about sharing and permissions, see Managing Permissions for Shared Folders.

Figure 3.59: A window displaying all objects with names that match the specified cluster name

13. Select the name of the cluster you created from Figure 3.59 and click the **OK** button therein. Figure 3.60 will then appear. From the **Group or user names** list of Figure 3.60, select the cluster name. Then, select the **Allow** check box against **Full Control** permission in the **Permissions for …** list and click the **OK** button.



Group or user names:

SYSTEM
Administrators (ATTP-EGIFSNJ01\Administrators)
ATTP-EGIRACNJ01 (ATTP\ATTP-EGIRACNJ01$)
ATTP-EGIRACNJ02 (ATTP\ATTP-EGIRACNJ02$)
Users (ATTP-EGIFSNJ01\Users)

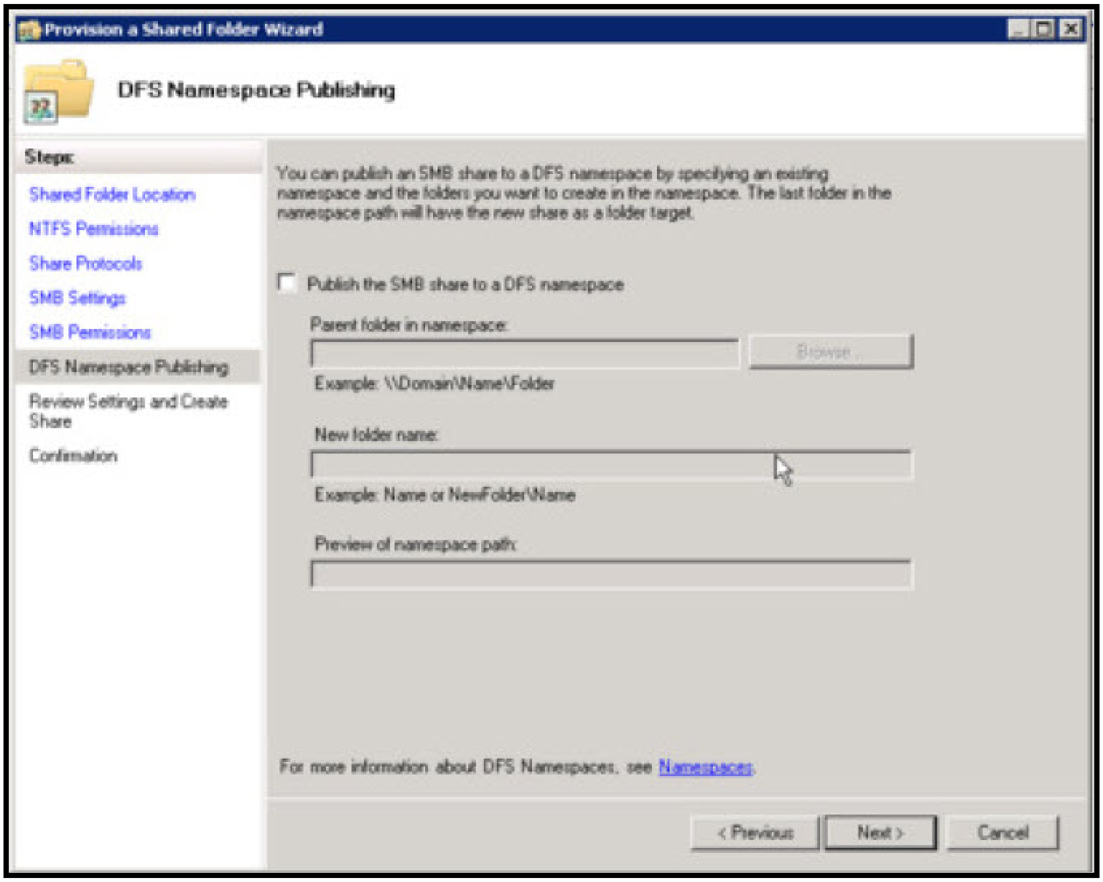
Permissions for ATTP-EGIRACNJ01	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□

For special permissions or advanced settings, click Advanced.

For more information about sharing and permissions, see Managing Permissions for Shared Folders.

Figure 3.60: Granting Full Control to cluster

14. Once you return to the **SMB Settings** section, click on the **Next** button to move on. Figure 3.61 will then appear. Accept the default settings of Figure 3.61 by clicking the **Next** button.



You can publish an SMB share to a DFS namespace by specifying an existing namespace and the folders you want to create in the namespace. The last folder in the namespace path will have the new share as a folder target.

□ Publish the SMB share to a DFS namespace

Parent folder in namespace:

Example: \\Domain\Name\Folder

New folder name:

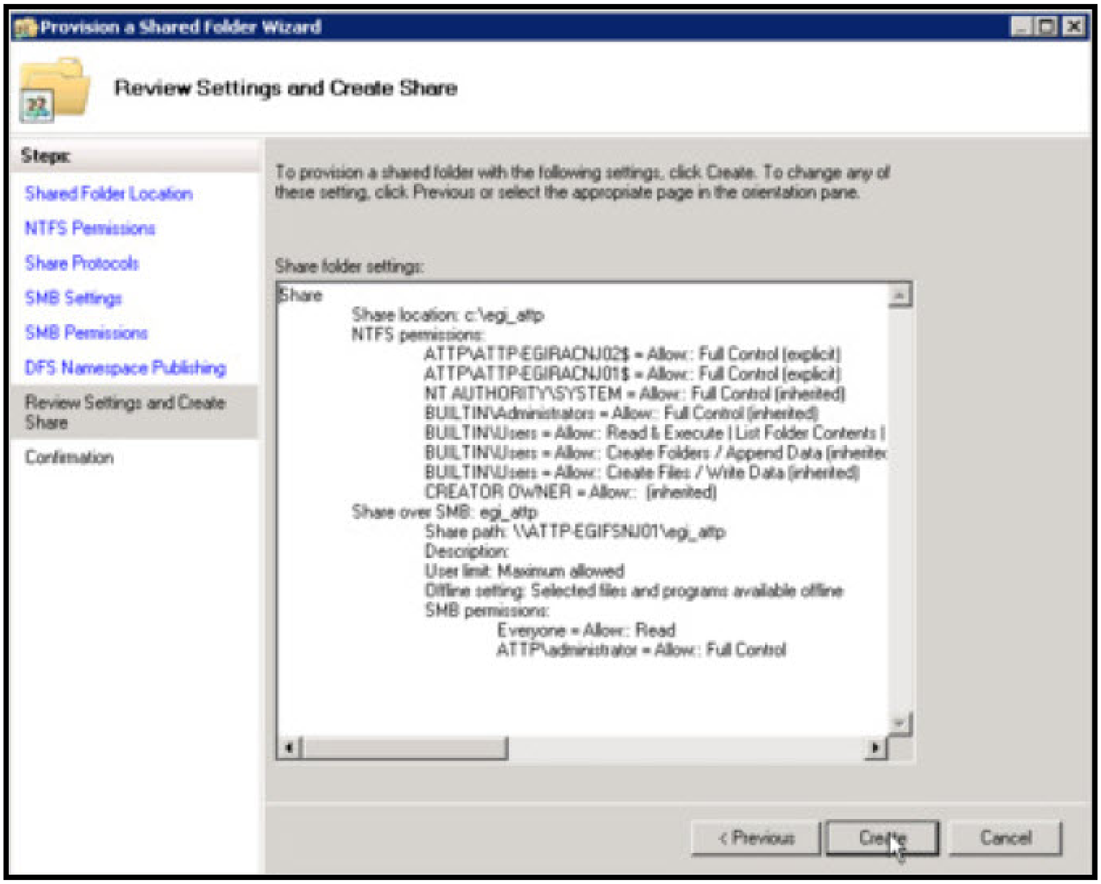
Example: Name or NewFolder\Name

Preview of namespace path:

For more information about DFS Namespaces, see Namespaces.

Figure 3.61: Accepting the default settings of DFS Namespace Publishing section

15. Figure 3.62 then appears displaying the configuration of the File share that you intend creating. Review the configuration and click the **Create** button therein, if you want to confirm creation of a file share with the displayed settings.



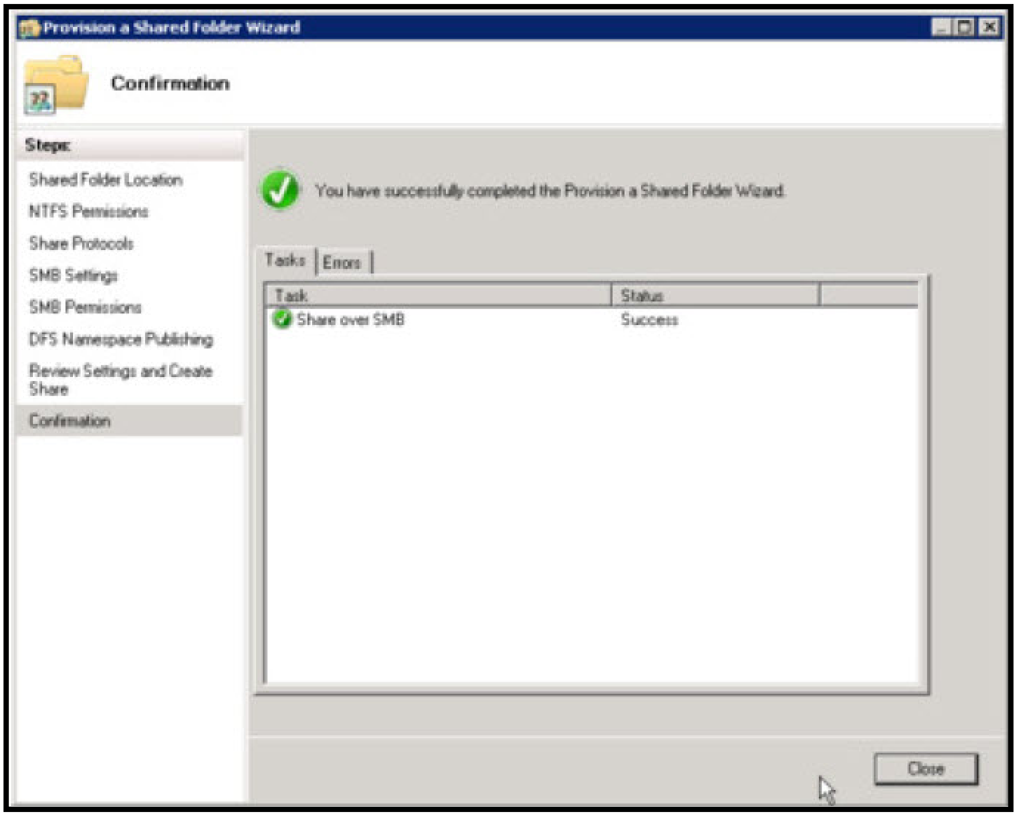
To provision a shared folder with the following settings, click Create. To change any of these setting, click Previous or select the appropriate page in the orientation pane.

Share folder settings:

```
Share
          Share location: c:\egi_attp
          NTFS permissions:
                    ATTP\ATTP-EGIRACNJ02$ = Allow:: Full Control (explicit)
                    ATTP\ATTP-EGIRACNJ01$ = Allow:: Full Control (explicit)
                    NT AUTHORITY\SYSTEM = Allow:: Full Control (inherited)
                    BUILTIN\Administrators = Allow:: Full Control (inherited)
                    BUILTIN\Users = Allow:: Read & Execute | List Folder Contents |
                    BUILTIN\Users = Allow:: Create Folders / Append Data (inheritec
                    BUILTIN\Users = Allow:: Create Files / Write Data (inherited)
                    CREATOR OWNER = Allow::  (inherited)
          Share over SMB: egi_attp
                    Share path: \\ATTP-EGIFSNJ01\egi_attp
                    Description:
                    User limit: Maximum allowed
                    Offline setting: Selected files and programs available offline
                    SMB permissions:
                              Everyone = Allow:: Read
                              ATTP\administrator = Allow:: Full Control
```

Figure 3.62: Reviewing the share settings

16. If share creation is successful, then Figure 3.63 will appear indicating the same. Click the **Close** button therein to close the wizard.



You have successfully completed the Provision a Shared Folder Wizard.

Task	Status
Share over SMB	Success

Figure 3.63: Successful creation of the file share

3.3.8.3 Configuring Cluster Quorum Settings

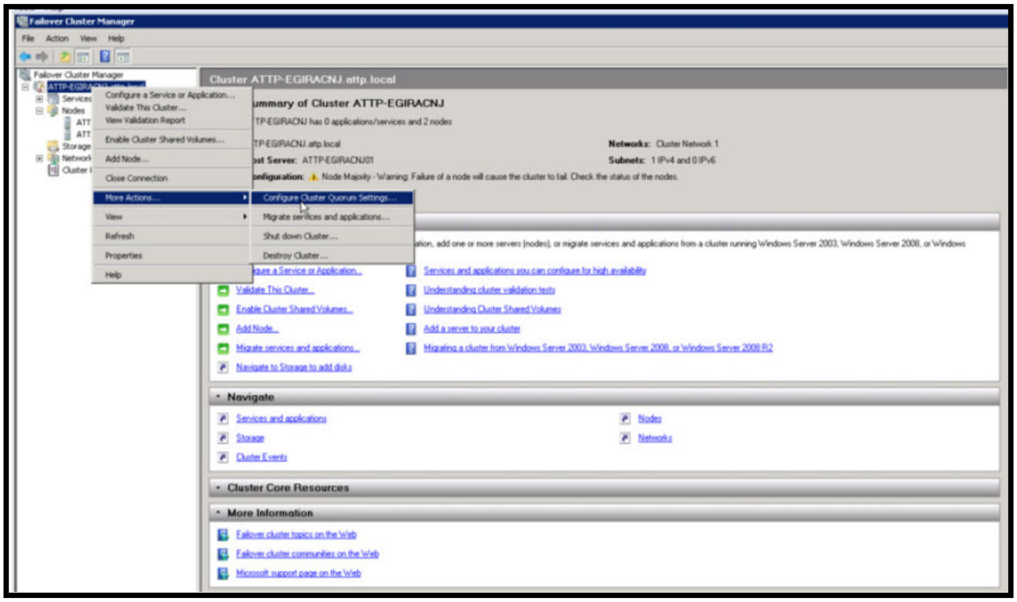
As stated earlier, the quorum for a cluster is the number of elements that must be online for that cluster to continue running.

When network problems occur, they can interfere with communication between cluster nodes. A small set of nodes might be able to communicate together across a functioning part of a network, but might not be able to communicate with a different set of nodes in another part of the network. This can cause serious issues. In this “split” situation, at least one of the sets of nodes must stop running as a cluster.

To prevent the issues that are caused by a split in the cluster, the cluster software requires that any set of nodes running as a cluster must use a voting algorithm to determine whether, at a given time, that set has quorum. Because a given cluster has a specific set of nodes and a specific quorum configuration, the cluster will know how many “votes” constitutes a majority (that is, a quorum). If the number drops below the majority, the cluster stops running. Nodes will still listen for the presence of other nodes, in case another node appears again on the network, but the nodes will not begin to function as a cluster until the quorum exists again.

In Windows Server 2008, a majority of ‘votes’ is what determines whether a cluster achieves quorum. Nodes can vote, and where appropriate, either a disk in cluster storage (called a “disk witness”) or a file share (called a “file share witness”) can vote. In the **Node and File Share Majority** quorum mode, each node plus a designated file share created by the administrator (the “file share witness”) can vote, whenever they are available and in communication. The cluster functions only with a majority of the votes, that is, more than half.To configure a cluster with this quorum mode, do the following:

1. Launch the **Failover Cluster Manager**. In the tree-view in the left panel of the cluster manager, right-click on the node representing the cluster that you created, move your mouse pointer over **More Actions**, and select the **Configure Cluster Quota Settings** option.


Failover Cluster Manager
File
Action
View
Help
Failover Cluster Manager
ATTP-EGIRACNJ.attp.local
Services
Nodes
ATT
ATT
Storage
Network
Cluster I
Configure a Service or Application...
Validate This Cluster...
View Validation Report
Enable Cluster Shared Volumes...
Add Node...
Close Connection
More Actions...
View
Refresh
Properties
Help
Configure Cluster Quorum Settings...
Migrate services and applications...
Shut down Cluster...
Destroy Cluster...
Cluster ATTP-EGIRACNJ.attp.local
ummary of Cluster ATTP-EGIRACNJ
Validate This Cluster...
Enable Cluster Shared Volumes...
Add Node...
Migrate services and applications...
Navigate to Storage to add disks
Services and applications you can configure for high availability
Understanding cluster validation tests
Understanding Cluster Shared Volumes
Add a server to your cluster
Migrating a cluster from Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2
Navigate
Services and applications
Storage
Cluster Events
Nodes
Networks
Cluster Core Resources
More Information
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web

TP-EGIRACNJ has 0 applications/services and 2 nodes

TP-EGIRACNJ.attp.local

Networks: Cluster Network 1

st Server: ATTP-EGIRACNJ01

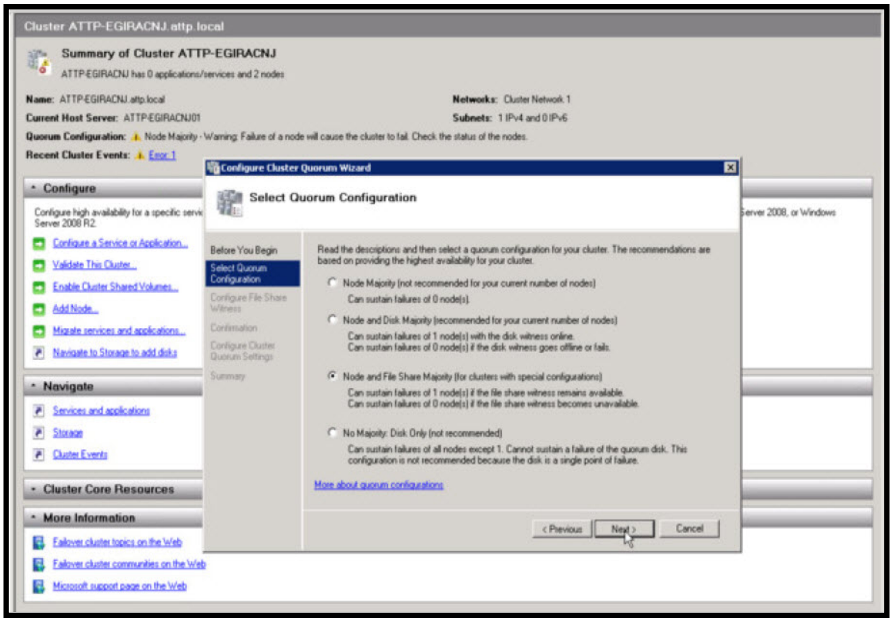
Subnets: 1 IPv4 and 0 IPv6

nfiguration: ⚠ Node Majority - Warning: Failure of a node will cause the cluster to fail. Check the status of the nodes.

ation, add one or more servers (nodes), or migrate services and applications from a cluster running Windows Server 2003, Windows Server 2008, or Windows

Figure 3.64: Selecting the Configure Cluster Quota Settings option

2. From the **Select Quorum Configuration** window that appears next, select the **Node and File Sharing Majority (for clusters with special configuration)** option (see Figure 3.65). Then, click the **Next** button therein.



Cluster ATTP-EGIRACNJ.attp.local

Summary of Cluster ATTP-EGIRACNJ

ATTP-EGIRACNJ has 0 applications/services and 2 nodes

Name: ATTP-EGIRACNJ.attp.local
Networks: Cluster Network 1
Current Host Server: ATTP-EGIRACNJ01
Subnets: 1 IPv4 and 0 IPv6
Quorum Configuration: ⚠ Node Majority - Warning: Failure of a node will cause the cluster to fail. Check the status of the nodes.
Recent Cluster Events: ⚠ Error: 1

Configure Cluster Quorum Wizard

Select Quorum Configuration

Read the descriptions and then select a quorum configuration for your cluster. The recommendations are based on providing the highest availability for your cluster.

○ Node Majority (not recommended for your current number of nodes)
Can sustain failures of 0 node(s).

○ Node and Disk Majority (recommended for your current number of nodes)
Can sustain failures of 1 node(s) with the disk witness online.
Can sustain failures of 0 node(s) if the disk witness goes offline or fails.

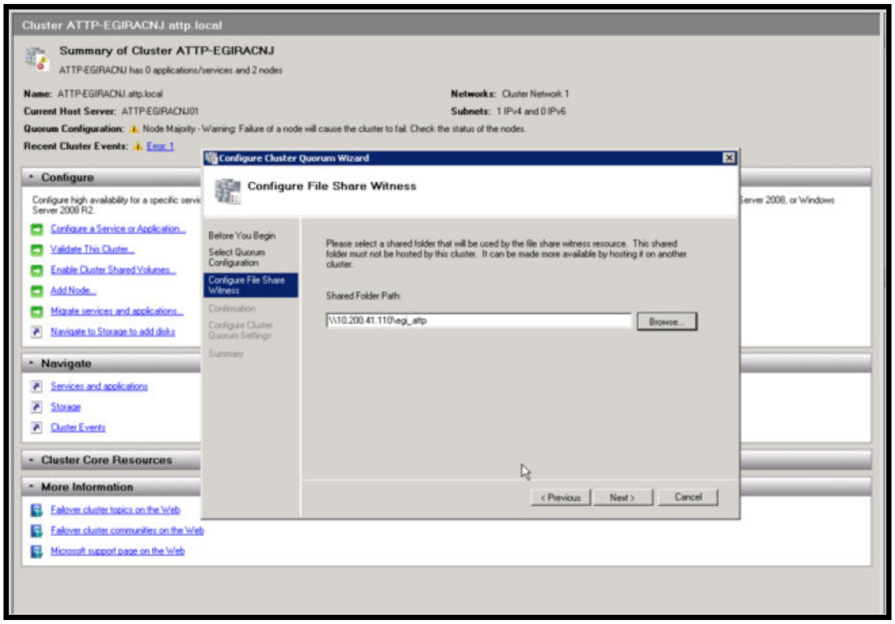
● Node and File Share Majority (for clusters with special configurations)
Can sustain failures of 1 node(s) if the file share witness remains available.
Can sustain failures of 0 node(s) if the file share witness becomes unavailable.

○ No Majority: Disk Only (not recommended)
Can sustain failures of all nodes except 1. Cannot sustain a failure of the quorum disk. This configuration is not recommended because the disk is a single point of failure.

Configure
Configure high availability for a specific servi
Server 2008 R2.
Server 2008, or Windows
Configure a Service or Application...
Validate This Cluster...
Enable Cluster Shared Volumes...
Add Node...
Migrate services and applications...
Navigate to Storage to add disks
Navigate
Services and applications
Storage
Cluster Events
Cluster Core Resources
More Information
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web
Before You Begin
Select Quorum Configuration
Configure File Share Witness
Confirmation
Configure Cluster Quorum Settings
Summary
More about quorum configurations
< Previous
Next >
Cancel

Figure 3.65: Selecting the Node and File Sharing Majority option

3. In the **Shared Folder Path** text box of Figure 3.66, enter the full path to the shared folder that you had created earlier on the file share server (refer to Section **3.3.8.2**). Then, click the **Next** button.



Cluster ATTP-EGIRACNJ.attp.local

Summary of Cluster ATTP-EGIRACNJ

ATTP-EGIRACNJ has 0 applications/services and 2 nodes

Name: ATTP-EGIRACNJ.attp.local
Networks: Cluster Network 1
Current Host Server: ATTP-EGIRACNJ01
Subnets: 1 IPv4 and 0 IPv6
Quorum Configuration: ⚠ Node Majority - Warning: Failure of a node will cause the cluster to fail. Check the status of the nodes.
Recent Cluster Events: ⚠ Error: 1

Configure Cluster Quorum Wizard

Configure File Share Witness

Please select a shared folder that will be used by the file share witness resource. This shared folder must not be hosted by this cluster. It can be made more available by hosting it on another cluster.

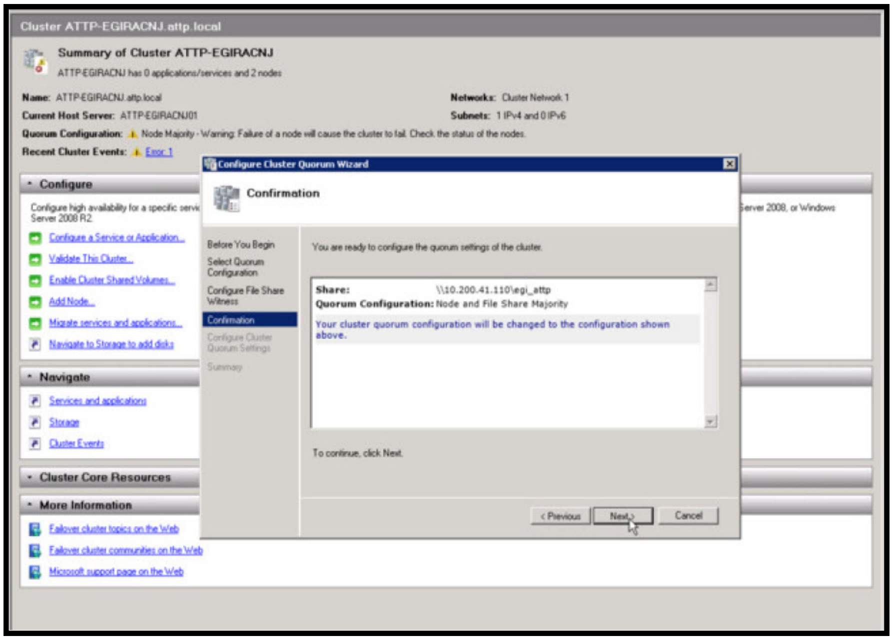
Shared Folder Path: \\10.200.41.110\egi_attp

Configure
Configure high availability for a specific servi
Server 2008 R2.
Server 2008, or Windows
Configure a Service or Application...
Validate This Cluster...
Enable Cluster Shared Volumes...
Add Node...
Migrate services and applications...
Navigate to Storage to add disks
Navigate
Services and applications
Storage
Cluster Events
Cluster Core Resources
More Information
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web
Before You Begin
Select Quorum Configuration
Configure File Share Witness
Confirmation
Configure Cluster Quorum Settings
Summary
Browse...
< Previous
Next >
Cancel

Figure 3.66: Entering the full path to the shared folder

4. Review the quorum settings once more in Figure 3.67, and click the **Next** button to proceed with

the settings.


Cluster ATTP-EGIRACNJ.attp.local
Configure Cluster Quorum Wizard
Confirmation
Configure
Configure a Service or Application...
Validate This Cluster...
Enable Cluster Shared Volumes...
Add Node...
Migrate services and applications...
Navigate to Storage to add disks
Navigate
Services and applications
Storage
Cluster Events
Cluster Core Resources
More Information
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web
Before You Begin
Select Quorum Configuration
Configure File Share Witness
Confirmation
Configure Cluster Quorum Settings
Summary
< Previous
Next >
Cancel

Summary of Cluster ATTP-EGIRACNJ

ATTP-EGIRACNJ has 0 applications/services and 2 nodes

Name: ATTP-EGIRACNJ.attp.local

Current Host Server: ATTP-EGIRACNJ01

Quorum Configuration: Node Majority - Warning: Failure of a node will cause the cluster to fail. Check the status of the nodes.

Recent Cluster Events: Error: 1

Networks: Cluster Network 1

Subnets: 1 IPv4 and 0 IPv6

Configure high availability for a specific servic ... Server 2008, or Windows Server 2008 R2.

You are ready to configure the quorum settings of the cluster.

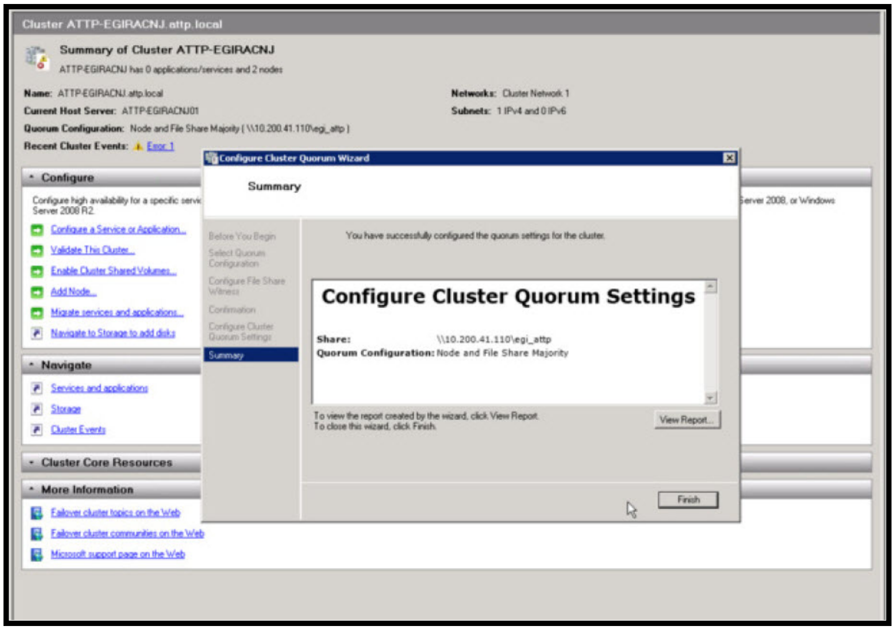
Share: \\10.200.41.110\egi_attp
Quorum Configuration: Node and File Share Majority

Your cluster quorum configuration will be changed to the configuration shown above.

To continue, click Next.

Figure 3.67: Reviewing the quorum settings

5. Click the **Finish** button in Figure 3.68 to end the quorum configuration process.


Cluster ATTP-EGIRACNJ.attp.local
Configure Cluster Quorum Wizard
Summary
Configure
Configure a Service or Application...
Validate This Cluster...
Enable Cluster Shared Volumes...
Add Node...
Migrate services and applications...
Navigate to Storage to add disks
Navigate
Services and applications
Storage
Cluster Events
Cluster Core Resources
More Information
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web
Before You Begin
Select Quorum Configuration
Configure File Share Witness
Confirmation
Configure Cluster Quorum Settings
Summary
View Report...
Finish

Summary of Cluster ATTP-EGIRACNJ

ATTP-EGIRACNJ has 0 applications/services and 2 nodes

Name: ATTP-EGIRACNJ.attp.local

Current Host Server: ATTP-EGIRACNJ01

Quorum Configuration: Node and File Share Majority (\\10.200.41.110\egi_attp)

Recent Cluster Events: Error: 1

Networks: Cluster Network 1

Subnets: 1 IPv4 and 0 IPv6

Configure high availability for a specific servic ... Server 2008, or Windows Server 2008 R2.

You have successfully configured the quorum settings for the cluster.

Configure Cluster Quorum Settings

Share: \\10.200.41.110\egi_attp
Quorum Configuration: Node and File Share Majority

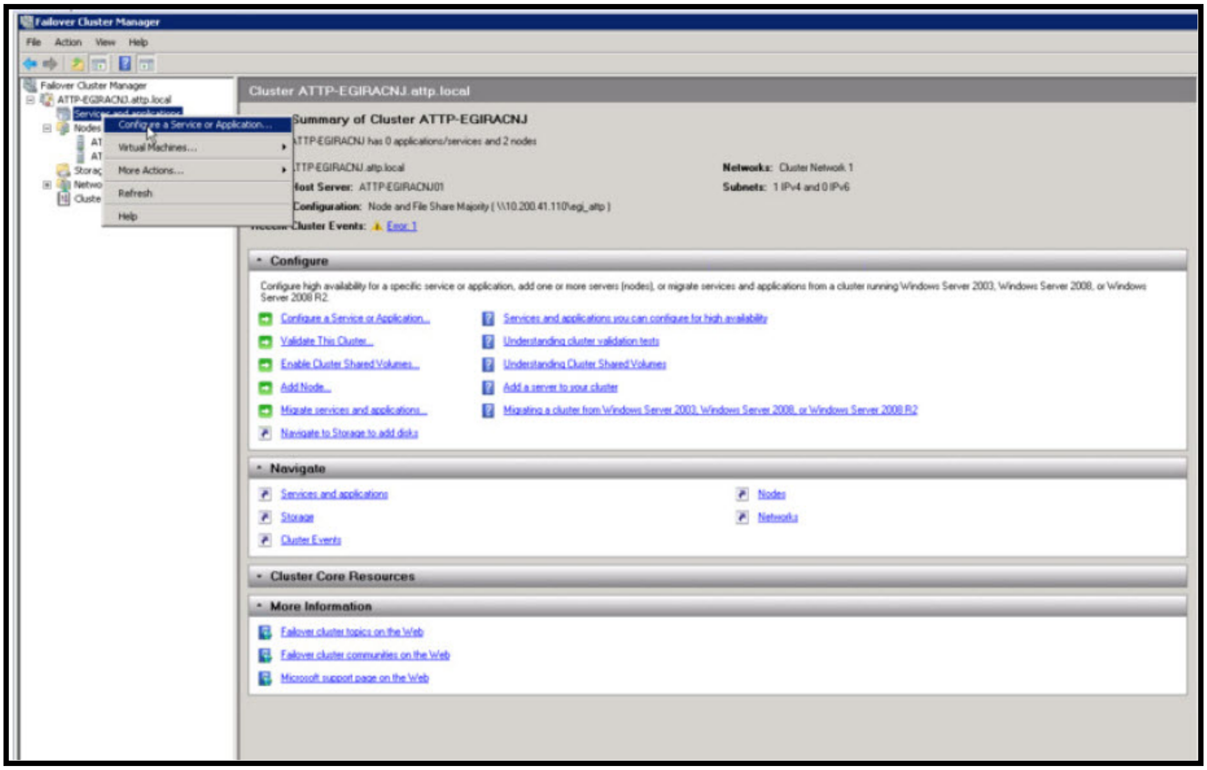
To view the report created by the wizard, click View Report.
To close this wizard, click Finish.

Figure 3.68: Completion of quorum configuration

3.3.8.4 Adding the eG Agent Service as a Cluster Resource

The final step is to add the eGurkhaAgent service as a cluster resource. For this, follow the steps discussed hereunder:

1. Launch the **Failover Cluster Manager**. In the tree-view in the left panel of the manager, expand the node representing the cluster, and right-click on the **Services and Applications** sub-node within. Then, pick the **Configure a Service or Application** option from the shortcut menu that pops up.


Failover Cluster Manager
File
Action
View
Help
Failover Cluster Manager
ATTP-EGIRACNJ.attp.local
Services and applications
Nodes
AT
AT
Storag
Netwo
Cluste
Configure a Service or Application...
Virtual Machines...
More Actions...
Refresh
Help
Cluster ATTP-EGIRACNJ.attp.local
Configure
Configure a Service or Application...
Validate This Cluster...
Enable Cluster Shared Volumes...
Add Node...
Migrate services and applications...
Navigate to Storage to add disks
Services and applications you can configure for high availability
Understanding cluster validation tests
Understanding Cluster Shared Volumes
Add a server to your cluster
Migrating a cluster from Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2
Navigate
Services and applications
Storage
Cluster Events
Nodes
Networks
Cluster Core Resources
More Information
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web

Summary of Cluster ATTP-EGIRACNJ

ATTP-EGIRACNJ has 0 applications/services and 2 nodes

ATTP-EGIRACNJ.attp.local

Host Server: ATTP-EGIRACNJ01

Configuration: Node and File Share Majority (\\10.200.41.110\egi_attp)

Recent Cluster Events: Error: 1

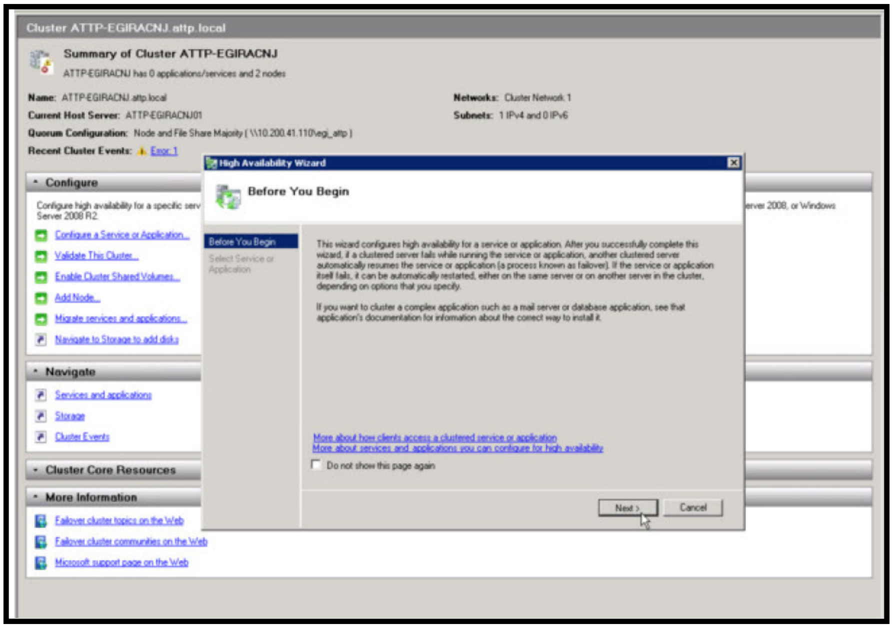
Networks: Cluster Network 1

Subnets: 1 IPv4 and 0 IPv6

Configure high availability for a specific service or application, add one or more servers (nodes), or migrate services and applications from a cluster running Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2.

Figure 3.69: Choosing to configure a service or application

2. When the wizard opens, click the **Next** button in the welcome screen of the wizard to proceed to the next step of the service configuration process.



Cluster ATTP-EGIRACNJ.attp.local

Summary of Cluster ATTP-EGIRACNJ

ATTP-EGIRACNJ has 0 applications/services and 2 nodes

Name: ATTP-EGIRACNJ.attp.local

Current Host Server: ATTP-EGIRACNJ01

Quorum Configuration: Node and File Share Majority (\\10.200.41.110\egi_attp)

Recent Cluster Events: Error: 1

Networks: Cluster Network 1

Subnets: 1 IPv4 and 0 IPv6

High Availability Wizard

Before You Begin

This wizard configures high availability for a service or application. After you successfully complete this wizard, if a clustered server fails while running the service or application, another clustered server automatically resumes the service or application (a process known as failover). If the service or application itself fails, it can be automatically restarted, either on the same server or on another server in the cluster, depending on options that you specify.

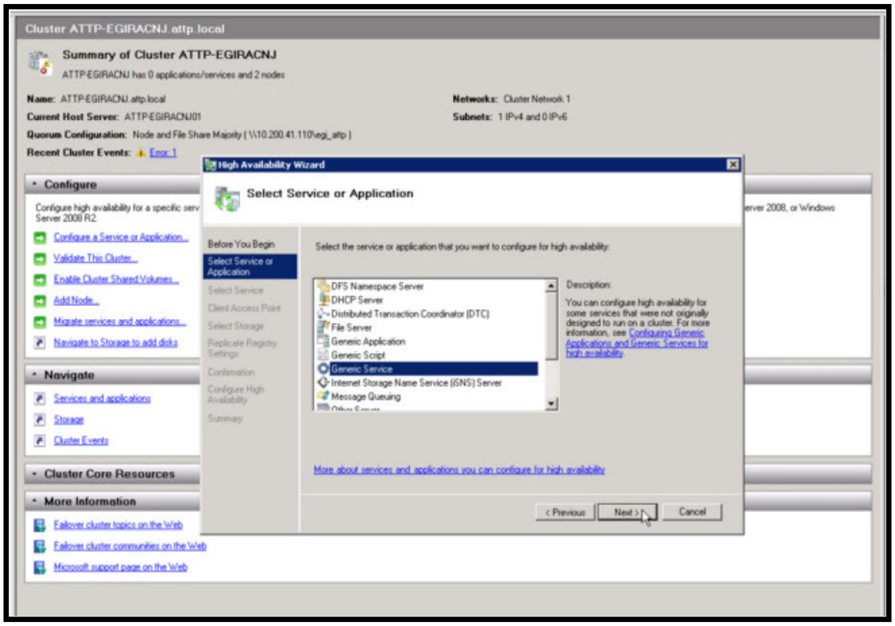
If you want to cluster a complex application such as a mail server or database application, see that application's documentation for information about the correct way to install it.

□ Do not show this page again

Configure
Configure high availability for a specific serv
Server 2008 R2
erver 2008, or Windows
Configure a Service or Application...
Validate This Cluster...
Enable Cluster Shared Volumes...
Add Node...
Migrate services and applications...
Navigate to Storage to add disks
Navigate
Services and applications
Storage
Cluster Events
Cluster Core Resources
More Information
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web
Before You Begin
Select Service or Application
More about how clients access a clustered service or application
More about services and applications you can configure for high availability
Next >
Cancel

Figure 3.70: The welcome screen of the High Availability wizard

3. When Figure 3.71 appears, select the **Generic Service** option and click the **Next** button.



Cluster ATTP-EGIRACNJ.attp.local

Summary of Cluster ATTP-EGIRACNJ

ATTP-EGIRACNJ has 0 applications/services and 2 nodes

Name: ATTP-EGIRACNJ.attp.local

Current Host Server: ATTP-EGIRACNJ01

Quorum Configuration: Node and File Share Majority (\\10.200.41.110\egi_attp)

Recent Cluster Events: Error: 1

Networks: Cluster Network 1

Subnets: 1 IPv4 and 0 IPv6

High Availability Wizard

Select Service or Application

Select the service or application that you want to configure for high availability:

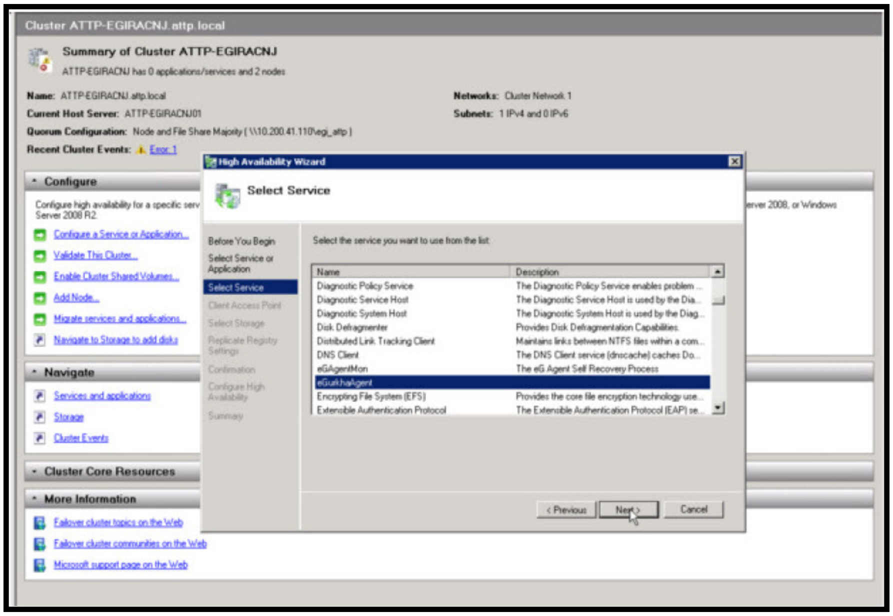
Description:

You can configure high availability for some services that were not originally designed to run on a cluster. For more information, see Configuring Generic Applications and Generic Services for high availability.

Configure
Configure high availability for a specific serv
Server 2008 R2
erver 2008, or Windows
Configure a Service or Application...
Validate This Cluster...
Enable Cluster Shared Volumes...
Add Node...
Migrate services and applications...
Navigate to Storage to add disks
Navigate
Services and applications
Storage
Cluster Events
Cluster Core Resources
More Information
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web
Before You Begin
Select Service or Application
Select Service
Client Access Point
Select Storage
Replicate Registry Settings
Confirmation
Configure High Availability
Summary
DFS Namespace Server
DHCP Server
Distributed Transaction Coordinator (DTC)
File Server
Generic Application
Generic Script
Generic Service
Internet Storage Name Service (iSNS) Server
Message Queuing
Other Server
More about services and applications you can configure for high availability
< Previous
Next >
Cancel

Figure 3.71: Selecting the Generic Service option

4. In Figure 3.72, select the **eGurkhaAgent** service from the list of services displayed therein and click the **Next** button.



Cluster ATTP-EGIRACNJ.attp.local

Summary of Cluster ATTP-EGIRACNJ

ATTP-EGIRACNJ has 0 applications/services and 2 nodes

Name: ATTP-EGIRACNJ.attp.local

Current Host Server: ATTP-EGIRACNJ01

Quorum Configuration: Node and File Share Majority (\\10.200.41.110\egi_attp)

Recent Cluster Events: Error: 1

Networks: Cluster Network 1

Subnets: 1 IPv4 and 0 IPv6

High Availability Wizard

Select Service

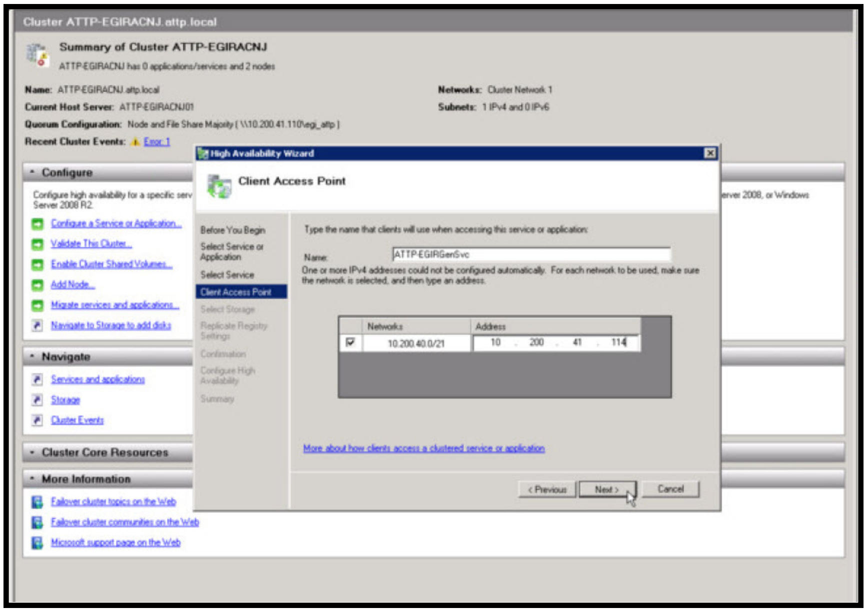
Select the service you want to use from the list:

Name	Description
Diagnostic Policy Service	The Diagnostic Policy Service enables problem ...
Diagnostic Service Host	The Diagnostic Service Host is used by the Dia...
Diagnostic System Host	The Diagnostic System Host is used by the Diag...
Disk Defragmenter	Provides Disk Defragmentation Capabilities.
Distributed Link Tracking Client	Maintains links between NTFS files within a com...
DNS Client	The DNS Client service (dnscache) caches Do...
eGAgentMon	The eG Agent Self Recovery Process
eGurkhaAgent	
Encrypting File System (EFS)	Provides the core file encryption technology use...
Extensible Authentication Protocol	The Extensible Authentication Protocol (EAP) se...

Configure
Configure high availability for a specific serv
Server 2008 R2.
erver 2008, or Windows
Configure a Service or Application...
Validate This Cluster...
Enable Cluster Shared Volumes...
Add Node...
Migrate services and applications...
Navigate to Storage to add disks
Navigate
Services and applications
Storage
Cluster Events
Cluster Core Resources
More Information
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web
Before You Begin
Select Service or Application
Select Service
Client Access Point
Select Storage
Replicate Registry Settings
Confirmation
Configure High Availability
Summary
< Previous
Next >
Cancel

Figure 3.72: Selecting the eGurhaAgent service

5. In the **Client Access Point** page that appears next, provide input for the network name and IP addresses that clients will be using when accessing the **eGurkhaAgent** service. Then, click the **Next** button in Figure 3.73.



Cluster ATTP-EGIRACNJ.attp.local

Summary of Cluster ATTP-EGIRACNJ

ATTP-EGIRACNJ has 0 applications/services and 2 nodes

Name: ATTP-EGIRACNJ.attp.local

Current Host Server: ATTP-EGIRACNJ01

Quorum Configuration: Node and File Share Majority (\\10.200.41.110\egi_attp)

Recent Cluster Events: Error: 1

Networks: Cluster Network 1

Subnets: 1 IPv4 and 0 IPv6

High Availability Wizard

Client Access Point

Type the name that clients will use when accessing this service or application:

Name: ATTP-EGIRGenSvc

One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.

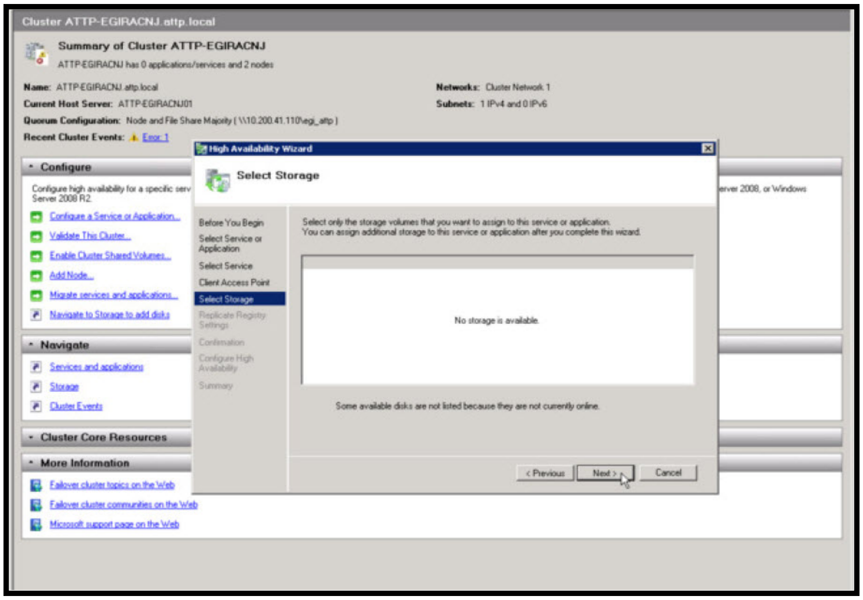
	Networks	Address
☑	10.200.40.0/21	10 . 200 . 41 . 114

More about how clients access a clustered service or application

Configure
Configure high availability for a specific serv
Server 2008 R2.
erver 2008, or Windows
Configure a Service or Application...
Validate This Cluster...
Enable Cluster Shared Volumes...
Add Node...
Migrate services and applications...
Navigate to Storage to add disks
Navigate
Services and applications
Storage
Cluster Events
Cluster Core Resources
More Information
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web
Before You Begin
Select Service or Application
Select Service
Client Access Point
Select Storage
Replicate Registry Settings
Confirmation
Configure High Availability
Summary
< Previous
Next >
Cancel

Figure 3.73: Entering the network name and IP address using which clients will be accessing the clustered resource

6. When Figure 3.74, click on the **Next** button to move on.



Cluster ATTP-EGIRACNJ.attp.local

Summary of Cluster ATTP-EGIRACNJ

ATTP-EGIRACNJ has 0 applications/services and 2 nodes

Name: ATTP-EGIRACNJ.attp.local
Current Host Server: ATTP-EGIRACNJ01
Quorum Configuration: Node and File Share Majority (\\10.200.41.110\egi_attp)
Recent Cluster Events: Error: 1
Networks: Cluster Network 1
Subnets: 1 IPv4 and 0 IPv6

Configure high availability for a specific serv... erver 2008, or Windows Server 2008 R2.

High Availability Wizard

Select Storage

Select only the storage volumes that you want to assign to this service or application.
You can assign additional storage to this service or application after you complete this wizard.

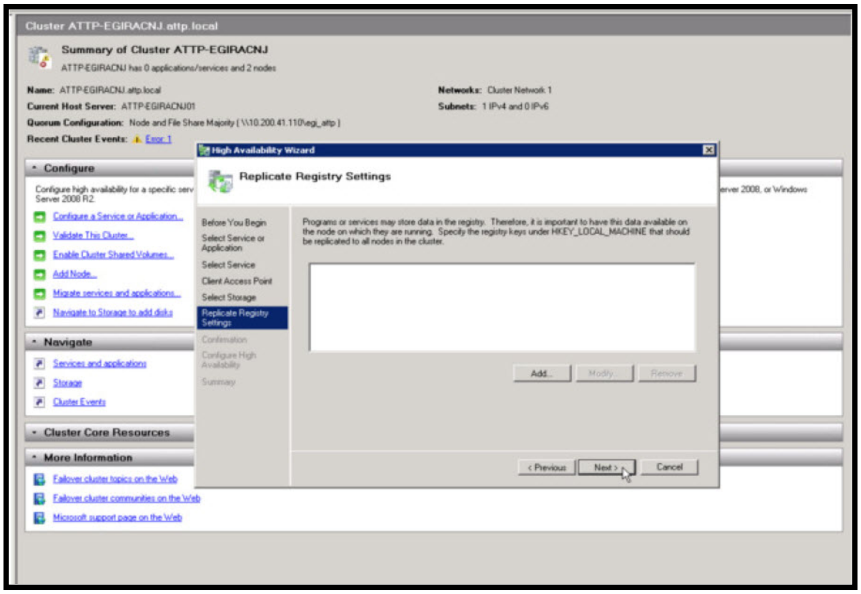
No storage is available.

Some available disks are not listed because they are not currently online.

Configure
Configure a Service or Application...
Validate This Cluster...
Enable Cluster Shared Volumes...
Add Node...
Migrate services and applications...
Navigate to Storage to add disks
Navigate
Services and applications
Storage
Cluster Events
Cluster Core Resources
More Information
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web
Before You Begin
Select Service or Application
Select Service
Client Access Point
Select Storage
Replicate Registry Settings
Confirmation
Configure High Availability
Summary
< Previous
Next >
Cancel

Figure 3.74: Clicking the Next button in the Select Storage page

7. To skip the **Replicate Registry Settings** page and move to the next step, click the **Next** button in Figure 3.75.



Cluster ATTP-EGIRACNJ.attp.local

Summary of Cluster ATTP-EGIRACNJ

ATTP-EGIRACNJ has 0 applications/services and 2 nodes

Name: ATTP-EGIRACNJ.attp.local
Current Host Server: ATTP-EGIRACNJ01
Quorum Configuration: Node and File Share Majority (\\10.200.41.110\egi_attp)
Recent Cluster Events: Error: 1
Networks: Cluster Network 1
Subnets: 1 IPv4 and 0 IPv6

Configure high availability for a specific serv... erver 2008, or Windows Server 2008 R2.

High Availability Wizard

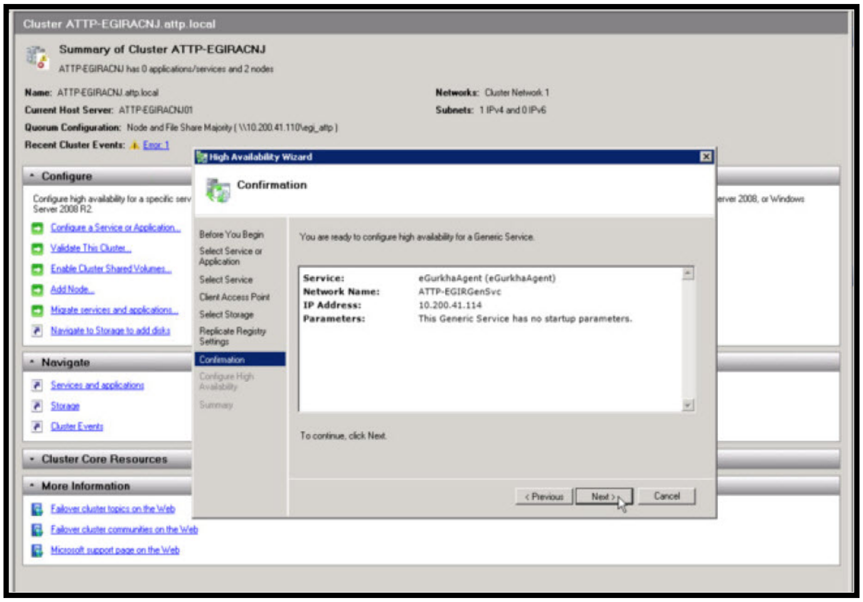
Replicate Registry Settings

Programs or services may store data in the registry. Therefore, it is important to have this data available on the node on which they are running. Specify the registry keys under HKEY_LOCAL_MACHINE that should be replicated to all nodes in the cluster.

Configure
Configure a Service or Application...
Validate This Cluster...
Enable Cluster Shared Volumes...
Add Node...
Migrate services and applications...
Navigate to Storage to add disks
Navigate
Services and applications
Storage
Cluster Events
Cluster Core Resources
More Information
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web
Before You Begin
Select Service or Application
Select Service
Client Access Point
Select Storage
Replicate Registry Settings
Confirmation
Configure High Availability
Summary
Add...
Modify...
Remove
< Previous
Next >
Cancel

Figure 3.75: Skipping the Replicate Registry Settings page

8. Once the **Confirmation** page appears (see Figure 3.76), quickly review the service configuration displayed therein, and click the **Next** button to confirm the addition of that service as a clustered resource.



Cluster ATTP-EGIRACNJ.attp.local

Summary of Cluster ATTP-EGIRACNJ

ATTP-EGIRACNJ has 0 applications/services and 2 nodes

Name: ATTP-EGIRACNJ.attp.local

Current Host Server: ATTP-EGIRACNJ01

Quorum Configuration: Node and File Share Majority (\\10.200.41.110\egi_attp)

Recent Cluster Events: Error: 1

Networks: Cluster Network 1

Subnets: 1 IPv4 and 0 IPv6

High Availability Wizard

Confirmation

You are ready to configure high availability for a Generic Service.

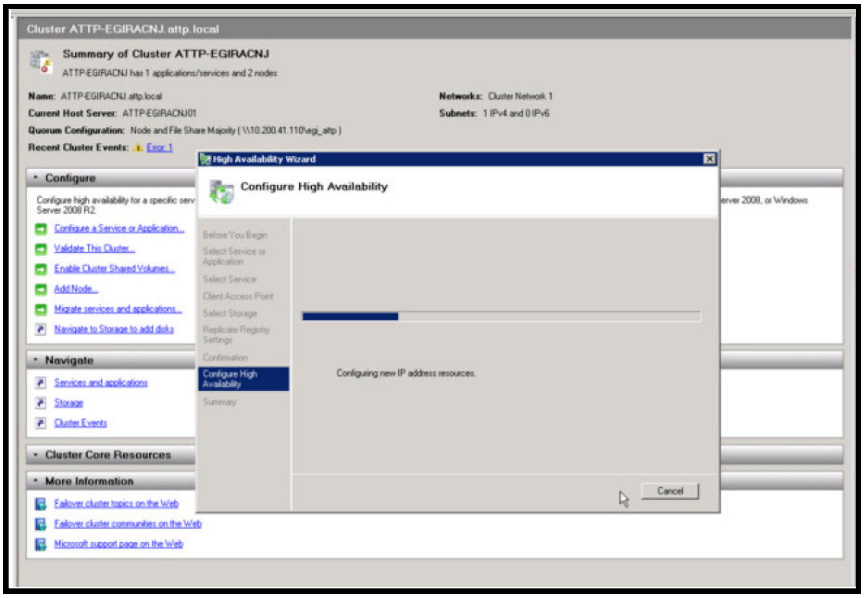
```
Service:          eGurkhaAgent (eGurkhaAgent)
Network Name:     ATTP-EGIRGenSvc
IP Address:       10.200.41.114
Parameters:       This Generic Service has no startup parameters.
```

To continue, click Next.

Configure
Configure high availability for a specific serv... Server 2008 R2.
...erver 2008, or Windows
Configure a Service or Application...
Validate This Cluster...
Enable Cluster Shared Volumes...
Add Node...
Migrate services and applications...
Navigate to Storage to add disks
Navigate
Services and applications
Storage
Cluster Events
Cluster Core Resources
More Information
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web
Before You Begin
Select Service or Application
Select Service
Client Access Point
Select Storage
Replicate Registry Settings
Confirmation
Configure High Availability
Summary
< Previous
Next >
Cancel

Figure 3.76: Reviewing the service configuration

9. Upon confirmation, the cluster manager will then begin configuring the high availability of the **eGurkhaAgent** service (see Figure 3.77).



Cluster ATTP-EGIRACNJ.attp.local

Summary of Cluster ATTP-EGIRACNJ

ATTP-EGIRACNJ has 1 applications/services and 2 nodes

Name: ATTP-EGIRACNJ.attp.local

Current Host Server: ATTP-EGIRACNJ01

Quorum Configuration: Node and File Share Majority (\\10.200.41.110\egi_attp)

Recent Cluster Events: Error: 1

Networks: Cluster Network 1

Subnets: 1 IPv4 and 0 IPv6

High Availability Wizard

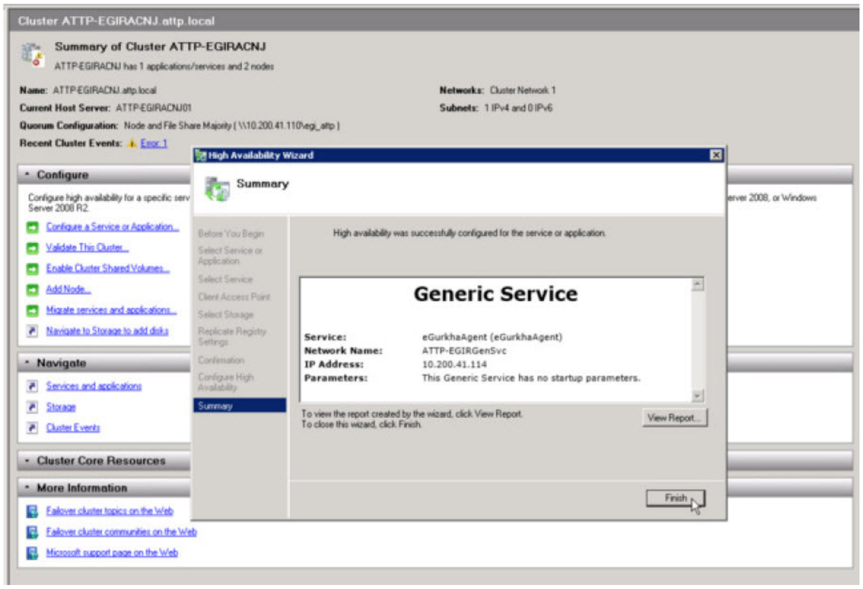
Configure High Availability

Configuring new IP address resources.

Configure
Configure high availability for a specific serv... Server 2008 R2.
...erver 2008, or Windows
Configure a Service or Application...
Validate This Cluster...
Enable Cluster Shared Volumes...
Add Node...
Migrate services and applications...
Navigate to Storage to add disks
Navigate
Services and applications
Storage
Cluster Events
Cluster Core Resources
More Information
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web
Before You Begin
Select Service or Application
Select Service
Client Access Point
Select Storage
Replicate Registry Settings
Confirmation
Configure High Availability
Summary
Cancel

Figure 3.77: High availability configuration in progress for the eGurkhaAgent service

10. Once the configuration process ends, Figure 3.78 appears confirming the successful completion of the high availability configuration, and displaying the details of the **eGurkhaAgent** service for which high availability was configured.



Cluster ATTP-EGIRACNJ.attp.local

Summary of Cluster ATTP-EGIRACNJ

ATTP-EGIRACNJ has 1 applications/services and 2 nodes

Name: ATTP-EGIRACNJ.attp.local

Current Host Server: ATTP-EGIRACNJ01

Quorum Configuration: Node and File Share Majority (\\10.200.41.110\egi_attp)

Recent Cluster Events: ⚠ Error: 1

Networks: Cluster Network 1

Subnets: 1 IPv4 and 0 IPv6

Configure high availability for a specific serv ... erver 2008, or Windows Server 2008 R2

High Availability Wizard

Summary

High availability was successfully configured for the service or application.

Generic Service

Service: eGurkhaAgent (eGurkhaAgent)
Network Name: ATTP-EGIRGenSvc
IP Address: 10.200.41.114
Parameters: This Generic Service has no startup parameters.

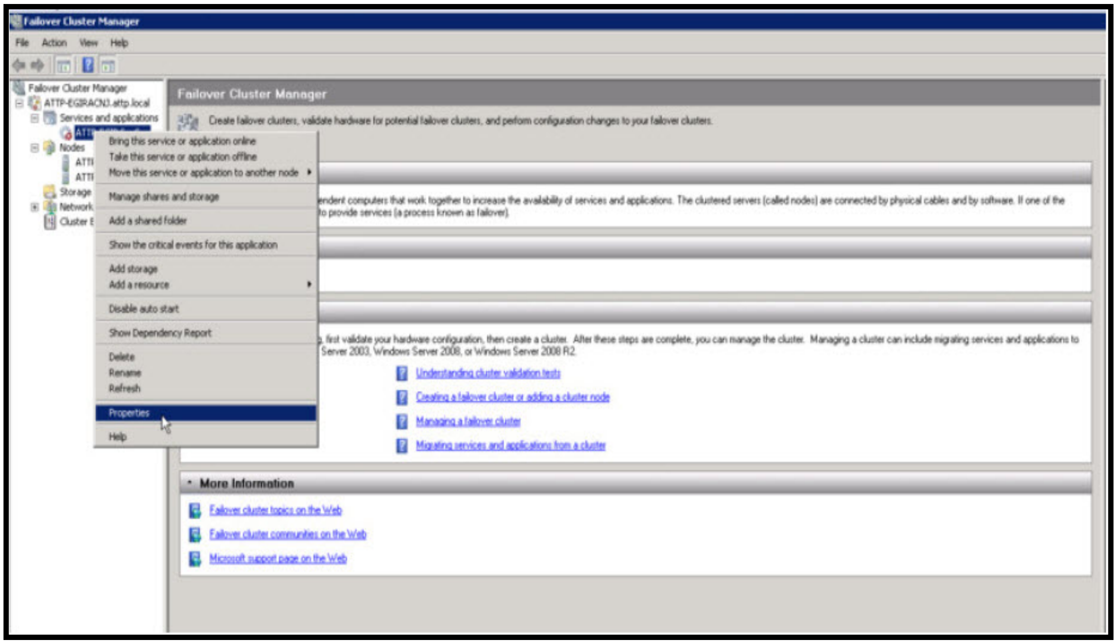
To view the report created by the wizard, click View Report.
To close this wizard, click Finish.

Configure
Configure a Service or Application...
Validate This Cluster...
Enable Cluster Shared Volumes...
Add Node...
Migrate services and applications...
Navigate to Storage to add disks
Navigate
Services and applications
Storage
Cluster Events
Cluster Core Resources
More Information
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web
Before You Begin
Select Service or Application
Select Service
Client Access Point
Select Storage
Replicate Registry Settings
Confirmation
Configure High Availability
Summary
View Report...
Finish

Figure 3.78: A message indicating the successful configuration of high availability for the eGurkhaAgent service

11. Click the **Finish** button in Figure 3.78 to exit the wizard.

12. Now, proceed to indicate which node in the failover cluster owns the **eGurkhaAgent** service. For that, expand the **Services and Applications** node in the tree-structure in the left panel of the **Failover Cluster Manager**, and right-click on the sub-node representing the **eGurkhaAgent** service. From the shortcut menu that pops up, select the **Properties** option (see Figure 3.79).


Failover Cluster Manager
File Action View Help
Failover Cluster Manager
ATTP-EGIRACN3.attp.local
Services and applications
ATT
Nodes
ATT
ATT
Storage
Network
Cluster E
Failover Cluster Manager
Bring this service or application online
Take this service or application offline
Move this service or application to another node
Manage shares and storage
Add a shared folder
Show the critical events for this application
Add storage
Add a resource
Disable auto start
Show Dependency Report
Delete
Rename
Refresh
Properties
Help
More Information
Understanding cluster validation tests
Creating a failover cluster or adding a cluster node
Managing a failover cluster
Migrating services and applications from a cluster
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web

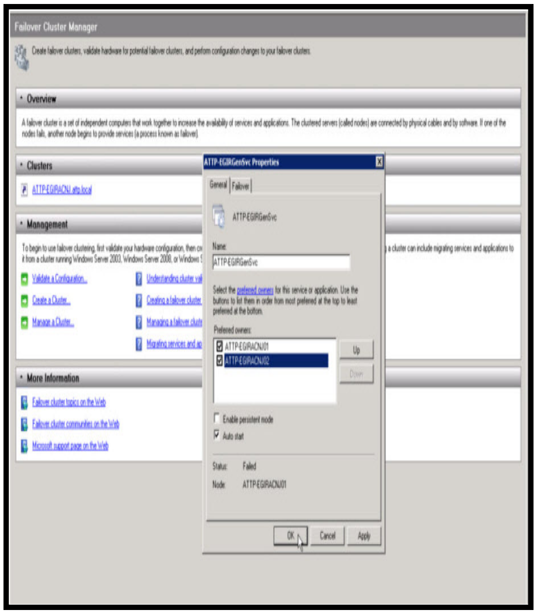
Create failover clusters, validate hardware for potential failover clusters, and perform configuration changes to your failover clusters.

endent computers that work together to increase the availability of services and applications. The clustered servers (called nodes) are connected by physical cables and by software. If one of the to provide services (a process known as failover).

, first validate your hardware configuration, then create a cluster. After these steps are complete, you can manage the cluster. Managing a cluster can include migrating services and applications to Server 2003, Windows Server 2008, or Windows Server 2008 R2.

Figure 3.79: Editing the Properties of the eGurkhaAgent service that has been added as a cluster resource

13. Figure 3.80 then appears. In the **General** tab of Figure 3.80, the nodes added to the failover cluster you have created will be listed in the **Preferred owners** section. You can either set a single node as the owner of the service by selecting the check box that corresponds to that node; in this case, you will have to deselect the check box corresponding to the other node. You can also have both nodes as the owners of the clustered resource and configure the order of preference - i.e., which node should be owner 1 and which should be owner 2. To toggle the order, use the **Up** and **Down** buttons adjacent to the **Preferred owners** box. Then, click the **Apply** and **OK** buttons in Figure 3.80 to save the changes you made.



ATTP-EGIRGenSvc Properties

Name: ATTP-EGIRGenSvc

Select the preferred owners for this service or application. Use the buttons to list them in order from most preferred at the top to least preferred at the bottom.

Preferred owners:

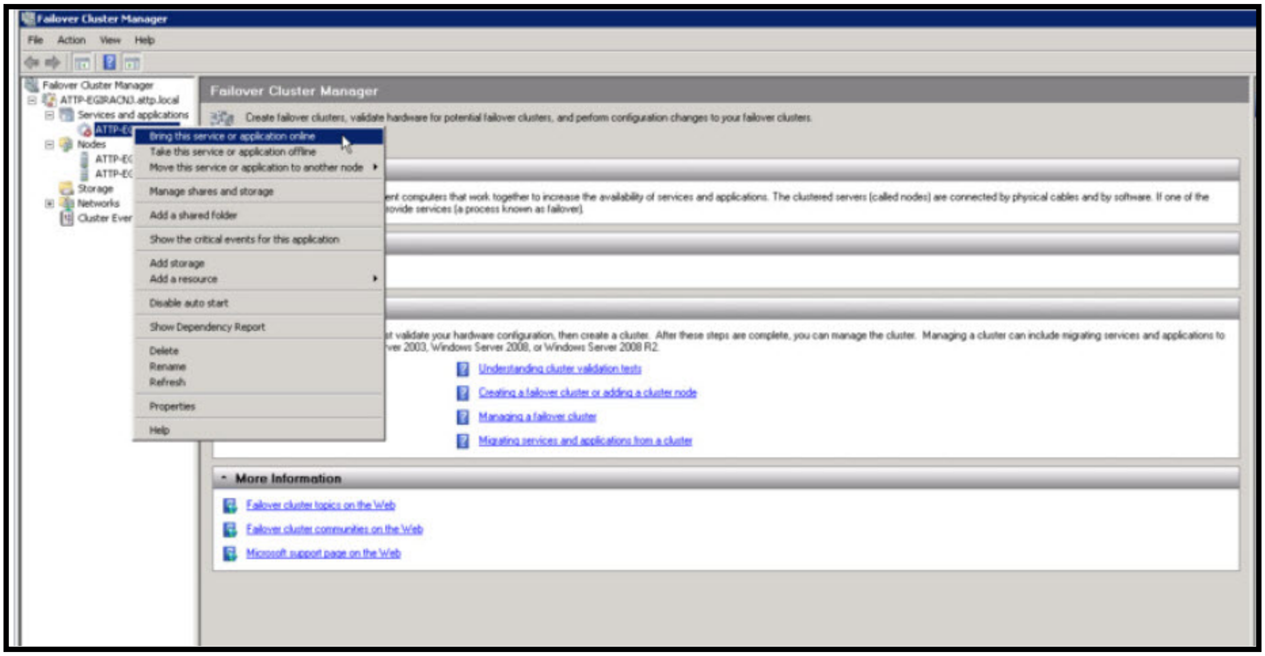
☑ ATTP-EGIRACNJ01
☑ ATTP-EGIRACNJ02

☐ Enable persistent mode
☑ Auto start

Status: Failed
Node: ATTP-EGIRACNJ01

Figure 3.80: Configuring the preferred owners of the clustered eGurkhaAgent service

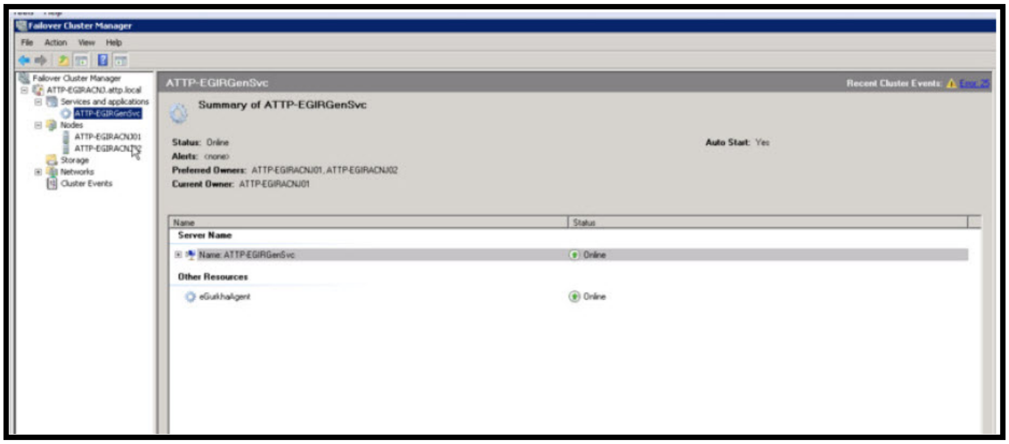
14. Finally, bring the service online. For this, right-click on the node representing the clustered service in the tree-view in the left panel of the **Failover Cluster Manager**, and choose the **Bring service or application online** option (see Figure 3.81).



Failover Cluster Manager
File Action View Help
Failover Cluster Manager
ATTP-EGIRACNJ.attp.local
Services and applications
Nodes
Storage
Networks
Cluster Events
Bring this service or application online
Take this service or application offline
Move this service or application to another node
Manage shares and storage
Add a shared folder
Show the critical events for this application
Add storage
Add a resource
Disable auto start
Show Dependency Report
Delete
Rename
Refresh
Properties
Help
Create failover clusters, validate hardware for potential failover clusters, and perform configuration changes to your failover clusters.
Understanding cluster validation tests
Creating a failover cluster or adding a cluster node
Managing a failover cluster
Migrating services and applications from a cluster
More Information
Failover cluster topics on the Web
Failover cluster communities on the Web
Microsoft support page on the Web

Figure 3.81: Bringing the clustered service online

15. Once the service goes online, Figure 3.82 will appear confirming the same.



Summary of ATTP-EGIRGenSvc

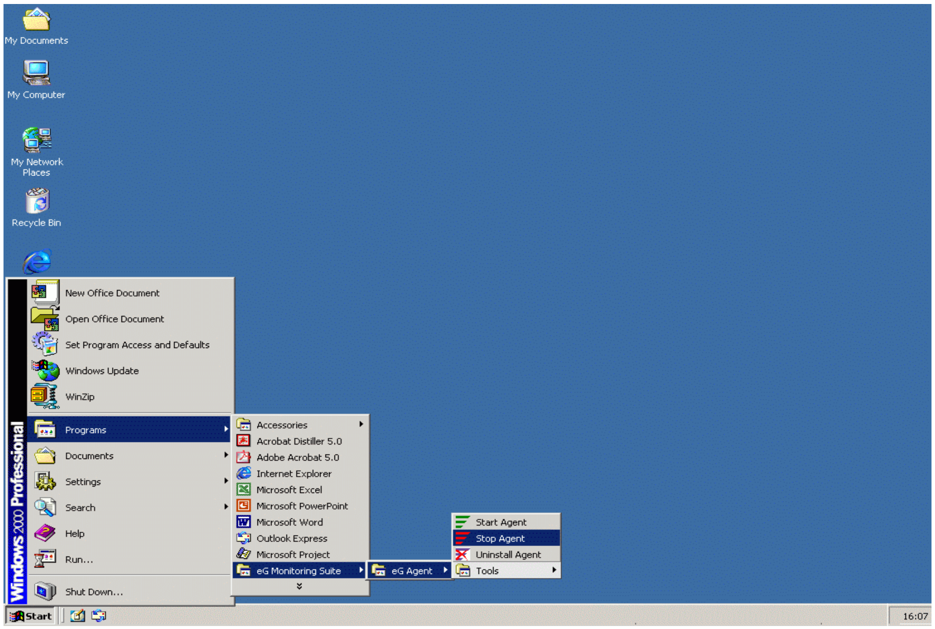
Status: Online
Alerts: <none>
Preferred Owners: ATTP-EGIRACNJ01, ATTP-EGIRACNJ02
Current Owner: ATTP-EGIRACNJ01
Auto Start: Yes

Name	Status
Server Name	
Name: ATTP-EGIRGenSvc	Online
Other Resources	
eGurkhaAgent	Online

Figure 3.82: The right panel of the Failover Cluster Manager indicating that the service is online

3.3.9 Stopping the eG Agent

To stop the eG agent on a Windows host, click the **Start** button on the task bar. From thereon, select All Programs > eG Monitoring Suite > eG Agent > Stop Agent.



Stopping the eG agent

Note that the eG agent can be stopped only by a user with "administrator" privileges. Therefore, before attempting to stop the agent, click on **Start Search** on the task bar of the agent host, right-click on **Command Prompt**, and then select the **Run as administrator** option, as depicted by

Figure 3.83. This implies that the command that is issued at the command prompt soon after, will be run with administrator privileges.

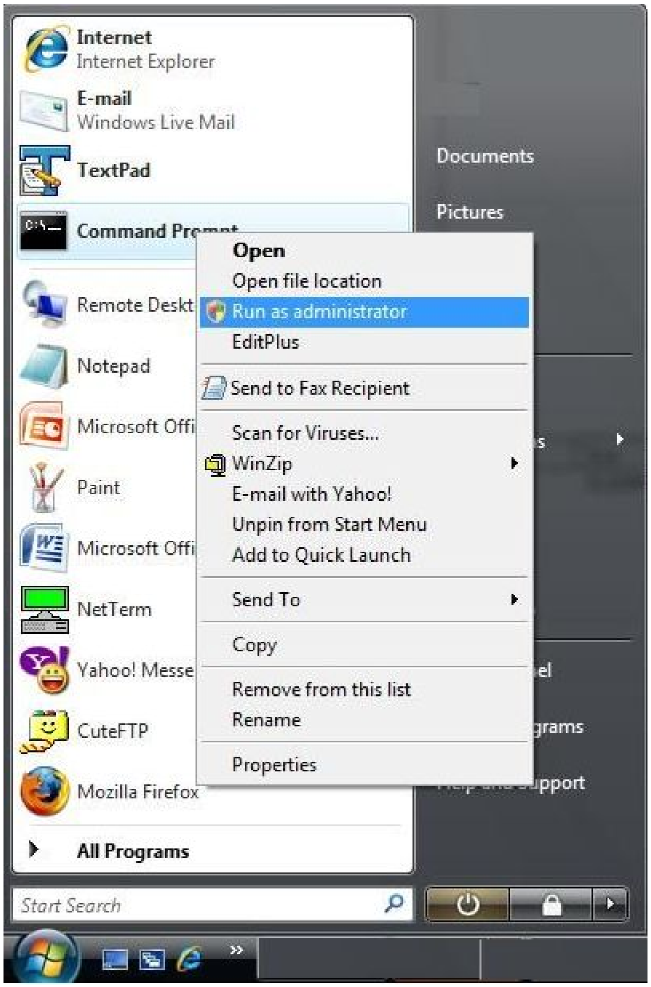


Figure 3.83: Stopping the eG agent on Windows

Then, at the command prompt, switch to the <EG_AGENT_INSTALL_DIR>\bin directory and execute the **stop_agent** command.

In case of Windows 2008, follow the menu sequence depicted by Figure 3.84.

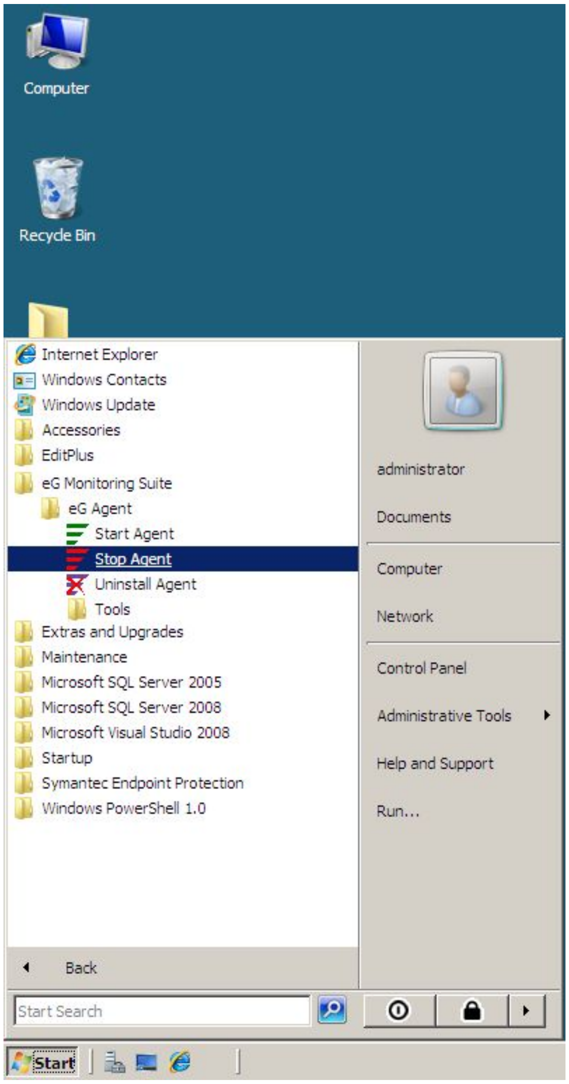
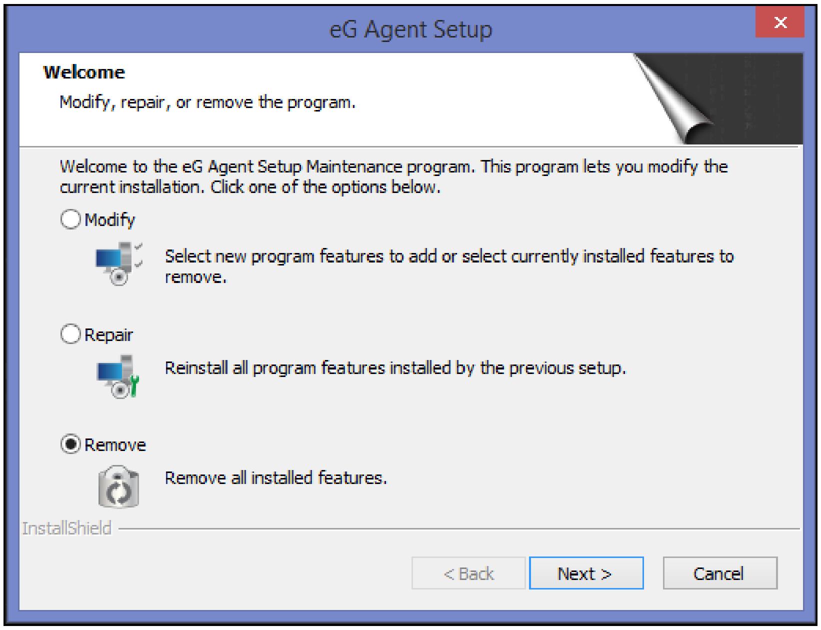


Figure 3.84: Stopping an eG agent on Windows 2008

3.3.10 Uninstalling an eG Agent

1. It is essential to stop the agent before uninstalling it. To stop it, first choose the eG Monitoring Suite option of the Windows Programs menu. Next, choose eG Agent. Finally, select **Stop Agent** from the options available.

2. To uninstall the eG Agent, select Uninstall Agent from the options available under the eG Agent menu. The screen depicted by Figure 3.85 will appear. Here, select the **Remove** option and click the **Next >** button.



eG Agent Setup

Welcome

Modify, repair, or remove the program.

Welcome to the eG Agent Setup Maintenance program. This program lets you modify the current installation. Click one of the options below.

○ Modify

Select new program features to add or select currently installed features to remove.

○ Repair

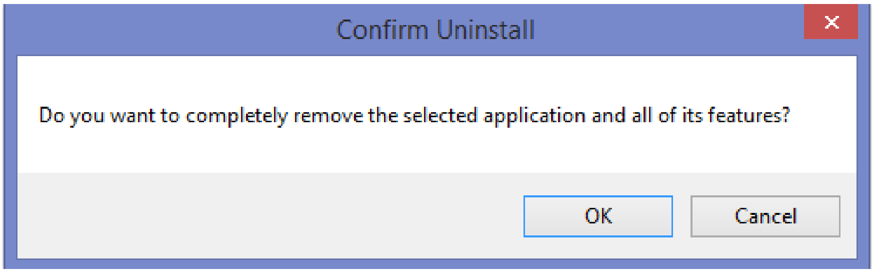
Reinstall all program features installed by the previous setup.

● Remove

Remove all installed features.

Figure 3.85: Uninstalling the eG agent

3. This process requires the confirmation of the user to remove the package and its related components as in Figure 3.86. Click the **OK** button.



Confirm Uninstall

Do you want to completely remove the selected application and all of its features?

Figure 3.86: Uninstall process seeking the confirmation of the user to delete the eG agent

Note:

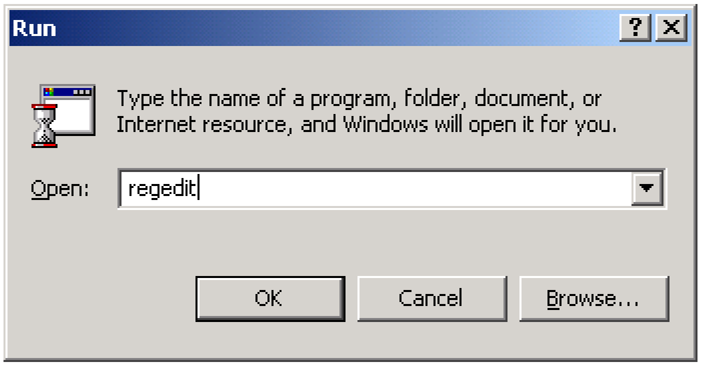
If the eG agent and manager are installed on the same host, then, during uninstallation, it is highly recommended that you uninstall the eG agent first and then the eG manager.

3.3.11 Manually Uninstalling the eG Agent

To manually uninstall the eG agent on Windows, do the following:

1. Stop the eG Agent using the menu sequence: Start -> Programs -> eG Monitoring Suite -> eG Agent -> Stop Agent.

2. Open the Windows registry by typing **regedit** in the **Run** dialog box (which appears upon following the Start -> Run menu sequence), and clicking the **OK** button therein (see Figure 3.87).

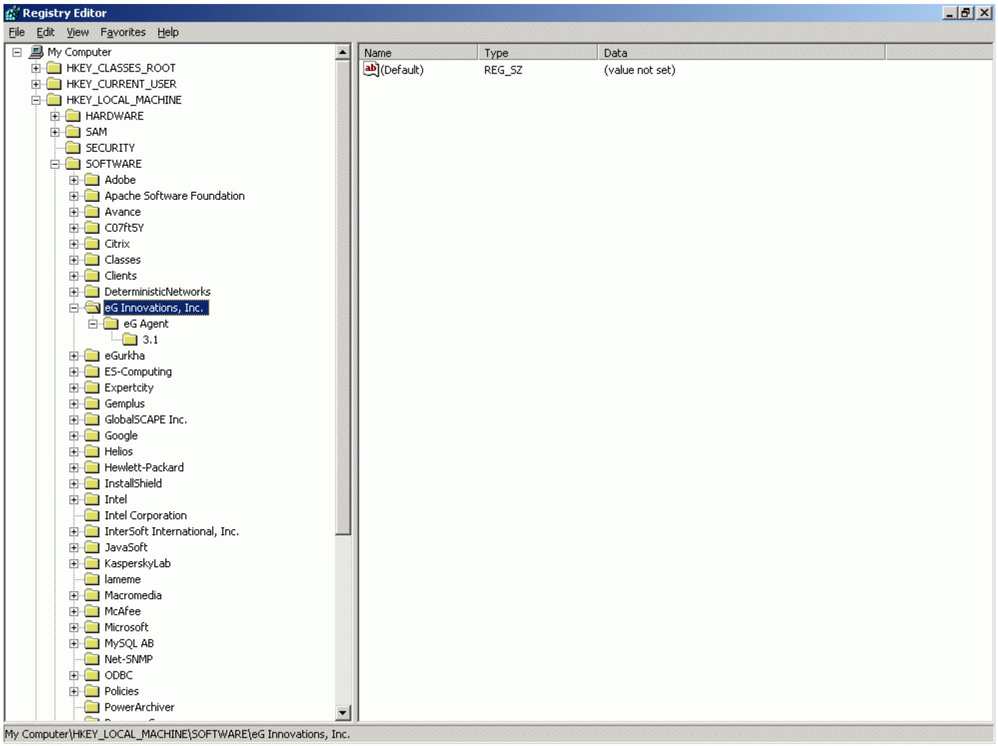


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

Figure 3.87: Opening the Windows registry

3. In the **Registry Editor** (see Figure 3.87) that opens, look for the **eG Innovations, Inc.** entry in the **My Computer\HKEY_LOCAL_MACHINE\SOFTWARE** node sequence (see Figure 3.88).



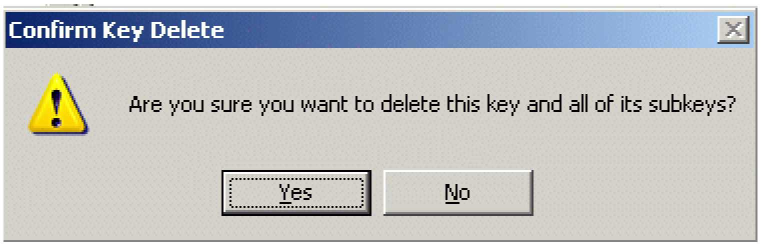
Name	Type	Data
(Default)	REG_SZ	(value not set)

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\eG Innovations, Inc.

Figure 3.88: Selecting the eG Innovations, Inc. entry

4. Delete the selected entry by pressing the **Delete** key on the keyboard, and confirm deletion by

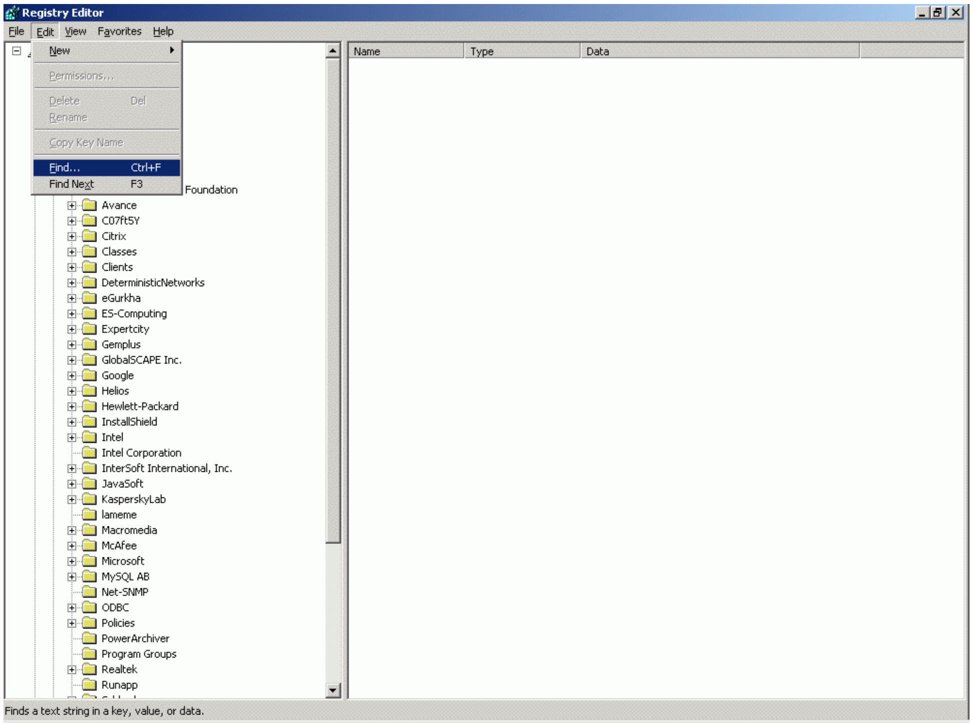
clicking the **OK** button in Figure 3.89 that appears.



Are you sure you want to delete this key and all of its subkeys?

Figure 3.89: Confirming deletion of the selected key

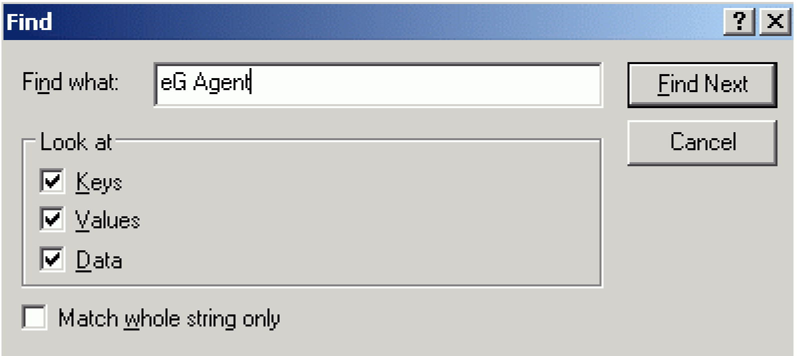
5. Then, place the cursor on the **My Computer** key at the top of the registry tree (see Figure 3.88) and then proceed to choose the **Find** option from the **Edit** menu (see Figure 3.90).



Finds a text string in a key, value, or data.

Figure 3.90: Selecting the Find option

6. When the **Find** dialog box appears (see Figure 3.91), specify **eG Agent** as the string to search for.



Find what: eG Agent

Look at

☑ Keys

☑ Values

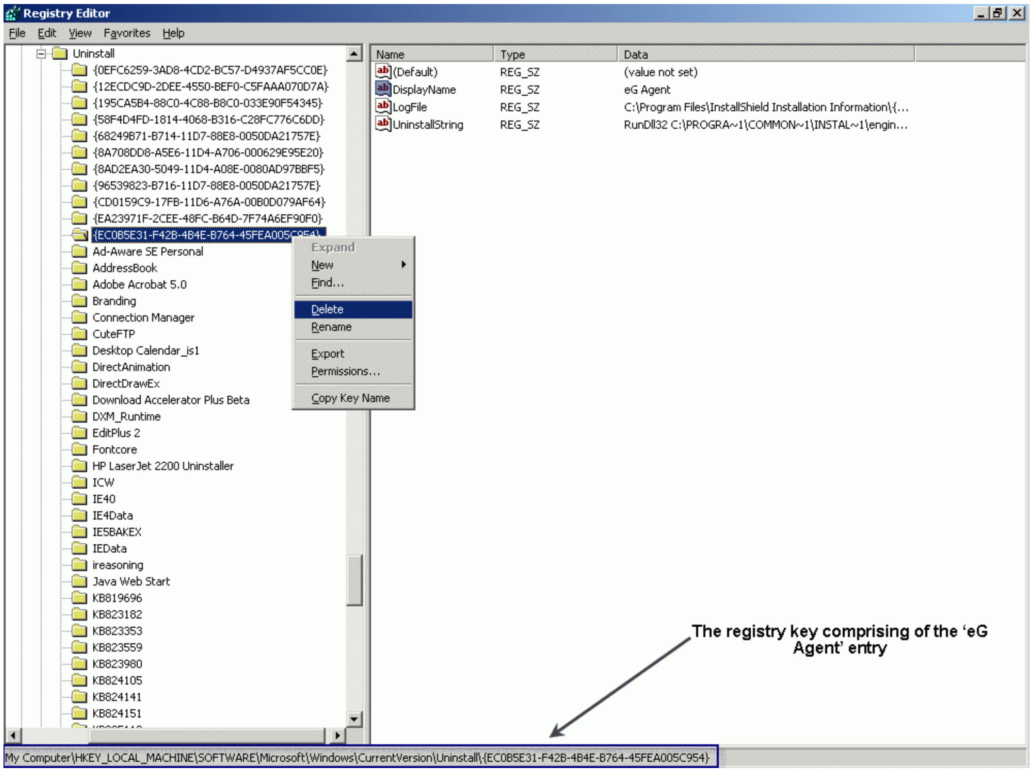
☑ Data

□ Match whole string only

Figure 3.91: Finding the string 'eG Agent'

7. Then, click the **Find Next** button in Figure 3.91 to trigger the search.

8. Continue searching until the **eG Agent** entry present under the key indicated by Figure 3.92 is located.


Registry Editor
File Edit View Favorites Help
Uninstall
{0EFC6259-3AD8-4CD2-BC57-D4937AF5CC0E}
{12ECDC9D-2DEE-4550-BEF0-C5FAAA070D7A}
{195CA5B4-88C0-4C88-B8C0-033E90F54345}
{58F4D4FD-1814-4068-B316-C28FC776C6DD}
{68249B71-B714-11D7-88E8-0050DA21757E}
{8A708DD8-A5E6-11D4-A706-000629E95E20}
{8AD2EA30-5049-11D4-A08E-0080AD97BBF5}
{96539823-B716-11D7-88E8-0050DA21757E}
{CD0159C9-17FB-11D6-A76A-00B0D079AF64}
{EA23971F-2CEE-48FC-B64D-7F74A6EF90F0}
{EC0B5E31-F42B-4B4E-B764-45FEA005C954}
Ad-Aware SE Personal
AddressBook
Adobe Acrobat 5.0
Branding
Connection Manager
CuteFTP
Desktop Calendar_is1
DirectAnimation
DirectDrawEx
Download Accelerator Plus Beta
DXM_Runtime
EditPlus 2
Fontcore
HP LaserJet 2200 Uninstaller
ICW
IE40
IE4Data
IE5BAKEX
IEData
ireasoning
Java Web Start
KB819696
KB823182
KB823353
KB823559
KB823980
KB824105
KB824141
KB824151
Expand
New
Find...
Delete
Rename
Export
Permissions...
Copy Key Name

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisplayName	REG_SZ	eG Agent
LogFile	REG_SZ	C:\Program Files\InstallShield Installation Information\{...
UninstallString	REG_SZ	RunDll32 C:\PROGRA~1\COMMON~1\INSTAL~1\engin...

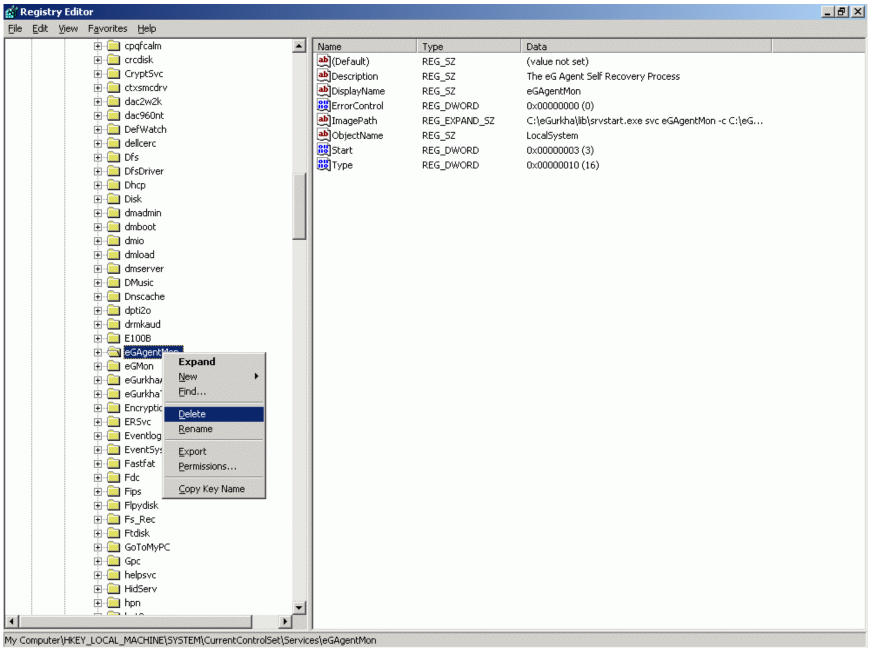
My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{EC0B5E31-F42B-4B4E-B764-45FEA005C954}

The registry key comprising of the 'eG Agent' entry

Figure 3.92: The registry key containing an 'eG Agent' entry

9. Next, delete the registry key by first selecting it from the tree-structure in the left pane of Figure 3.92, right-clicking on it, and choosing the **Delete** option from the shortcut menu that appears (see Figure 3.92). This will ensure that the **eG Agent** program no longer appears in the **Add/Remove Programs** list of the **Control Panel**.

10. Next, proceed to disable the **eGAgentMon** and **eGurkhaAgent** services. To do so, select the registry key corresponding to **My Computer\hkey_ local_ machine\system\CurrentControlSet\Services\eGAgentMon**, right-click on it, and choose the **Delete** option in the quick menu that appears (see Figure 3.93).

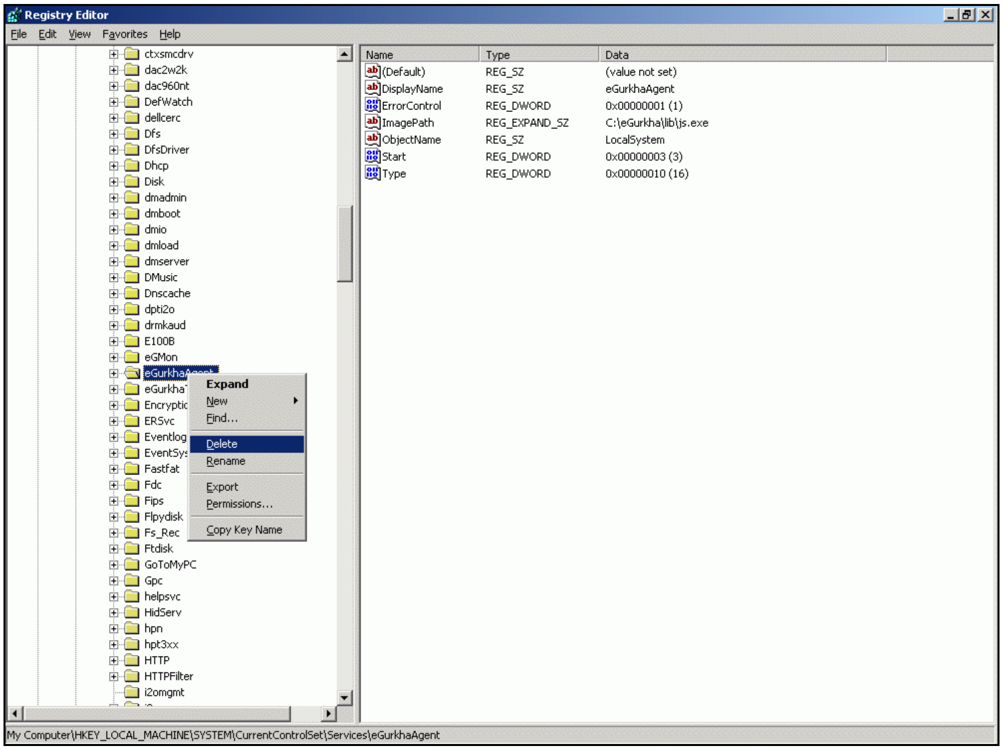


Name	Type	Data
(Default)	REG_SZ	(value not set)
Description	REG_SZ	The eG Agent Self Recovery Process
DisplayName	REG_SZ	eGAgentMon
ErrorControl	REG_DWORD	0x00000000 (0)
ImagePath	REG_EXPAND_SZ	C:\eGurkha\lib\srvstart.exe svc eGAgentMon -c C:\eG...
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000010 (16)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\eGAgentMon

Figure 3.93: Deleting the eGAgentMon key

11. Similarly, delete the **My Computer\hkey_ local_ machine\system\CurrentControlSet\Services\eGurkhaAgent** key (see Figure 3.94).



Name	Type	Data
(Default)	REG_SZ	(value not set)
DisplayName	REG_SZ	eGurkhaAgent
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	C:\eGurkha\lib\js.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000010 (16)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\eGurkhaAgent

Figure 3.94: Deleting the eGurkhaAgent key

12. Likewise, delete the **My Computer\hkey_ local_ machine\system\ControlSet001\Services\eGurkhaAgen**t and My **Computer\hkey_local_ machine\system\ControlSet002\Services\eGurkhaAgent** keys.

13. In the same manner, remove the **My Computer\hkey_ local_ machine\system\ControlSet001\Services\eGAgentMon** and the **My Computer\hkey_ local_machine\system\ControlSet002\Services\eGAgentMon** keys.

14. Deleting the registry keys corresponding to the agent services will only disable the services, and not completely remove them from the **Services** list. The **eGAgentMon** and **eGurkhaAgent** services will continue to appear in the **Services** list, but control operations (such as starting and stopping) can no longer be performed on them.

15. To remove the start menu items corresponding to the eG agent, right-click on the **eG Agent** option in the Start -> Programs -> eG Monitoring Suite menu sequence, and select the **Delete** option from the quick menu that appears (see Figure 3.95).

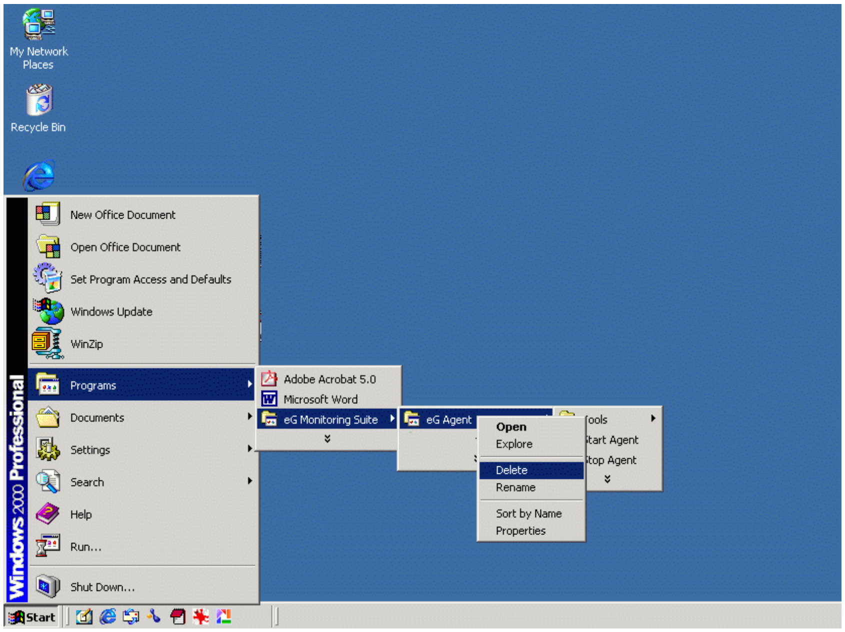


Figure 3.95: Deleting the eG Agent start menu options

16. Finally, remove the following directories from agent installation directory.

- <EG_AGENT_INSTALL_DIR>\agent
- <EG_AGENT_INSTALL_DIR>\JRE

Note:

If the manager is not installed on the same system as the agent, then the entire <EG_INSTALL_DIR> can be removed.

3.4 eG Agent on Unix

The procedure for installing and configuring an eG agent on Unix varies based on the following:

- The Unix operating system - whether Linux, Solaris, AIX, or HP-UX
- Whether the eG agent is installed for an Enterprise deployment of the eG manager or a SaaS deployment;

This section details the procedure involved in installing an eG agent on each Unix platform mentioned above and for the different deployment scenarios supported.

To know how to install the eG agent on Unix, refer to the following topics:

- Section **3.4.1**
- Section **3.4.2**
- Section **3.4.3**
- Section **3.4.4**

3.4.1 Installing an eG Agent on Solaris

There are two approaches to installing an eG agent on Solaris:

- The eG agent software for Solaris is available in the eG web site as a standard Solaris package called **eGagent** - one each for Solaris SPARC and AMD. You can **download** the eGagent package that corresponds to the type of processor (SPARC/AMD) used by the target Solaris host **from the eG web site**, and **manually run the eGagent** program on that host to install the eG agent. This approach is ideal if you want to deploy eG for a single organization - i.e., for the Enterprise deployment of eG.
- The eG agent software for Solaris is provided as a **packaged application** - one each for Solaris SPARC and AMD. You can **download** the **agent package** that corresponds to the target Solaris host **from the eG manager console**, extract the contents of the package to any folder in the target host, and **silently run the setup program in the extracted contents** to install and configure the agent on that host at one shot - i.e., to install the agent and also to configure agent-manager communication. If you are **deploying eG Enterprise for SaaS** , then it is **mandatory that your tenants use this approach** to install and configure the eG agents in their environment.

Both these approaches are discussed in this section.

3.4.1.1 Installing Solaris Agents for an Enterprise Deployment of the eG Manager

An Enterprise deployment of an eG manager is typically used to monitor only a single organization's IT infrastructure. In this case, it is recommended that the following procedure be used to install eG agents on Solaris hosts:

1. The eG agent software for Solaris is provided as a standard **Solaris** package called **eGagent**. You can download this package from the eG web site. The package for Solaris AMD, will be available in the **Solaris AMD** folder, and the same for Solaris SPARC, will be available in the **Solaris SPARC** folder. To know how to download, refer to the *eG Quick Installation Guide*.
2. After downloading the package to the Solaris host, login to that host, and type the following command at the command prompt.

```
pkgadd -d <path of the package eGagent>
```

Note:

Only a *super-user* can execute the above command.

3. The list of packages available are displayed next as shown below:

```
The following packages are available:  1  eGagent     eG Agent
(Sparc/AMD64) version 7
```

```
Select package(s) you wish to process (or ‘all’ to process
```

```
all packages). (default: all) [?,??,q]:
```

Choose the **all** option to install all the packages pertaining to the eG agent.

4. Next, decide the user account used for executing the eG agent. First enter the name of the eG user. The default value taken is “**egurkha**”.

```
Enter the name of the eG user [egurkha]:
```

Note:

If the agent is being installed on the same system as the manager, the eG user configured for the agent should be the same as that used for the manager.

5. Next, enter the path to the directory in which the eG agent will be installed. The default base directory for the eG agent is **/opt**. A subdirectory name **egurkha** will be created under the base directory. If the base directory is not **/opt**, a symbolic link will be created from the egurkha subdirectory of the base directory to **/opt/egurkha**.

```
Enter the directory where the eG Agent should be installed [/opt]:
```

6. Then, enter the group to which the eG user is to be associated with. The default value taken is “**egurkha**”. The installation will attempt to create the user account if it does not exist on the system. If you specify an existing user name, then this group prompt will not appear.

```
Enter the group to which the eG user is to be associated [egurkha]:
```

7. The install process will now request the user to confirm installation of the auto-restart feature. This feature will enable the agent to start automatically every time the system hosting the agent

reboots. Now, press **y** to install the auto-restart feature, or **n** to proceed without installing the same.

```
Would you like the eG Agent to auto-restart on system boot-up? y/n [n]
```

8. If the agent is installed on the same system as the manager some common files need not be reinstalled. When the installation process seeks the confirmation regarding installing the conflicting files, specify **n**.

```
The following files are already installed on the system and are being used by
another package. Do you want to install these conflicting files [y,n,?,q] n
```

9. A message indicating that installing the package requires super user permission appears and now the user needs to inform whether the process can proceed. If the user does not have the super user permissions, he/she needs to login as the super user before proceeding with the installation.

```
This package contains scripts which will be executed with super-user permission
during the process of installing this package.
```

```
Do you want to continue with the installation of <eGagent> [y,n,?] y
```

10. The following message will be displayed depicting the success of the agent installation.

```
********************************************************************
The eG Agent has been successfully installed!
Please login as <user name> and run the script
```

```
/opt/egurkha/bin/setup_agent
to configure the agent.
```

```
Installation of <eGagent> was successful.
```

If you install an eG agent using the procedure discussed above, then you will have to run a setup procedure later to configure agent-manager communication. To know how setup the eG agent, refer to the Section **3.4.7** topic.

3.4.1.2 Installing Solaris Agents for a SaaS Deployment of the eG Manager

As stated earlier, where eG Enterprise needs to support multiple tenants - eg., MSP environments with multiple customers, enterprises with multiple departments/domains - the individual tenants should use only this approach to deploy the eG agent on the Solaris hosts in their specific environments.

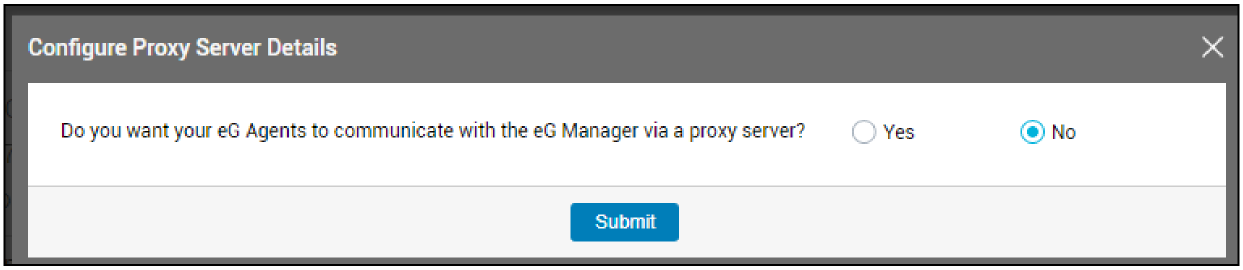
A key pre-requisite of this approach is that the eG manager should already be deployed and running.

To enable a tenant to install eG agents, the administrator should first make sure that the agent packages that correspond to the tenant's environment are accessible to the tenant from the eG manager console. For that, the administrator should do the following:

1. Login to the system hosting the eG manager.
2. From a browser, connect to the URL: https://www.eginnovations.com/eval712/AgentPackages
3. In this location, you will find a set of zip files. Each zip file is an agent package that corresponds to every operating system on which an eG agent can be installed.
4. Download the agent packages / zip files that correspond to the hosts in your tenant's environment, to any folder on the eG manager host. The Solaris- specific packages are as follows:
   - Solaris_AMD, for Solaris hosts supporting the AMD processor
   - Solaris_SPARC, for Solaris hosts supporting the SPARC processor
5. Copy the downloaded packages to the /opt/egurkha/agents/Universal/Latest folder on the eG manager.

The tenant can now proceed to install the eG agent using the procedure discussed hereunder:

1. Using a browser, connect to the URL of the eG management console.
2. Login to the eG management console using the credentials you used (corporate email ID and password) to register with eG Enterprise for SaaS.
3. Click the ⬇ icon in the top, right corner of the page that appears to download eG agents.
4. Doing so will invoke Figure 3.96, where you need to indicate if the eG agent you are downloading should communicate with the eG manager via a proxy server. If not, then pick the **No** option. If a proxy server is to be used for agent-manager communication, then select the **Yes** option.

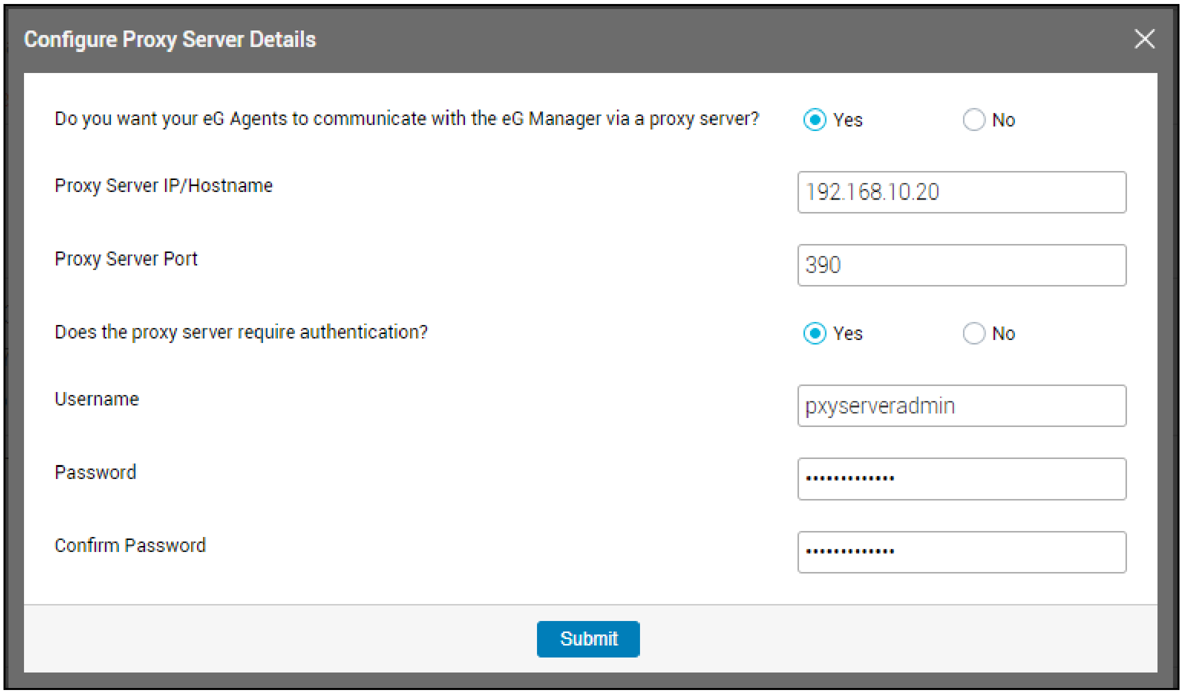


Configure Proxy Server Details

Do you want your eG Agents to communicate with the eG Manager via a proxy server? ○ Yes ● No

Figure 3.96: Indicating whether/not the eG agent being downloaded should communicate with the eG manager

5. If the **Yes** option is chosen in Figure 3.96, then Figure 3.97 will appear. Here, you need to provide the details of the proxy server used for agent-manager communication.



Configure Proxy Server Details

Do you want your eG Agents to communicate with the eG Manager via a proxy server? ● Yes ○ No

Proxy Server IP/Hostname: 192.168.10.20

Proxy Server Port: 390

Does the proxy server require authentication? ● Yes ○ No

Username: pxyserveradmin

Password: ••••••••••••••

Confirm Password: ••••••••••••••

Figure 3.97: Configuring agent-manager communication via a proxy server

6. Specify the following in Figure 3.97:

- **Proxy Server IP/Hostname**: Mention the IP address/hostname of the proxy server used for agent-manager communication.
- **Proxy Server Port**: Specify the port number at which the proxy server listens.
- **Does the proxy server require authentication?**: Indicate whether/not the proxy server requires authentication. Select the **No** option if authentication is required, and **Yes** if it is.
- **Username, Password, and Confirm Password**: If the proxy server requires authentication, then provide the credentials of a valid proxy server user against the **Username** and **Password** text boxes. Confirm the password by retyping it in the **Confirm Password** text box.
- Finally, click the **Submit** button to confirm the proxy server specifications and proceed with the downloading of the eG agent.

7. Figure 3.98 will appear. By default, Figure 3.98 lists the 'internal agent packages' that have been uploaded to the eG manager - i.e., agent packages to be used for monitoring components in an

agent-based manner. If you want to deploy a remote agent, click the **agentless monitoring** link in Figure 3.98. Likewise, to deploy an external agent, click the **external monitoring** link in the page.

Figure 3.98: eG's internal agent packages available for download from the eG manager console

Note:

Though the eG management console lists the packages meant for agent-less, agent-based, and external monitoring in separate pages, the procedure to download and install these packages remains the same across monitoring approaches.

8. To download an agent package for Solaris, click on the package that corresponds to the processor that the target host is using. For instance, to install an agent on a Solaris host running the AMD processor, download the Solaris_AMD.zip file by clicking on it.
9. If the host to which you have downloaded the package is the target Solaris host for agent installation, then login to that Solaris host as super-user. On the other hand, if you want to install the eG agent on a host different from the one on which the package has been downloaded, then first copy the agent package to any location on the target Solaris host. Then, login to that host as a super-user.
10. From the Shell prompt, open the folder to which the zip file has been copied/downloaded. Then, run the following command at the prompt to unzip the file and extract its contents.

    unzip <Zip_File_Name>

11. The following files will then be extracted:

    - **A tar file:** If you downloaded the agent package for a Solaris host running the AMD processor - i.e., if you downloaded Solaris_AMD.zip - then upon unzipping the file, you will find a file named eGagent_solaris_amd.tar.gz. If you downloaded the agent package for a Solaris host running the SPARC processor - i.e., if you downloaded Solaris_ SPARC.zip - then upon unzipping the file, you will find a file named eGagent_solaris_ sparc.tar.gz.
    - **iAgent_solaris script:** This is the script that installs the eG agent on a Solaris host.
    - **setup.sh:** This is the shell script that drives the silent installation of the eG agent. Running setup invokes the iAgent_solaris script and silently installs the agent on the target host.

- **eg_uaid:** In a multi-tenant setup, once a tenant - eg., a user representing a customer / a department / a domain - registers with eG Enterprise to use its monitoring services, eG automatically generates a unique UAID and assigns the same to that tenant. If that tenant later logs into the eG management console using the registered credentials (email ID and password) and downloads the agents, each agent so downloaded is automatically tagged with that UAID. The downloaded agents, once installed and configured, will automatically start discovering applications on their respective hosts. eG Enterprise auto-manages the discovered applications and auto-assigns them to the user who has the same UAID as the eG agent that discovered these applications. The eg_uaid file contains the UAID of the tenant who downloaded agent packages from the eG management console; this is the same UAID that will be assigned to each agent installed by that tenant.

12. Next, to install the eG agent on a Solaris host silently, from the Shell prompt, switch to the folder to which the files have been extracted. Then, run the **setup.sh** script by issuing the following command:

    ./setup.sh

13. Running setup will automatically install an eG agent on the target Solaris host, and will also automatically configure agent-manager communication. This eG agent will automatically report metrics to the eG manager from which the agent package was downloaded. Also, the hostname of such an agent is automatically set as its nick name.

    In a multi-tenant setup, a hostname may not be unique across tenant environments. To avoid nick name duplication, eG Enterprise automatically employs the following algorithm when assigning nick names:

    - At the time of setting the hostname of an agent host as its nick name, eG first checks if that hostname has already been assigned to any existing agent.
    - If it finds that the hostname has already been taken, then it will attempt to assign the FQDN - the fully qualified domain name - of the agent host as the nick name.
    - In the process, if eG finds that the FQDN is also in use, then it will break-down the FQDN into smaller strings, and try to assign each of these strings, one after another, to the agent.
    - If all these FQDN strings have already been assigned to other agents, then the eG agent will suffix the hostname of the agent host with the number 0, and try to assign this as the nick name of the eG agent. For instance, if the hostname of the eG agent host is solamd, then the nick name assigned to that agent will be solamd0.

- If this nick name is also taken, then eG will increment the number 0, which suffixes the hostname, by 1, and will try to assign the resultant string to the eG agent,. This way, eG will keep incrementing the number suffix until an unused string is found. Such a string will finally be assigned to the agent as its nick name.

  Note:

  - In a SaaS deployment, if a tenant manually adds components to be monitored by an eG agent, then you should only assign that agent's nick name to each of the components it monitors.

  - If you are downloading an agent for installation on an imaging system (e.g. for Citrix Provisioning services), or on a snapshot (for Citrix Machine Creation Services), or on a VM template for virtual servers, then, make sure you first enable the **Installation on a golden image / VM template** flag in Figure 3.98 and then proceed with the downloading. If this is done, then after the agent so downloaded is installed, setup will stop that agent. Also, setup will auto-delete the eg_nick.ini file of that agent, so that no nick name is assigned to that agent.

    On the other hand, if you download and install an agent on an imaging system / snapshot / VM template WITHOUT ENABLING the **Installation on a golden image / VM template** flag in Figure 3.98, then the installation will automatically start the agent and assign the hostname of the system as the nick name automatically. In such a case, you need to do the following:

    - On the snapshot / golden image / master VM, open the eg_nick.ini file in the <EG_AGENT_INSTALL_DIR>\agent\config directory.

    - Check to see if the **Nick** parameter in that file is set to any value. If this parameter has no value, it implies that no nick name was set for the eG agent on that snapshot / golden image / master VM. On the other hand, if the **Nick** parameter has a value, it indicates that a nick name was set for the eG agent. In this case, make sure that you delete the eg_nick.ini file on the snapshot / golden image / master VM before you proceed further.

    - Also, stop the eG agent.

3.4.2 Installing an eG Agent on Linux

There are two approaches to installing an eG agent on Linux:

- The eG agent software for Linux is available in the eG web site as a tar file and an iAgent script - a pair each for the 32-bit and 64-bit versions of Linux. You can **download** the tar file and iAgent script that corresponds to the bit version of the target Linux host **from the eG web site**, and **manually run the iAgent script** on that host to install the eG agent. This approach is ideal if you want to deploy eG for a single organization - i.e., for the Enterprise deployment of eG.

- The eG agent software for Linux is provided as a **packaged application** - one each for the 32-bit and 64-bit versions of Linux. You can **download** the **agent package** that corresponds to the target Linux host **from the eG manager console**, extract the contents of the package to any folder in the target host, and **silently run a setup script on that host** to install and configure the agent at one shot - i.e., to install the agent and also to configure agent-manager communication. If you are **deploying eG Enterprise for SaaS**, then it is **mandatory that your tenants use this approach** to install and configure the eG agents in their environment.

Both these approaches are discussed in this section.

3.4.2.1 Installing Linux Agents for an Enterprise Deployment of the eG Manager

An Enterprise deployment of the eG manager is typically used to monitor only a single organization's IT infrastructure. In this case, it is recommended that the following procedure be used to install eG agents on Linux hosts:

1. The standard eG agent software for 32-bit Linux hosts is provided as a tar file named **eGagent_linux.tar**. For installations on 64-bit Linux hosts, the **eGagent_linux_x64.tar** file is provided. An accompanying script drives the installation process for the eG agent. On 32-bit Linux hosts, this script is called **iAgent_linux**, and for 64-bit Linux hosts, this is called **iAgent_linux_x64**. You can download the tar file and installation script suitable to your environment from the eG web site. To know how, refer to the *eG Quick Installation Guide*.
2. After downloading, execute the **iAgent_linux** or the **iAgent_linux_x64** script (as the case may be), with the **eGagent_linux.tar** file or the **eGagent_linux_x64.tar** file (as the case may be) located in the same directory as the corresponding script file (i.e., **iAgent_linux** or **iAgent_linux_x64**).

   Note:

   The agent installation must be performed from a super-user account.
3. Next, specify the user account to be used for executing the eG agent. First enter the name of the eG user. The default value taken is “**egurkha**”.

```
This script will install the eG agent. The eG agent must be installed and executed by
a separate user. If you have installed the eG manager on the same system, you must use
the same user and the same installation directory for the manager and the agent.
```

```
Enter the name of the eG user [egurkha]:
```

Note:

- If the agent is being installed on the same system as the manager, the eG user configured for the agent should be the same as that used for the manager.
- You can specify the name of an existing user or a new user here. If you provide the name of a new user, then the eG agent installer will automatically create an eG user with that name. By default, the user account so created will only be a normal user account, and not a service account. Because a service account is more secure, administrators of high-security environments may prefer to use a service account for agent installation and operations, instead of a normal account. Such administrators can do the following:
    - Start the agent installation process by running the following command on a 32-bit Linux host:

      ```
      iAgent_linux -s
      ```

      On 64-bit Linux hosts, run the following command:

      ```
      iAgent_linux_x64 -s
      ```

    - When prompted for a user name, specify the name of the eG user account you want the installer to create. Once you provide a user name, the installer will automatically create a service account with that name.
    - Then, proceed with the installation as described by steps 3 to 8 below.

4. Then, enter the group with which the eG user is to be associated. The default value taken is "**egurkha**". The installation will attempt to create the user account if it does not exist on the system. If you specify an existing user name, then this group prompt will not appear.

```
Enter the group to which the eG user is to be associated [egurkha]:
```

5. Next enter the path to the directory in which the eG agent will reside. The default base directory for the eG agent is **/opt**. A subdirectory named egurkha will be created under the base directory. If the base directory is not **/opt**, a symbolic link will be created from the egurkha subdirectory of the base directory to **/opt/egurkha**.

```
Enter the directory in which the eG agent should be installed [/opt]:
```

6. The install process will now request the user to confirm installation of the auto-restart feature. This feature will enable the agent to start automatically every time the system hosting the agent reboots. Now, press **y** to install the auto-restart feature, or **n** to proceed without installing the same.

```
Would you like the eG agent to auto-restart on system boot-up? y/n [n] :
```

7. If the agent is installed on the same system as the manager some common files need not be reinstalled.

```
The following files are already installed on the system and are being used by another
package: Do you want to install these conflicting files [y,n,?,q] n
```

8. As in the case of the eG manager, the agent package contains components that need to be installed with the set-uid permissions set. These components must be installed for the agent to function properly. Following this step, the eG agent components are extracted and stored.
9. Finally, the following message will be displayed depicting the success of the installation.

```
The eG agent has been successfully installed! Please login as <eG user name> and run
the script /opt/egurkha/bin/setup_agent to configure the agent.
```

If you install an eG agent using the procedure discussed above, then you will have to run a setup procedure later to configure agent-manager communication. To know how setup the eG agent, refer to the Section **3.4.7** topic.

Note:

To install the eG agent on Tru64/FreeBSD/CentOS/openSUSE operating systems also, you will have to use the standard **Linux** package, and follow the installation procedure discussed above.

3.4.2.2 Installing Linux Agents for a SaaS Deployment of the eG Manager

As stated earlier, where eG Enterprise needs to support multiple tenants - eg., MSP environments with multiple customers, enterprises with multiple departments/domains - the individual tenants should use only this approach to deploy the eG agent on the Linux hosts in their specific environments.

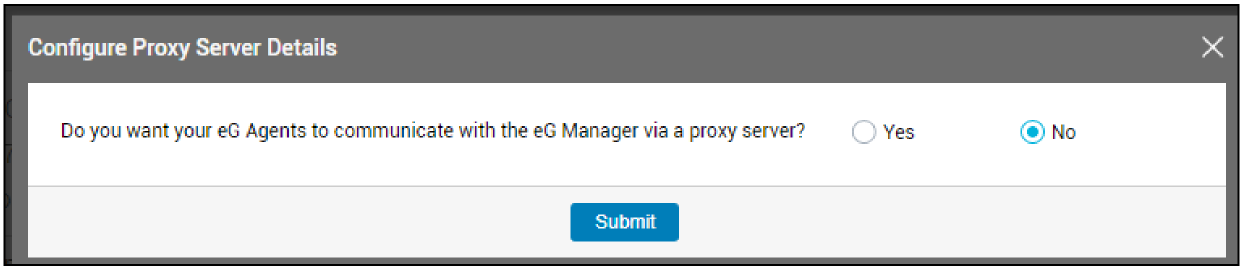
A key pre-requisite of this approach is that the eG manager should already be deployed and running.

To enable a tenant to install eG agents, the administrator should first make sure that the agent packages that correspond to the tenant's environment are accessible to the tenant from the eG manager console. For that, the administrator should do the following:

1. Login to the system hosting the eG manager.
2. From a browser, connect to the URL: https://www.eginnovations.com/eval712/AgentPackages
3. In this location, you will find a set of zip files. Each zip file is an agent package that corresponds to every operating system on which an eG agent can be installed.
4. Download the agent packages / zip files that correspond to the hosts in your tenant's environment, to any folder on the eG manager host. The Linux-specific packages are as follows:
   - Linux.zip, for 32-bit Linux systems
   - Linux_x64.zip, for 64-bit Linux systems
5. Copy the downloaded packages to the /opt/egurkha/agents/Universal/Latest folder on the eG manager.

The tenant can now proceed to install the eG agent using the procedure discussed hereunder:

1. Using a browser, connect to the URL of the eG management console.
2. Login to the eG management console using the credentials you used (corporate email ID and password) to register with eG Enterprise for SaaS.
3. Click the ⬇ icon in the top, right corner of the page that appears to download eG agents.
4. Doing so will invoke Figure 3.99, where you need to indicate if the eG agent you are downloading should communicate with the eG manager via a proxy server. If not, then pick the **No** option. If a proxy server is to be used for agent-manager communication, then select the **Yes** option.

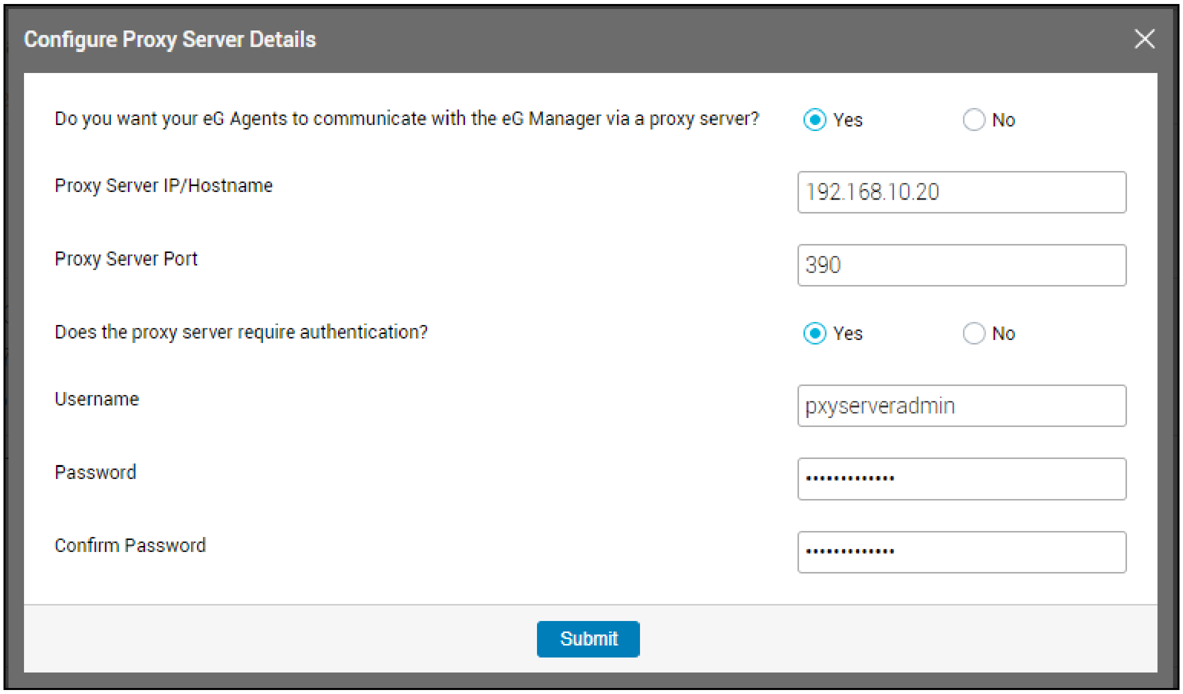


Configure Proxy Server Details

Do you want your eG Agents to communicate with the eG Manager via a proxy server? ○ Yes ● No

Figure 3.99: Indicating whether/not the eG agent being downloaded should communicate with the eG manager

5. If the **Yes** option is chosen in Figure 3.99, then Figure 3.100 will appear. Here, you need to provide the details of the proxy server used for agent-manager communication.



Configure Proxy Server Details

Do you want your eG Agents to communicate with the eG Manager via a proxy server?	● Yes ○ No
Proxy Server IP/Hostname	192.168.10.20
Proxy Server Port	390
Does the proxy server require authentication?	● Yes ○ No
Username	pxyserveradmin
Password	•••••••••••••
Confirm Password	•••••••••••••

Figure 3.100: Configuring agent-manager communication via a proxy server

6. Specify the following in Figure 3.100:

   - **Proxy Server IP/Hostname**: Mention the IP address/hostname of the proxy server used for agent-manager communication.
   - **Proxy Server Port**: Specify the port number at which the proxy server listens.
   - **Does the proxy server require authentication?**: Indicate whether/not the proxy server requires authentication. Select the **No** option if authentication is required, and **Yes** if it is.
   - **Username, Password, and Confirm Password**: If the proxy server requires authentication, then provide the credentials of a valid proxy server user against the **Username** and **Password** text boxes. Confirm the password by retyping it in the **Confirm Password** text box.
   - Finally, click the **Submit** button to confirm the proxy server specifications and proceed with the downloading of the eG agent.

7. Figure 3.101 will appear. By default, Figure 3.101 lists the 'internal agent packages' that have been uploaded to the eG manager - i.e., agent packages to be used for monitoring components in an agent-based manner. If you want to deploy a remote agent, click the **agentless monitoring** link in Figure 3.101. Likewise, to deploy an external agent, click the **external monitoring** link in the page.

Figure 3.101: eG's internal agent packages available for download from the eG manager console

Note:

Though the eG management console lists the packages meant for agent-less, agent-based, and external monitoring in separate pages, the procedure to download and install these packages remains the same across monitoring approaches.

8. To download an agent package for Linux, click on the package that corresponds to the bit version of Linux that the target host is using. For instance, to install an agent on a 32-bit Linux host, download the Linux.zip file by clicking on it.
9. If the host to which you have downloaded the package is the target Linux host for agent installation, then login to that Linux host as super-user. On the other hand, if you want to install the eG agent on a host different from the one on which the package has been downloaded, then first copy the agent package to any location on the target Linux host. Then, login to that host as a super-user.
10. From the Shell prompt, open the folder to which the zip file has been copied/downloaded. Then, run the following command at the prompt to unzip the file and extract its contents.

    unzip <Zip_File_Name>

11. The following files will then be extracted:

    - **A tar file:** If you downloaded the agent package for a 32-bit Linux host - i.e., if you downloaded Linux.zip - then upon unzipping the file, you will find a file named eGagent_ linux.tar.gz. If you downloaded the agent package for a 64-bit Linux host - i.e., if you downloaded Linux_x64.zip - then upon unzipping the file, you will find a file named eGagent_linux_x64.tar.gz.
    - **iAgent script:** This is the script that installs the eG agent on a Linux host. An iAgent_linux script will be extracted from Linux.zip (32-bit package), and an iAgent_linux_x64 script will be extracted from Linux_64.zip (64-bit package).
    - **setup.sh:** This is the shell script that drives the silent installation of the eG agent. Running setup invokes the iAgent script and silently installs the agent on the target host.
    - **eg_uaid:** In a multi-tenant setup, once a tenant - eg., a user representing a customer / a department / a domain - registers with eG Enterprise to use its monitoring services, eG automatically generates a unique UAID and assigns the same to that tenant. If that

tenant later logs into the eG management console using the registered credentials (email ID and password) and downloads the agents, each agent so downloaded is automatically tagged with that UAID. The downloaded agents, once installed and configured, will automatically start discovering applications on their respective hosts. eG Enterprise auto-manages the discovered applications and auto-assigns them to the user who has the same UAID as the eG agent that discovered these applications. The eg_uaid file contains the UAID of the tenant who downloaded agent packages from the eG management console; this is the same UAID that will be assigned to each agent installed by that tenant.

12. Next, to install the eG agent on a Linux host silently, from the Shell prompt, switch to the folder to which the files have been extracted. Then, run the **setup.sh** script by issuing the following command:

    ./setup.sh

13. Running setup will automatically install an eG agent on the target Linux host, and will also automatically configure manager-agent communication. This eG agent will automatically report metrics to the eG manager from which the agent package was downloaded. Also, the hostname of such an agent is automatically set as its nick name.

    In a multi-tenant setup, a hostname may not be unique across tenant environments. To avoid nick name duplication, eG Enterprise automatically employs the following algorithm when assigning nick names:

    - At the time of setting the hostname of an agent host as its nick name, eG first checks if that hostname has already been assigned to any existing agent.
    - If it finds that the hostname has already been taken, then it will attempt to assign the FQDN - the fully qualified domain name - of the agent host as the nick name.
    - In the process, if eG finds that the FQDN is also in use, then it will break-down the FQDN into smaller strings, and try to assign each of these strings, one after another, to the agent.
    - If all these FQDN strings have already been assigned to other agents, then the eG agent will suffix the hostname of the agent host with the number 0, and try to assign this as the nick name of the eG agent. For instance, if the hostname of the eG agent host is winpc, then the nick name assigned to that agent will be winpc0.
    - If this nick name is also taken, then eG will increment the number 0, which suffixes the hostname, by 1, and will try to assign the resultant string to the eG agent,. This way, eG will keep incrementing the number suffix until an unused string is found. Such a string will

finally be assigned to the agent as its nick name.

Note:

- In a SaaS deployment, if a tenant manually adds components to be monitored by an eG agent, then you should only assign that agent's nick name to each of the components it monitors.
- If you are downloading an agent for installation on an imaging system (e.g. for Citrix Provisioning services), or on a snapshot (for Citrix Machine Creation Services), or on a VM template for virtual servers, then, make sure you first enable the **Installation on a golden image / VM template** flag in Figure 3.101 and then proceed with the downloading. If this is done, then after the agent so downloaded is installed, setup will stop that agent. Also, setup will auto-delete the eg_nick.ini file of that agent, so that no nick name is assigned to that agent.

  On the other hand, if you download and install an agent on an imaging system / snapshot / VM template WITHOUT ENABLING the **Installation on a golden image / VM template** flag in Figure 3.101, then the installation will automatically start the agent and assign the hostname of the system as the nick name automatically. In such a case, you need to do the following:

  - On the snapshot / golden image / master VM, open the eg_nick.ini file in the <EG_AGENT_INSTALL_DIR>\agent\config directory.
  - Check to see if the **Nick** parameter in that file is set to any value. If this parameter has no value, it implies that no nick name was set for the eG agent on that snapshot / golden image / master VM. On the other hand, if the **Nick** parameter has a value, it indicates that a nick name was set for the eG agent. In this case, make sure that you delete the eg_nick.ini file on the snapshot / golden image / master VM before you proceed further.
  - Also, stop the eG agent.

Note:

If a tenant wants to install the eG agent on Tru64/FreeBSD/CentOS/openSUSE operating systems also, they will have to use the same installation procedure discussed above.

3.4.3 Installing an eG Agent on AIX

There are two approaches to installing an eG agent on AIX:

- The eG agent software for AIX is available in the eG web site as a tar file and an iAgent script. You can **download** the tar file and iAgent script **from the eG web site**, and **manually run the iAgent script** on the target Linux host to install the eG agent. This approach is ideal if you want to deploy AIX agents for a single organization - i.e., for the Enterprise deployment of eG.
- The eG agent software for AIX is provided as a **packaged application**. You can **download** the **agent package** for AIX **from the eG manager console**, extract the contents of the package to any folder in the target host, and **silently run a setup script on that host** to install and configure the agent at one shot - i.e., to install the agent and also to configure agent-manager communication. If you are **deploying eG Enterprise for SaaS**, then it is **mandatory that your tenants use this approach** to install and configure the eG agents in their environment.

Both these approaches are discussed in this section.

3.4.3.1 Installing AIX Agents for an Enterprise Deployment of the eG Manager

An Enterprise deployment of the eG manager is typically used to monitor only a single organization's IT infrastructure. In this case, it is recommended that the following procedure be used to install eG agents on AIX hosts:

1. The standard eG agent software for AIX is provided as a tar file named **eGagent_aix.tar**. An accompanying script, **iAgent_aix**, drives the installation process for the eG agent. You can download the tar file and installation script from the eG web site. To know how, refer to the *eG Quick Installation Guide*.
2. After downloading, execute the **iAgent_aix** script, with the **eGagent_aix.tar** file located in the same directory as the script file .

   Note:

   - The agent installation must be performed from a super-user account.
   - The name of the super-user should not exceed 8 characters. If it does, then the iAgent_aix script will prompt you to run the script using a different super-user account.
3. Next, specify the user account to be used for executing the eG agent. First enter the name of the eG user. The default value taken is “**egurkha**”.

```
This script will install the eG agent. The eG agent must be installed and executed by
a separate user. If you have installed the eG manager on the same system, you must use
the same user and the same installation directory for the manager and the agent.
```

```
Enter the name of the eG user [egurkha]:
```

Note:

If the agent is being installed on the same system as the manager, the eG user configured for the agent should be the same as that used for the manager.

4. Then, enter the group with which the eG user is to be associated. The default value taken is "**egurkha**". The installation will attempt to create the user account if it does not exist on the system. If you specify an existing user name, then this group prompt will not appear.

```
Enter the group to which the eG user is to be associated [egurkha]:
```

5. Next enter the path to the directory in which the eG agent will reside. The default base directory for the eG agent is **/opt**. A subdirectory named egurkha will be created under the base directory. If the base directory is not **/opt**, a symbolic link will be created from the egurkha subdirectory of the base directory to **/opt/egurkha**.

```
Enter the directory in which the eG agent should be installed [/opt]:
```

6. The install process will now request the user to confirm installation of the auto-restart feature. This feature will enable the agent to start automatically every time the system hosting the agent reboots. Now, press **y** to install the auto-restart feature, or **n** to proceed without installing the same.

```
Would you like the eG agent to auto-restart on system boot-up? y/n [n] :
```

7. If the agent is installed on the same system as the manager some common files need not be reinstalled.

```
The following files are already installed on the system and are being used by another
package: Do you want to install these conflicting files [y,n,?,q] n
```

8. As in the case of the eG manager, the agent package contains components that need to be installed with the set-uid permissions set. These components must be installed for the agent to function properly. Following this step, the eG agent components are extracted and stored.

9. Finally, the following message will be displayed depicting the success of the installation.

```
The eG agent has been successfully installed! Please login as <eG user name> and run
the script /opt/egurkha/bin/setup_agent to configure the agent.
```

If you install an eG agent using the procedure discussed above, then you will have to run a setup procedure later to configure agent-manager communication. To know how setup the eG agent, refer to the Section **3.4.7** topic.

3.4.3.2 Installing AIX Agents for a SaaS Deployment of the eG Manager

As stated earlier, where eG Enterprise needs to support multiple tenants - eg., MSP environments with multiple customers, enterprises with multiple departments/domains - the individual tenants should use only this approach to deploy the eG agent on the Linux hosts in their specific environments.

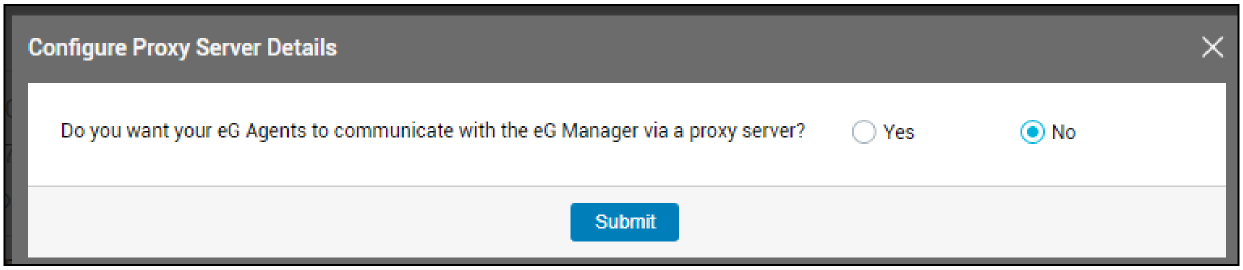
A key pre-requisite of this approach is that the eG manager should already be deployed and running.

To enable a tenant to install eG agents, the administrator should first make sure that the agent packages that correspond to the tenant's environment are accessible to the tenant from the eG manager console. For that, the administrator should do the following:

1. Login to the system hosting the eG manager.
2. From a browser, connect to the URL: https://www.eginnovations.com/eval712/AgentPackages
3. In this location, you will find a set of zip files. Each zip file is an agent package that corresponds to every operating system on which an eG agent can be installed.
4. Download the agent packages / zip files that correspond to the hosts in your tenant's environment, to any folder on the eG manager host. The AIX agent package will be listed therein as **AIX.zip**.
5. Copy the downloaded packages to the /opt/egurkha/agents/Universal/Latest folder on the eG manager.

The tenant can now proceed to install the eG agent using the procedure discussed hereunder:

1. Using a browser, connect to the URL of the eG management console.
2. Login to the eG management console using the credentials you used (corporate email ID and password) to register with eG Enterprise for SaaS.
3. Click the ⬇ icon in the top, right corner of the page that appears to download eG agents.
4. Doing so will invoke Figure 3.102 , where you need to indicate if the eG agent you are downloading should communicate with the eG manager via a proxy server. If not, then pick the **No** option. If a proxy server is to be used for agent-manager communication, then select the **Yes** option.

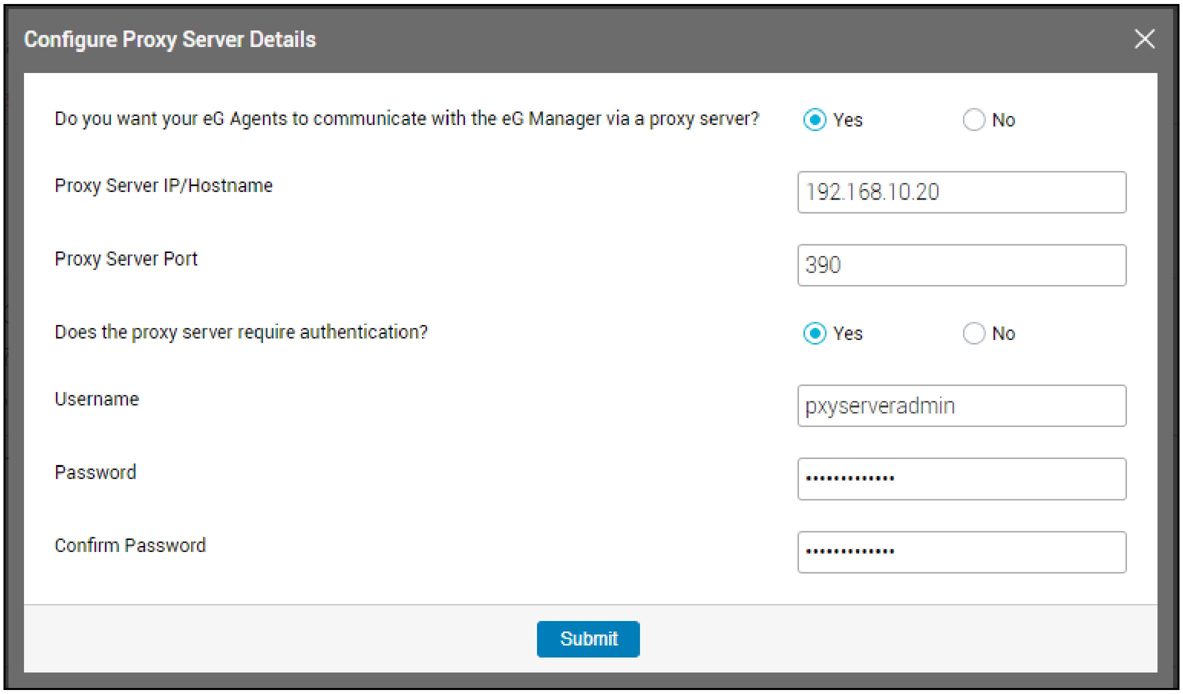


Configure Proxy Server Details

Do you want your eG Agents to communicate with the eG Manager via a proxy server? ○ Yes ● No

Figure 3.102: Indicating whether/not the eG agent being downloaded should communicate with the eG manager

5. If the **Yes** option is chosen in Figure 3.102, then Figure 3.103 will appear. Here, you need to provide the details of the proxy server used for agent-manager communication.



Configure Proxy Server Details

Do you want your eG Agents to communicate with the eG Manager via a proxy server? ● Yes ○ No

Proxy Server IP/Hostname: 192.168.10.20

Proxy Server Port: 390

Does the proxy server require authentication? ● Yes ○ No

Username: pxyserveradmin

Password: •••••••••••••

Confirm Password: •••••••••••••

Figure 3.103: Configuring agent-manager communication via a proxy server

6. Specify the following in Figure 3.103:

- **Proxy Server IP/Hostname**: Mention the IP address/hostname of the proxy server used for agent-manager communication.
- **Proxy Server Port**: Specify the port number at which the proxy server listens.
- **Does the proxy server require authentication?**: Indicate whether/not the proxy server requires authentication. Select the **No** option if authentication is required, and **Yes** if it is.

- **Username, Password, and Confirm Password**: If the proxy server requires authentication, then provide the credentials of a valid proxy server user against the **Username** and **Password** text boxes. Confirm the password by retyping it in the **Confirm Password** text box.
- Finally, click the **Submit** button to confirm the proxy server specifications and proceed with the downloading of the eG agent.

7. Figure 3.104 will appear. By default, Figure 3.104 lists the 'internal agent packages' that have been uploaded to the eG manager - i.e., agent packages to be used for monitoring components in an agent-based manner. If you want to deploy a remote agent, click the **agentless monitoring** link in Figure 3.104. Likewise, to deploy an external agent, click the **external monitoring** link in the page.

Figure 3.104: eG's internal agent packages available for download from the eG manager console

Note:

Though the eG management console lists the packages meant for agent-less, agent-based, and external monitoring in separate pages, the procedure to download and install these packages remains the same across monitoring approaches.

8. To download an agent package for AIX, click on the package named **AIX** in Figure 3.104.
9. If the host to which you have downloaded the package is the target AIX host for agent installation, then login to that AIX host as super-user. On the other hand, if you want to install the eG agent on a host different from the one on which the package has been downloaded, then first copy the agent package to any location on the target AIX host. Then, login to that host as a super-user.
10. From the Shell prompt, open the folder to which the zip file has been copied/downloaded. Then, run the following command at the prompt to unzip the file and extract its contents.

    unzip <Zip_File_Name>

11. The following files will then be extracted:

    - **A tar file:** Upon unzipping AIX.zip, you will find a tar file named eGagent_aix.tar.gz.
    - **iAgent script:** This is the script that installs the eG agent on an AIX host. An iAgent_aix script will be extracted from AIX.zip .
    - **setup.sh:** This is the shell script that drives the silent installation of the eG agent. Running setup invokes the iAgent_aix script and silently installs the agent on the target host.

- **eg_uaid:** In a multi-tenant setup, once a tenant - eg., a user representing a customer / a department / a domain - registers with eG Enterprise to use its monitoring services, eG automatically generates a unique UAID and assigns the same to that tenant. If that tenant later logs into the eG management console using the registered credentials (email ID and password) and downloads the agents, each agent so downloaded is automatically tagged with that UAID. The downloaded agents, once installed and configured, will automatically start discovering applications on their respective hosts. eG Enterprise auto-manages the discovered applications and auto-assigns them to the user who has the same UAID as the eG agent that discovered these applications. The eg_uaid file contains the UAID of the tenant who downloaded agent packages from the eG management console; this is the same UAID that will be assigned to each agent installed by that tenant.

12. Next, to install the eG agent on the AIX host silently, from the shell prompt, switch to the folder to which the files have been extracted. Then, run the **setup.sh** script by issuing the following command:

    ./setup.sh

13. Running setup will automatically install an eG agent on the target AIX host, and will also automatically configure agent-manager communication. This eG agent will automatically report metrics to the eG manager from which the agent package was downloaded. Also, the hostname of such an agent is automatically set as its nick name.

    In a multi-tenant setup, a hostname may not be unique across tenant environments. To avoid nick name duplication, eG Enterprise automatically employs the following algorithm when assigning nick names:

    - At the time of setting the hostname of an agent host as its nick name, eG first checks if that hostname has already been assigned to any existing agent.
    - If it finds that the hostname has already been taken, then it will attempt to assign the FQDN - the fully qualified domain name - of the agent host as the nick name.
    - In the process, if eG finds that the FQDN is also in use, then it will break-down the FQDN into smaller strings, and try to assign each of these strings, one after another, to the agent.
    - If all these FQDN strings have already been assigned to other agents, then the eG agent will suffix the hostname of the agent host with the number 0, and try to assign this as the nick name of the eG agent. For instance, if the hostname of the eG agent host is winpc, then the nick name assigned to that agent will be winpc0.

- If this nick name is also taken, then eG will increment the number 0, which suffixes the hostname, by 1, and will try to assign the resultant string to the eG agent,. This way, eG will keep incrementing the number suffix until an unused string is found. Such a string will finally be assigned to the agent as its nick name.

  Note:

  - In a SaaS deployment, if a tenant manually adds components to be monitored by an eG agent, then you should only assign that agent's nick name to each of the components it monitors.
  - If you are downloading an agent for installation on an imaging system (e.g. for Citrix Provisioning services), or on a snapshot (for Citrix Machine Creation Services), or on a VM template for virtual servers, then, make sure you first enable the **Installation on a golden image / VM template** flag in Figure 3.104 and then proceed with the downloading. If this is done, then after the agent so downloaded is installed, setup will stop that agent. Also, setup will auto-delete the eg_nick.ini file of that agent, so that no nick name is assigned to that agent.

    On the other hand, if you download and install an agent on an imaging system / snapshot / VM template WITHOUT ENABLING the **Installation on a golden image / VM template** flag in Figure 3.104, then the installation will automatically start the agent and assign the hostname of the system as the nick name automatically. In such a case, you need to do the following:

    - On the snapshot / golden image / master VM, open the eg_nick.ini file in the <EG_ AGENT_INSTALL_DIR>\agent\config directory.
    - Check to see if the **Nick** parameter in that file is set to any value. If this parameter has no value, it implies that no nick name was set for the eG agent on that snapshot / golden image / master VM. On the other hand, if the **Nick** parameter has a value, it indicates that a nick name was set for the eG agent. In this case, make sure that you delete the eg_nick.ini file on the snapshot / golden image / master VM before you proceed further.
    - Also, stop the eG agent.

3.4.4 Installing an eG Agent on HP-UX

There are two approaches to installing an eG agent on HP-UX:

- The eG agent software for HP-UX is available in the eG web site as a depot file and an iAgent script. you can **download** the depot file and iAgent script **from the eG web site**, and

manually run the iAgent script on the target to install the eG agent. This approach is ideal if you want to deploy HP-UX agents for a single organization - i.e., for the Enterprise deployment of eG.

- The eG agent software for HP-UX is provided as a **packaged application**. You can **download** the **agent package from the eG manager console**, extract the contents of the package to any folder in the target host, and **silently run a setup script on that host** to install and configure the agent at one shot - i.e., to install the agent and also to configure agent-manager communication. If you are **deploying eG Enterprise for SaaS**, then it is **mandatory that your tenants use this approach** to install and configure the eG agents in their environment.

Both these approaches are discussed in this section.

3.4.4.1 Installing HP-UX Agents for an Enterprise Deployment of the eG Manager

An Enterprise deployment of the eG manager is typically used to monitor only a single organization's IT infrastructure. In this case, it is recommended that the following procedure be used to install eG agents on HP-UX hosts:

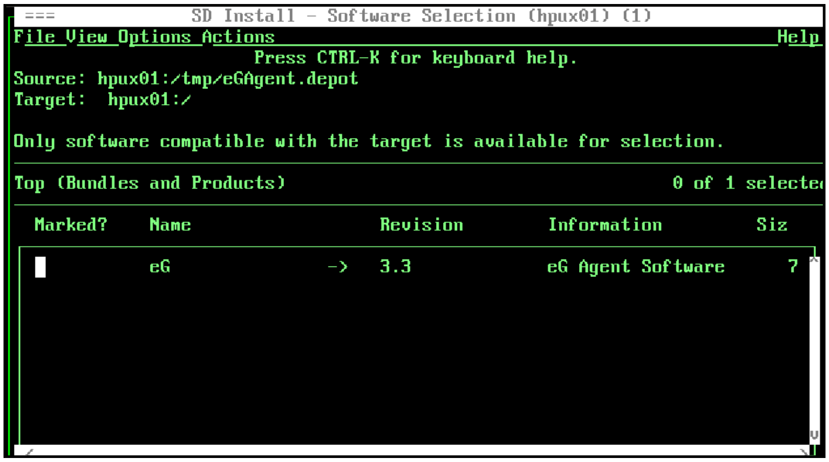
1. The standard eG agent software for HP-UX is provided as a depot file by name **eGAgent_hpux.depot.** An accompanying script called **iAgent_hpux** drives the installation process for the agent. You can download the tar file and installation script from the **HP-UX** folder in the eG web site. To know how, refer to the *eG Quick Installation Guide*.

2. After downloading, execute the **iAgent_hpux** script with the depot file located in the same directory as the script file .

3. Execute the **iAgent_hpux**script or iAgent script from the super-user account.

```
# ./iAgent
05/22/19 12:18:02 IST  BEGIN swreg SESSION (non-interactive)
•Session started for user "root@hpux01".
•Beginning Selection
•Targets:                hpux01
•Objects:                /var/spool/sw/eGAgent.depot
•Selection succeeded.

05/22/19 12:18:02 IST  END swreg SESSION (non-interactive)
NOTE:    The interactive UI was invoked, since no software was specified.
Starting the terminal version of swinstall...
Navigation in swinstall:
• use the "Tab" key to move between screen elements
• use the arrow  keys to move within screen elements
• use "Ctrl-F" for context-sensitive help anywhere in swinstall
On screens with a menubar at the top like this:
|File View Options Actions               Help|
       | -- -- ---- ---------------- --|
•use "Tab" to move from the list to the menubar
•use the arrow keys to move around
•use "Return" to pull down a menu or select a menu item
•use "Tab" to move from the menubar to the list without selecting a menu item
•use the spacebar to select an item in the list
On any screen, press "CTRL-K" for more information on how to use the keyboard.
Press "Return" to continue...
```

4. On pressing Enter, the screen depicted by Figure 3.105 appears:

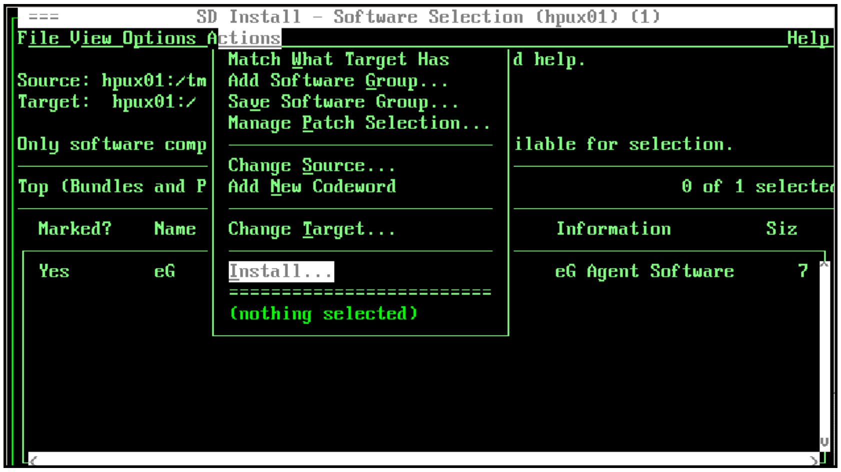


```
===             SD Install - Software Selection (hpux01) (1)
File View Options Actions                                    Help
                       Press CTRL-K for keyboard help.
Source: hpux01:/tmp/eGAgent.depot
Target:  hpux01:/

Only software compatible with the target is available for selection.

Top (Bundles and Products)                              0 of 1 selecte

  Marked?    Name              Revision        Information        Siz

  █          eG            ->  3.3             eG Agent Software    7
```

Figure 3.105: The swinstall terminal interface

5. Highlight the software using the spacebar and mark the software by pressing **m**. Then, using the

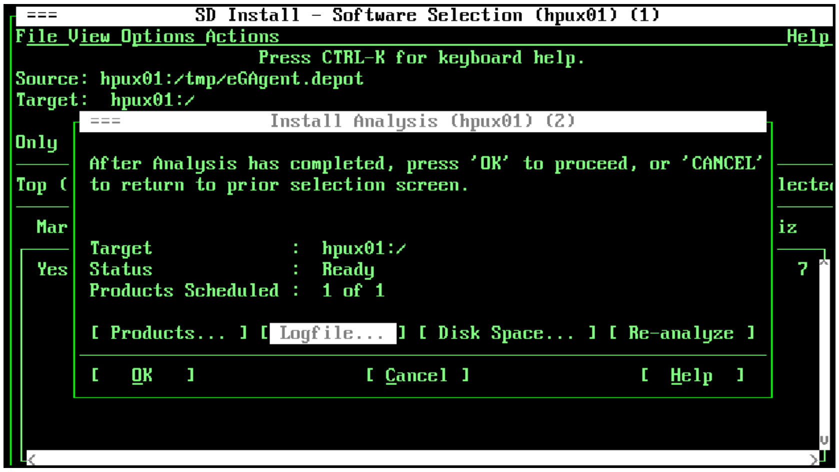
tab key, move to the menu bar on top and select **Install** from the **Actions** menu as depicted by Figure 3.106 below. This will begin the install analysis process.



```
 ===                SD Install - Software Selection (hpux01) (1)
File View Options Actions                                           Help
                   Match What Target Has       d help.
Source: hpux01:/tm Add Software Group...
Target:  hpux01:/  Save Software Group...
                   Manage Patch Selection...
Only software comp                             ilable for selection.
                   Change Source...
Top (Bundles and P Add New Codeword                        0 of 1 selecte

  Marked?    Name  Change Target...              Information          Siz

  Yes        eG    Install...                    eG Agent Software       7
                   =========================
                   (nothing selected)
```

Figure 3.106: Commencing the install analysis process

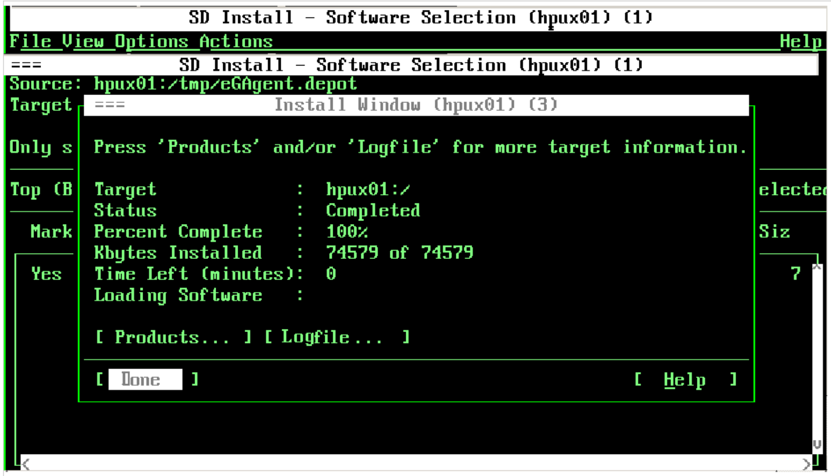
6. The screen that displays the status of the install analysis will then appear (see Figure 3.107):



```
 ===                SD Install - Software Selection (hpux01) (1)
File View Options Actions                                           Help
                         Press CTRL-K for keyboard help.
Source: hpux01:/tmp/eGAgent.depot
Target:  hpux01:/
       ===               Install Analysis (hpux01) (2)
Only
       After Analysis has completed, press 'OK' to proceed, or 'CANCEL'
Top (  to return to prior selection screen.                         lecte

 Mar                                                                iz
       Target            :  hpux01:/
 Yes   Status            :  Ready                                     7
       Products Scheduled :  1 of 1

       [ Products... ] [ Logfile... ] [ Disk Space... ] [ Re-analyze ]

       [    OK    ]              [ Cancel ]                [  Help  ]
```

Figure 3.107: A screen displaying the status of the install analysis process

7. Once the status changes to **Ready**, press Enter to bring up the screen depicted by Figure 3.108:



```
                    SD Install - Software Selection (hpux01) (1)
File View Options Actions                                          Help
===                SD Install - Software Selection (hpux01) (1)
Source: hpux01:/tmp/eGAgent.depot
Target  ===              Install Window (hpux01) (3)

Only s  Press 'Products' and/or 'Logfile' for more target information.

Top (B  Target               :  hpux01:/                          electe
        Status               :  Completed
  Mark  Percent Complete     :  100%                              Siz
        Kbytes Installed     :  74579 of 74579
  Yes   Time Left (minutes):   0                                     7
        Loading Software     :

        [ Products... ] [ Logfile... ]

        [ Done ]                                      [  Help  ]
```

Figure 3.108: Completing the install analysis process

8. Once the status becomes **Completed**, press **Done**.
9. Now, press **Tab** and choose File -> Exit to exit.
10. The install process will then prompt you to specify the name of the eG user.

```
Enter the name of the eG user [egurkha]: bob
```

11. Next, enter the path to the directory in which the eG agent is to be installed. The default base directory for an eG agent is **/opt**. A subdirectory named **egurkha** will be created under this base directory in the previous step.

```
Enter the directory in which the eG agent should be installed [/opt]:
```

12. Then, enter the name of the group with which the eG user is associated. If you specify an existing user name, then this group prompt will not appear.

```
Enter the group to which the eG user is to be associated [egurkha]:
```

13. Would you like the eG agent to auto-restart on system boot-up? y/n [n]

    The install process will now request the user to confirm installation of the auto-restart feature. This feature will enable the agent to start automatically every time the system hosting the agent reboots. Now, press **y** to install the auto-restart feature, or **n** to proceed without installing the same.

14. Upon successful installation of the agent, the following message appears:

```
The eG agent has been successfully installed!
Please login as <user name> and run the script
/opt/egurkha/bin/setup_agent to configure the agent.
```

If you install an eG agent using the procedure discussed above, then you will have to run a setup procedure later to configure agent-manager communication. To know how setup the eG agent, refer to the Section **3.4.7** topic.

3.4.4.2 Installing HP-UX Agents for a SaaS Deployment of the eG Manager

As stated earlier, where eG Enterprise needs to support multiple tenants - eg., MSP environments with multiple customers, enterprises with multiple departments/domains - the individual tenants should use only this approach to deploy the eG agent on the Linux hosts in their specific environments.

A key pre-requisite of this approach is that the eG manager should already be deployed and running.

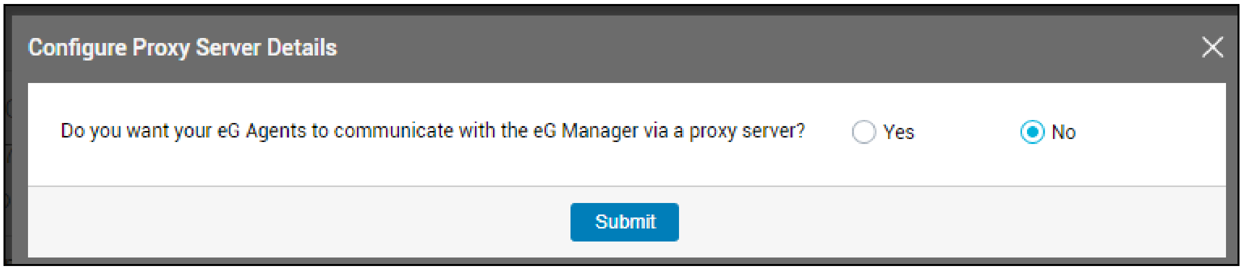
To enable a tenant to install eG agents, the administrator should first make sure that the agent packages that correspond to the tenant's environment are accessible to the tenant from the eG manager console. For that, the administrator should do the following:

1. Login to the system hosting the eG manager.
2. From a browser, connect to the URL: https://www.eginnovations.com/eval712/AgentPackages
3. In this location, you will find a set of zip files. Each zip file is an agent package that corresponds to every operating system on which an eG agent can be installed.
4. Download the agent packages / zip files that correspond to the hosts in your tenant's environment, to any folder on the eG manager host. The HP-UX agent package will be listed therein as **HPUX.zip**.
5. Copy the downloaded packages to the /opt/egurkha/agents/Universal/Latest folder on the eG manager.

The tenant can now proceed to install the eG agent using the procedure discussed hereunder:

1. Using a browser, connect to the URL of the eG management console.
2. Login to the eG management console using the credentials you used (corporate email ID and password) to register with eG Enterprise for SaaS.
3. Click the ⬇ icon in the top, right corner of the page that appears to download eG agents.
4. Doing so will invoke Figure 3.109, where you need to indicate if the eG agent you are downloading should communicate with the eG manager via a proxy server. If not, then pick the **No** option. If a proxy server is to be used for agent-manager communication, then select the **Yes**

option.

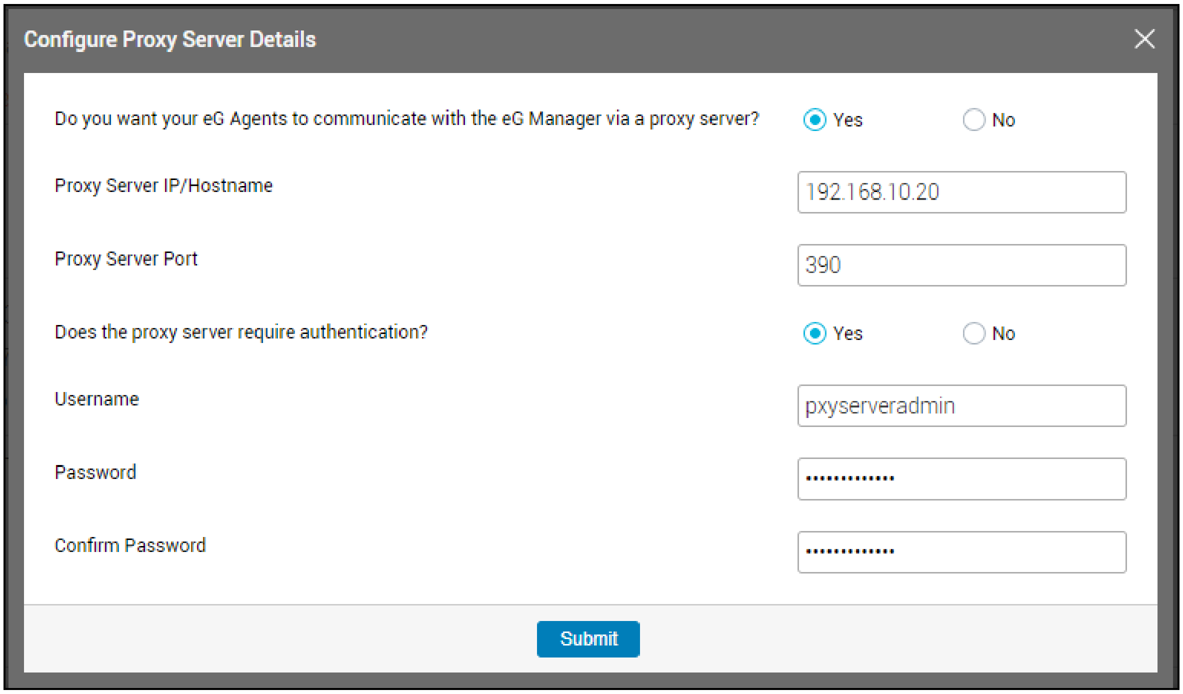


Configure Proxy Server Details

Do you want your eG Agents to communicate with the eG Manager via a proxy server? ○ Yes ● No

Figure 3.109: Indicating whether/not the eG agent being downloaded should communicate with the eG manager

5. If the **Yes** option is chosen in Figure 3.109, then Figure 3.110 will appear. Here, you need to provide the details of the proxy server used for agent-manager communication.



Configure Proxy Server Details

Do you want your eG Agents to communicate with the eG Manager via a proxy server? ● Yes ○ No

Proxy Server IP/Hostname: 192.168.10.20

Proxy Server Port: 390

Does the proxy server require authentication? ● Yes ○ No

Username: pxyserveradmin

Password: •••••••••••••

Confirm Password: •••••••••••••

Figure 3.110: Configuring agent-manager communication via a proxy server

6. Specify the following in Figure 3.110:

- **Proxy Server IP/Hostname**: Mention the IP address/hostname of the proxy server used for agent-manager communication.
- **Proxy Server Port**: Specify the port number at which the proxy server listens.

- **Does the proxy server require authentication?**: Indicate whether/not the proxy server requires authentication. Select the **No** option if authentication is required, and **Yes** if it is.
- **Username, Password, and Confirm Password**: If the proxy server requires authentication, then provide the credentials of a valid proxy server user against the **Username** and **Password** text boxes. Confirm the password by retyping it in the **Confirm Password** text box.
- Finally, click the **Submit** button to confirm the proxy server specifications and proceed with the downloading of the eG agent.

7. Figure 3.111 will appear. By default, Figure 3.111 lists the 'internal agent packages' that have been uploaded to the eG manager - i.e., agent packages to be used for monitoring components in an agent-based manner. If you want to deploy a remote agent, click the **agentless monitoring** link in Figure 3.111. Likewise, to deploy an external agent, click the **external monitoring** link in the page.

   Figure 3.111: eG's internal agent packages available for download from the eG manager console

   Note:

   Though the eG management console lists the packages meant for agent-less, agent-based, and external monitoring in separate pages, the procedure to download and install these packages remains the same across monitoring approaches.

8. To download an agent package for HP-UX, click on the package named **HP-UX**in Figure 3.111.
9. If the host to which you have downloaded the package is the target HP-UX host for agent installation, then login to that HP-UX host as super-user. On the other hand, if you want to install the eG agent on a host different from the one on which the package has been downloaded, then first copy the agent package to any location on the target HP-UX host. Then, login to that host as a super-user.
10. From the prompt, open the folder to which the zip file has been copied/downloaded. Then, run the following command at the prompt to unzip the file and extract its contents.

    unzip <Zip_File_Name>

11. The following files will then be extracted:

- **A tar file:** Upon unzipping HPUX.zip, you will find a tar file named eGagent_hpux.tar.gz.
- **iAgent script:** This is the script that installs the eG agent on an HP-UX host. An iAgent_ hpux script will be extracted from HPUX.zip .
- **setup.sh:** This is the shell script that drives the silent installation of the eG agent. Running setup invokes the iAgent_hpux script and silently installs the agent on the target host.
- **eg_uaid:** In a multi-tenant setup, once a tenant - eg., a user representing a customer / a department / a domain - registers with eG Enterprise to use its monitoring services, eG automatically generates a unique UAID and assigns the same to that tenant. If that tenant later logs into the eG management console using the registered credentials (email ID and password) and downloads the agents, each agent so downloaded is automatically tagged with that UAID. The downloaded agents, once installed and configured, will automatically start discovering applications on their respective hosts. eG Enterprise auto-manages the discovered applications and auto-assigns them to the user who has the same UAID as the eG agent that discovered these applications. The eg_uaid file contains the UAID of the tenant who downloaded agent packages from the eG management console; this is the same UAID that will be assigned to each agent installed by that tenant.

12. Next, to install the eG agent on the HP-UX host silently, from the command prompt, switch to the folder to which the files have been extracted. Then, run the **setup.sh** script by issuing the following command:

    ./setup.sh

13. Running setup will automatically install an eG agent on the target HP-UX host, and will also automatically configure agent-manager communication. This eG agent will automatically report metrics to the eG manager from which the agent package was downloaded. Also, the hostname of such an agent is automatically set as its nick name.

    In a multi-tenant setup, a hostname may not be unique across tenant environments. To avoid nick name duplication, eG Enterprise automatically employs the following algorithm when assigning nick names:

    - At the time of setting the hostname of an agent host as its nick name, eG first checks if that hostname has already been assigned to any existing agent.
    - If it finds that the hostname has already been taken, then it will attempt to assign the FQDN - the fully qualified domain name - of the agent host as the nick name.

- In the process, if eG finds that the FQDN is also in use, then it will break-down the FQDN into smaller strings, and try to assign each of these strings, one after another, to the agent.
- If all these FQDN strings have already been assigned to other agents, then the eG agent will suffix the hostname of the agent host with the number 0, and try to assign this as the nick name of the eG agent. For instance, if the hostname of the eG agent host is winpc, then the nick name assigned to that agent will be winpc0.
- If this nick name is also taken, then eG will increment the number 0, which suffixes the hostname, by 1, and will try to assign the resultant string to the eG agent,. This way, eG will keep incrementing the number suffix until an unused string is found. Such a string will finally be assigned to the agent as its nick name.

  Note:

  - In a SaaS deployment, if a tenant manually adds components to be monitored by an eG agent, then you should only assign that agent's nick name to each of the components it monitors.
  - If you are downloading an agent for installation on an imaging system (e.g. for Citrix Provisioning services), or on a snapshot (for Citrix Machine Creation Services), or on a VM template for virtual servers, then, make sure you first enable the **Installation on a golden image / VM template** flag in Figure 3.111 and then proceed with the downloading. If this is done, then after the agent so downloaded is installed, setup will stop that agent. Also, setup will auto-delete the eg_nick.ini file of that agent, so that no nick name is assigned to that agent.

    On the other hand, if you download and install an agent on an imaging system / snapshot / VM template WITHOUT ENABLING the **Installation on a golden image / VM template** flag in Figure 3.111, then the installation will automatically start the agent and assign the hostname of the system as the nick name automatically. In such a case, you need to do the following:

    - On the snapshot / golden image / master VM, open the eg_nick.ini file in the <EG_ AGENT_INSTALL_DIR>\agent\config directory.
    - Check to see if the **Nick** parameter in that file is set to any value. If this parameter has no value, it implies that no nick name was set for the eG agent on that snapshot / golden image / master VM. On the other hand, if the **Nick** parameter has a value, it indicates that a nick name was set for the eG agent. In this case, make sure that you

delete the eg_nick.ini file on the snapshot / golden image / master VM before you proceed further.

- Also, stop the eG agent.

3.4.5 Installing an eG Agent on an HP-UX Server Running an Itanium Processor

There are two approaches to installing an eG agent on HP-UX servers running an Itanium processor:

- The eG agent software for HP-UX Itanium is available in the eG web site as a tar file and an iAgent script. you can **download** the tar file and iAgent script **from the eG web site**, and **manually run the iAgent script** on the target to install the eG agent. This approach is ideal if you want to deploy HP-UX agents for a single organization - i.e., for the Enterprise deployment of eG.
- The eG agent software for HP-UX Itanium is provided as a **packaged application**. You can **download** the **agent package from the eG manager console**, extract the contents of the package to any folder in the target host, and **silently run a setup script on that host** to install and configure the agent at one shot - i.e., to install the agent and also to configure agent-manager communication. If you are **deploying eG Enterprise for SaaS**, then it is **mandatory that your tenants use this approach** to install and configure the eG agents in their environment.

Both these approaches are discussed in this section.

3.4.5.1 Installing HP-UX Itanium Agents for an Enterprise Deployment of the eG Manager

An Enterprise deployment of the eG manager is typically used to monitor only a single organization's IT infrastructure. In this case, it is recommended that the following procedure be used to install eG agents on HP-UX hosts running an Itanium processor:

1. The eG agent software for **Hpux_Itanium** is provided as a tar file named **eGagent.tar**. An accompanying script called **iAgent** drives the installation process for the agent. You can download the tar file and installation script from the **HP-UX Itanium** folder in the eG web site. To know how, refer to the *eG Quick Installation Guide*.
2. To start the installation process, execute the **iAgent** script, with the **eGagent.tar** file located in the same directory as **iAgent**.

Note:

The agent installation must be performed from a super-user account.

3. Next, specify the user account to be used for executing the eG agent. First enter the name of the eG user. The default value taken is “**egurkha**”.

```
This script will install the eG agent. The eG agent must be installed and executed by
a separate user. If you have installed the eG manager on the same system, you must use
the same user and the same installation directory for the manager and the agent.
Enter the name of the eG user [egurkha]:
```

Note:

If the agent is being installed on the same system as the manager, the eG user configured for the agent should be the same as that used for the manager.

4. Then, enter the group to which the eG user is to be associated with. The default value taken is “**egurkha**”. The installation will attempt to create the user account if it does not exist on the system. If you specify an existing user name, then this group prompt will not appear.

```
Enter the group to which the eG user is to be associated [egurkha]:
```

5. The install process will now request the user to confirm installation of the auto-restart feature. This feature will enable the agent to start automatically every time the system hosting the agent reboots. Now, press **y** to install the auto-restart feature, or **n** to proceed without installing the same.

```
Would you like the eG agent to auto-restart on system boot-up? y/n [n] :
```

6. If the agent is installed on the same system as the manager some common files need not be reinstalled.
7. As in the case of the eG manager, the agent package contains components that need to be installed with the set-uid permissions set. These components must be installed for the agent to function properly. Following this step, the eG agent components are extracted and stored.
8. The eG agent will be installed in the default **/opt** base directory. Upon successful installation, the following message will be displayed.

```
The eG agent has been successfully installed! Please login as <eG user name> and run
the script /opt/egurkha/bin/setup_agent to configure the agent.
```

If you install an eG agent using the procedure discussed above, then you will have to run a setup procedure later to configure agent-manager communication. To know how setup the eG agent, refer to the Section **3.4.7** topic.

3.4.5.2 Installing HP-UX Itanium Agents for a SaaS Deployment of the eG Manager

As stated earlier, where eG Enterprise needs to support multiple tenants - eg., MSP environments with multiple customers, enterprises with multiple departments/domains - the individual tenants should use only this approach to deploy the eG agent on the Linux hosts in their specific environments.

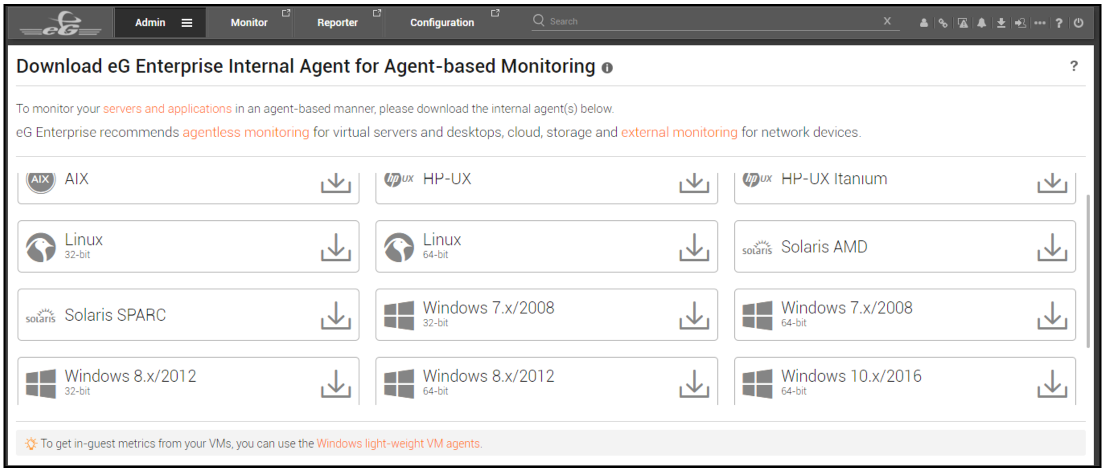
A key pre-requisite of this approach is that the eG manager should already be deployed and running.

To enable a tenant to install eG agents, the administrator should first make sure that the agent packages that correspond to the tenant's environment are accessible to the tenant from the eG manager console. For that, the administrator should do the following:

1. Login to the system hosting the eG manager.
2. From a browser, connect to the URL: https://www.eginnovations.com/eval712/AgentPackages
3. In this location, you will find a set of zip files. Each zip file is an agent package that corresponds to every operating system on which an eG agent can be installed.
4. Download the agent packages / zip files that correspond to the hosts in your tenant's environment, to any folder on the eG manager host. The HP-UX agent for Itanium package will be listed therein as **HPUX_Itanium.zip**.
5. Copy the downloaded packages to the /opt/egurkha/agents/Universal/Latest folder on the eG manager.

The tenant can now proceed to install the eG agent using the procedure discussed hereunder:

1. Using a browser, connect to the URL of the eG management console.
2. Login to the eG management console using the credentials you used (corporate email ID and password) to register with eG Enterprise for SaaS.
3. Click the ⬇ icon in the top, right corner of the page that appears to download eG agents.
4. Figure 3.112 will appear. By default, Figure 3.112 lists the 'internal agent packages' that have been uploaded to the eG manager - i.e., agent packages to be used for monitoring components in an agent-based manner. If you want to deploy a remote agent, click the **agentless monitoring** link in Figure 3.112. Likewise, to deploy an external agent, click the **external monitoring** link in the page.



Download eG Enterprise Internal Agent for Agent-based Monitoring

To monitor your servers and applications in an agent-based manner, please download the internal agent(s) below.

eG Enterprise recommends agentless monitoring for virtual servers and desktops, cloud, storage and external monitoring for network devices.

AIX
HP-UX
HP-UX Itanium
Linux 32-bit
Linux 64-bit
Solaris AMD
Solaris SPARC
Windows 7.x/2008 32-bit
Windows 7.x/2008 64-bit
Windows 8.x/2012 32-bit
Windows 8.x/2012 64-bit
Windows 10.x/2016 64-bit

To get in-guest metrics from your VMs, you can use the Windows light-weight VM agents.

Figure 3.112: eG's internal agent packages available for download from the eG manager console

Note:

Though the eG management console lists the packages meant for agent-less, agent-based, and external monitoring in separate pages, the procedure to download and install these packages remains the same across monitoring approaches.

5. To download an agent package for HP-UX Itanium, click on the package named **HP-UX Itanium**in Figure 3.112.
6. If the host to which you have downloaded the package is the target HP-UX host for agent installation, then login to that HP-UX host as super-user. On the other hand, if you want to install the eG agent on a host different from the one on which the package has been downloaded, then first copy the agent package to any location on the target HP-UX host. Then, login to that host as a super-user.
7. From the prompt, open the folder to which the zip file has been copied/downloaded. Then, run the following command at the prompt to unzip the file and extract its contents.

   unzip <Zip_File_Name>

8. The following files will then be extracted:

   - **A tar file:** Upon unzipping HPUX_ Itanium.zip, you will find a tar file named eGagent.tar.gz.
   - **iAgent script:** This is the script that installs the eG agent on an HP-UX host. An iAgent script will be extracted from HPUX_Itanium.zip .

- **setup.sh:** This is the shell script that drives the silent installation of the eG agent. Running setup invokes the iAgent script and silently installs the agent on the target host.
- **eg_uaid:** In a multi-tenant setup, once a tenant - eg., a user representing a customer / a department / a domain - registers with eG Enterprise to use its monitoring services, eG automatically generates a unique UAID and assigns the same to that tenant. If that tenant later logs into the eG management console using the registered credentials (email ID and password) and downloads the agents, each agent so downloaded is automatically tagged with that UAID. The downloaded agents, once installed and configured, will automatically start discovering applications on their respective hosts. eG Enterprise auto-manages the discovered applications and auto-assigns them to the user who has the same UAID as the eG agent that discovered these applications. The eg_uaid file contains the UAID of the tenant who downloaded agent packages from the eG management console; this is the same UAID that will be assigned to each agent installed by that tenant.

9. Next, to install the eG agent on the HP-UX host silently, from the command prompt, switch to the folder to which the files have been extracted. Then, run the **setup.sh** script by issuing the following command:

   ./setup.sh

10. Running setup will automatically install an eG agent on the target HP-UX host, and will also automatically configure agent-manager communication. This eG agent will automatically report metrics to the eG manager from which the agent package was downloaded. Also, the hostname of such an agent is automatically set as its nick name.

    In a multi-tenant setup, a hostname may not be unique across tenant environments. To avoid nick name duplication, eG Enterprise automatically employs the following algorithm when assigning nick names:

    - At the time of setting the hostname of an agent host as its nick name, eG first checks if that hostname has already been assigned to any existing agent.
    - If it finds that the hostname has already been taken, then it will attempt to assign the FQDN - the fully qualified domain name - of the agent host as the nick name.
    - In the process, if eG finds that the FQDN is also in use, then it will break-down the FQDN into smaller strings, and try to assign each of these strings, one after another, to the agent.
    - If all these FQDN strings have already been assigned to other agents, then the eG agent will suffix the hostname of the agent host with the number 0, and try to assign this as the

nick name of the eG agent. For instance, if the hostname of the eG agent host is winpc, then the nick name assigned to that agent will be winpc0.

- If this nick name is also taken, then eG will increment the number 0, which suffixes the hostname, by 1, and will try to assign the resultant string to the eG agent,. This way, eG will keep incrementing the number suffix until an unused string is found. Such a string will finally be assigned to the agent as its nick name.

  Note:

  - In a SaaS deployment, if a tenant manually adds components to be monitored by an eG agent, then you should only assign that agent's nick name to each of the components it monitors.
  - If you are installing the eG agent on an imaging system (e.g. for Citrix Provisioning services), or on a snapshot (for Citrix Machine Creation Services), or on a VM template for virtual servers, you will need to make sure that the nick name is NOT set for the agent on the imaging system/snapshot/VM template. In such environments, when installing the eG agent, make sure that you do not provide a nick name for that agent when prompted. If you are downloading the agent from the eG manager in a SaaS environment, the installation will automatically start the agent and assign the hostname of the system as the nick name automatically. In such a case, you need to:

    - On the snapshot / golden image / master VM, open the eg_nick.ini file in the <EG_AGENT_INSTALL_DIR>\agent\config directory.
    - Check to see if the **Nick** parameter in that file is set to any value. If this parameter has no value, it implies that no nick name was set for the eG agent on that snapshot / golden image / master VM. On the other hand, if the **Nick** parameter has a value, it indicates that a nick name was set for the eG agent. In this case, make sure that you delete the eg_nick.ini file on the snapshot / golden image / master VM before you proceed further.

3.4.6 Silent Mode Installation of the eG Agent on Unix

Silent mode installation is a standard way to ensure repeatability of the installation process. Administrators use this process when installing/uninstalling the same software in multiple locations/servers. For instance, in large environments comprising of hundreds of components, the eG agent software might have to be installed on each host to ensure that the applications on the hosts are monitored. By using the silent mode installation in such environments, you can ensure that agents are installed easily, in a secure, non-intrusive manner.

The following sectionstopics discuss how to install an agent on Unix hosts in the silent mode.

- Section **3.4.6.1**
- Section **3.4.6.2**
- Section **3.4.6.3**
- Section **3.4.6.4**
- Section **3.4.6.5**

3.4.6.1 Installing an eG Agent on Linux in the Silent Mode

To install an eG agent on Linux in the silent mode, do the following:

1. First, manually install the eG agent on any of the target Linux hosts in your environment, by following the procedure provided in the Section **3.4.2** topic . Typically, this is achieved by executing the **iAgent_linux.sh** script, with the **eGagent_linux.tar** file located in the same directory as the script.
2. Upon successful installation, a **silent_ install** script and an **iAgent_ linux** file will get automatically created in the **/opt/egurkha/bin** directory of the agent host.
3. Next, copy the **iAgent_linux** file and **silent_install** script from the **/opt/egurkha/bin** directory to any location on the Linux host on which you want to install an eG agent in the silent mode. To the same location, copy the **eGagent_linux.tar** file as well.
4. Next, login to the target host as the **root** user and edit the **silent_install** script, so that it contains the inputs required for your specific agent installation. An extract from the **silent_install** script is provided below:

```
eGuser=john
#eG user - please make sure that the user account exists

eGgroup=ainstallgrp

#eG user’s group

serviceaccount=no

#whether the user we are going to create is a service account or a normal account

eGInstallDir=/opt

#eG install directory

autoRestart=y

#whether the agent should auto-restart

licenseAcceptance=y

#licenseAcceptance the license

eGManager=192.168.10.54

#eG manager host

eGManagerPort=7077

#eG manager port

useProxy=n

#use Proxy?

proxyHost=n

#proxy server

proxyPort=n

#proxy port

setAuthentication=n
```

```
#use auhentication for proxy?

proxyUsername=none

#user name for proxy access - none

proxyPassword=none

#password for proxy access

useSSL=n

#use SSL for communication with the manager? y/n

trustedCertificates=n

#use trusted certificates for SSL communication with the manager? y/n

setNickName=n

#set the nickname for the agent - y/n

nickNameToUse=‘hostname‘

#the nick name to set for this agent
```

5. The parameters that you may need to edit include the following:

   a. **eGuser** : Here, either provide the name of an existing user to the target host or that of a new user. If you provide the name of the new user, then the agent installer will automatically create a normal (by default) user account with that name.

   b. **eGgroup** : Specify the group to which the eG user belongs.

   c. **serviceaccount** : If the name of a new user is specified against **eGuser**, then the agent installer will automatically create a user account with that name. By default, the user account so created will only be a normal user account, and not a service account. Because a service account is more secure, administrators of high-security environments may prefer to use a service account for agent installation and operations, instead of a normal account. To create a service account with the **eGuser**name specified, set this parameter to **yes**. To create only a normal user account, set this parameter to **no**.

   d. **eGInstallDir** : Specify the location on the target host in which the agent is to be installed.

e. **autoRestart** : Whether the agent is to be auto-restarted or not upon system reboot; enter **y** to restart the agent, or **n** to not restart.

f. **licenseAcceptance**: Whether to accept the terms and conditions of the eG license or not; enter **y** to accept the terms, or **n** to reject the same.

g. **eGManager**: Specify the IP address of the eG manager to which the agent should report.

h. **eGManagerPort** : Specify the port at which the eG manager listens.

i. **useProxy** : Indicate whether the agent communicates with the manager via a proxy server; if so, set this flag to **y**; if not, set this flag to **n**.

j. **proxyHost** : This parameter is applicable only if **useProxy** is set to **y**. In this case, specify the IP address of the proxy server against **proxyHost**. If **useProxy** is set to **n** instead, set this parameter to **n** as well.

k. **proxyPort** : This parameter too is applicable only if **useProxy** is set to **y**. In this case, specify the port number at which the proxy server listens against **proxyPort**. If **useProxy** is set to **n** instead, set this parameter to **n** as well.

l. **setAuthentication**: This flag is applicable only if **useProxy** is set to **y**. In this case, use this flag to indicate whether the proxy server requires authentication or not. Set this flag to **y** if authentication is required. If authentication is not required, set this flag to **n**. Similarly, if **useProxy** is set to **n**, set the **setAuthentication** flag also to **n.**

m. **proxyUsername** : This parameter is applicable only if **setAuthentication** is set to **y**. In this case, against **proxyUsername**, provide the user name for authenticating communication via the proxy server. If **setAuthentication** is set to **n**, then set **proxyUsername** to **none**.

n. **ProxyPassword**: This parameter is applicable only if **setAuthentication** is set to **y**. In this case, against **proxyPassword**, provide the password that corresponding to the specified **proxyUsername**. If **setAuthentication** is set to **n**, then set **proxyUsername** to **none**.

o. **useSSL**: Set this flag to **y**, if you want the eG agent to communicate with the manager via SSL. If not, set this flag to **n**.

p. **trustedCertificates**: This flag is applicable only if **useSSL** is set to **y**. To allow trusted certificates only, set this flag to **y**. To enable the agent to accept any certificate, set this flag to **n**. If **useSSL** is set to **n** instead, the **trustedCertificates** flag should be set to **n** as well.

q. **setNickName**: If you want to set a nick name for the agent, set this flag to **y**. If not, set this flag to **n**.

r. **nickNameToUse**: This flag is applicable only if **setNickName** is set to **y**. In such a case, specify the nick name to be assigned to the agent. By default, the host name of the agent host will be set as the nick name. You can change this nick name, if need be.

Note:

You cannot configure specific applications (such as ColdFusion/Sybase) for monitoring in the silent mode. For this purpose, you will have to follow the separate configuration instructions provided for these applications in the this document.

6. Once all the aforesaid parameters are configured with the values relevant to your agent installation, save the file.

   Note:

   Make sure that the **eGuser** account exists on the target system before you run the **silent_install** script.

7. Provide **execute** permissions for the **silent_install** script and run the script on the target host. To grant execute permissions, issue the following command from the directory that holds the **silent_install** script (say, **\tmp**): **chmod +x silent_install**
8. Upon successful execution of the script, the eG agent will be automatically installed and started on the host.

Note:

- Follow the same procedure discussed above to install the eG agent on Tru64, FreeBSD, CentOS, and openSUSE hosts, in the silent mode.
- If you are installing the eG agent on an imaging system (e.g. for Citrix Provisioning services), or on a snapshot (for Citrix Machine Creation Services), or on a VM template for virtual servers, you will need to make sure that the nick name is NOT set for the agent on the imaging system/snapshot/VM template. In such environments, when installing the eG agent, make sure that you do not provide a nick name for that agent when prompted. If you are downloading the agent from the eG manager in a SaaS environment, the installation will automatically start the agent and assign the hostname of the system as the nick name automatically. In such a case, you need to:
  - On the snapshot / golden image / master VM, open the eg_nick.ini file in the <EG_AGENT_ INSTALL_DIR>\agent\config directory.
  - Check to see if the **Nick** parameter in that file is set to any value. If this parameter has no value, it implies that no nick name was set for the eG agent on that snapshot / golden image / master

VM. On the other hand, if the **Nick** parameter has a value, it indicates that a nick name was set for the eG agent. In this case, make sure that you delete the eg_nick.ini file on the snapshot / golden image / master VM before you proceed further.

3.4.6.2 Installing an eG Agent on Solaris in the Silent Mode

To install an eG agent on Solaris in the silent mode, do the following:

1. First, manually install an eG agent on a target Solaris host using the installation instructions provided in the Section **3.4.1** topic. Typically, this is achieved by executing the **pkgadd -d** command on the target host from a super-user account.
2. After manual installation of the agent, you will find that a directory named **egurkha** is automatically created in the install location specified during installation. Now, tar the **egurkha** folder as **eGagent_solaris.tar** to a temporary folder (say, **/tmp**) on the agent host. For this purpose, issue the following command at the shell prompt: **tar -cvf /tmp/eGagent_solaris.tar egurkha**
3. Manual installation will also automatically create a **silent_install** script and an **iAgent_solaris** in the **/opt/egurkha/bin** directory of the agent host. Copy these two script files as well to the temporary folder (ay, **/tmp**).
4. Then, copy the **eGagent_solaris.tar**, **silent_install**, and **iAgent_solaris** files to any location (say, **/tmp**) on that Solaris host on which you want to install an eG agent in the silent mode.
5. Next, login as **root** user to the target Solaris host and edit the **silent_install** script so that it contains the inputs required for the agent installation on that host. For this, follow the procedure explained in step 4 of the Section **3.4.6.1** topic.
6. Once all the aforesaid parameters are configured with the values relevant to your agent installation, save the file.

   Note:

   Make sure that the **eGuser** account exists on the target system before you run the **silent_install** script.

7. Provide **execute** permissions for the **silent_install** script and run the script on the target host. To grant execute permissions, issue the following command from the directory that holds the **silent_install** script (say, **\tmp**): **chmod +x silent_install**
8. Upon successful execution of the script, the eG agent will be automatically installed and started on the host.

Troubleshooting Tips

If the silent install script on a target Solaris host fails with the exception 'su:No directory!', it indicates that the eG user on the target host does not have a valid home directory. While installing an eG agent on a Solaris host in the silent mode, make sure that the user specified as the eG user has a valid home directory on that host. If not, create a valid home directory for the eG user on that host, and then proceed with the silent agent installation.

Note:

If you are installing the eG agent on an imaging system (e.g. for Citrix Provisioning services), or on a snapshot (for Citrix Machine Creation Services), or on a VM template for virtual servers, you will need to make sure that the nick name is NOT set for the agent on the imaging system/snapshot/VM template. In such environments, when installing the eG agent, make sure that you do not provide a nick name for that agent. If you are downloading the agent from the eG manager in a SaaS environment, the installation will automatically start the agent and assign the hostname of the system as the nick name automatically. In such a case, you need to:

- On the snapshot / golden image / master VM, open the eg_nick.ini file in the <EG_AGENT_INSTALL_DIR>\agent\config directory.
- Check to see if the **Nick** parameter in that file is set to any value. If this parameter has no value, it implies that no nick name was set for the eG agent on that snapshot / golden image / master VM. On the other hand, if the **Nick** parameter has a value, it indicates that a nick name was set for the eG agent. In this case, make sure that you delete the eg_nick.ini file on the snapshot / golden image / master VM before you proceed further.

3.4.6.3 Installing an eG Agent on AIX in the Silent Mode

To install an eG agent on AIX in the silent mode, do the following:

1. First, manually install the eG agent on any of the target AIX hosts in your environment, by following the procedure provided in the Section **3.4.3** topic. Typically, this is achieved by executing the **iAgent_aix.sh** script, with the **eGagent_aix.tar** file located in the same directory as **iAgent_aix.sh**.
2. Upon successful installation, a **silent_install** script and an **iAgent_aix** file will get automatically created in the **/opt/egurkha/bin** directory of the agent host.
3. Next, copy the **iAgent_aix** file and **silent_install** script from the **/opt/egurkha/bin** directory to any location on the AIX host on which you want to install an eG agent in the silent mode. To the same location, copy the **eGagent_aix.tar** file as well.

4. Then, login to the AIX host as **root** user and edit the **silent_install** script. To achieve this, follow the procedure detailed at steps 4 of Section **3.4.6.1**.
5. Once all the aforesaid parameters are configured with the values relevant to your agent installation, save the file.

   Note:

   Make sure that the **eGuser** account exists on the target system before you run the **silent_install** script.

6. Provide **execute** permissions for the **silent_install** script and run the script on the target host. To grant execute permissions, issue the following command from the directory that holds the **silent_install** script (say, **\tmp**): **chmod +x silent_install**
7. Upon successful execution of the script, the eG agent will be automatically installed and started on the host.

Note:

If you are installing the eG agent on an imaging system (e.g. for Citrix Provisioning services), or on a snapshot (for Citrix Machine Creation Services), or on a VM template for virtual servers, you will need to make sure that the nick name is NOT set for the agent on the imaging system/snapshot/VM template. In such environments, when installing the eG agent, make sure that you do not provide a nick name for that agent. If you are downloading the agent from the eG manager in a SaaS environment, the installation will automatically start the agent and assign the hostname of the system as the nick name automatically. In such a case, you need to:

- On the snapshot / golden image / master VM, open the eg_nick.ini file in the <EG_AGENT_INSTALL_DIR>\agent\config directory.
- Check to see if the **Nick** parameter in that file is set to any value. If this parameter has no value, it implies that no nick name was set for the eG agent on that snapshot / golden image / master VM. On the other hand, if the **Nick** parameter has a value, it indicates that a nick name was set for the eG agent. In this case, make sure that you delete the eg_nick.ini file on the snapshot / golden image / master VM before you proceed further.

3.4.6.4 Installing an eG Agent on HPUX in the Silent Mode

To install an eG agent on HPUX in the silent mode, do the following:

1. First, manually install an eG agent on a target HPUX host using the installation instructions provided in Section **3.4.4**. Typically, this is achieved by executing the **iAgent_hpux** script from

the super-user account.

2. After manual installation of the agent, you will find that a directory named **egurkha** is automatically created in the install location specified during installation. Now, tar the **egurkha** folder as **eGagent_hpux.tar** to a temporary folder (say, **/tmp**) on the agent host. For this purpose, issue the following command at the shell prompt: **tar -cvf /tmp/eGagent_hpux.tar egurkha**
3. Manual installation will also automatically create a **silent_install** script and an **iAgent_hpux_ silent** in the **/opt/egurkha/bin** directory of the agent host. Copy these two script files as well to the temporary folder (ay, **/tmp**).
4. Then, copy the **eGagent_hpux.tar**, **silent_install**, and **iAgent_hpux_silent** files to any location (say, **/tmp**) on that HPUX host on which you want to install an eG agent in the silent mode.
5. Next, login as **root** user to the target HPUX host and edit the **silent_install** script so that it contains the inputs required for the agent installation on that host. For this, follow the procedure explained in step 4 of Section **3.4.6.1**.
6. Once all the aforesaid parameters are configured with the values relevant to your agent installation, save the file.

   Note:

   Make sure that the **eGuser** account exists on the target system before you run the **silent_install** script.

7. Provide **execute** permissions for the **silent_install** script and run the script on the target host. To grant execute permissions, issue the following command from the directory that holds the **silent_install** script (say, **\tmp**): **chmod +x silent_install**
8. Upon successful execution of the script, the eG agent will be automatically installed and started on the host.

Note:

If you are installing the eG agent on an imaging system (e.g. for Citrix Provisioning services), or on a snapshot (for Citrix Machine Creation Services), or on a VM template for virtual servers, you will need to make sure that the nick name is NOT set for the agent on the imaging system/snapshot/VM template. In such environments, when installing the eG agent, make sure that you do not provide a nick name for that agent. If you are downloading the agent from the eG manager in a SaaS environment, the installation will automatically start the agent and assign the hostname of the system as the nick name automatically. In such a case, you need to:

- On the snapshot / golden image / master VM, open the eg_nick.ini file in the <EG_AGENT_ INSTALL_DIR>\agent\config directory.
- Check to see if the **Nick** parameter in that file is set to any value. If this parameter has no value, it implies that no nick name was set for the eG agent on that snapshot / golden image / master VM. On the other hand, if the **Nick** parameter has a value, it indicates that a nick name was set for the eG agent. In this case, make sure that you delete the eg_nick.ini file on the snapshot / golden image / master VM before you proceed further.

3.4.6.5 Installing an eG Agent on HPUX Host with Itanium Processor in the Silent Mode

To install an eG agent on HPUX Itanium in the silent mode, do the following:

1. First, manually install an eG agent on a target HPUX host using the installation instructions provided in Section **3.4.5**. Typically, this is achieved by executing the **iAgent** script from the super-user account.
2. After manual installation of the agent, you will find that a directory named **egurkha** is automatically created in the install location specified during installation. Now, tar the **egurkha** folder as **eGagent_hpux_itanimum.tar** to a temporary folder (say, **/tmp**) on the agent host. For this purpose, issue the following command at the shell prompt:

   tar -cvf /tmp/eGagent_hpux_itanium.tar egurkha

3. Manual installation will also automatically create a **silent_install_itanium** script and an **iAgent_ hpux_itanium_silent** in the **/opt/egurkha/bin** directory of the agent host. Copy these two script files as well to the temporary folder (ay, **/tmp**).
4. Then, copy the **eGagent_hpux_itanium.tar**, **silent_install_itanium**, and **iAgent_hpux_ itanium_silent** files to any location (say, **/tmp**) on that HPUX host on which you want to install an eG agent in the silent mode.
5. Next, login as **root** user to the target HPUX host and edit the **silent_install_itanium** script so that it contains the inputs required for the agent installation on that host. For this, follow the procedure explained in step 4 of Section **3.4.6.1**.
6. Once all the aforesaid parameters are configured with the values relevant to your agent installation, save the file.

   Note:

Make sure that the **eGuser** account exists on the target system before you run the **silent_install_itanium** script.

7. Provide **execute** permissions for the **silent_install_itanium** script and run the script on the target host. To grant execute permissions, issue the following command from the directory that holds the **silent_install_itanium** script (say, **\tmp**): **chmod +x silent_install_itanium**
8. Upon successful execution of the script, the eG agent will be automatically installed and started on the host.

Note:

If you are installing the eG agent on an imaging system (e.g. for Citrix Provisioning services), or on a snapshot (for Citrix Machine Creation Services), or on a VM template for virtual servers, you will need to make sure that the nick name is NOT set for the agent on the imaging system/snapshot/VM template. In such environments, when installing the eG agent, make sure that you do not provide a nick name for that agent. If you are downloading the agent from the eG manager in a SaaS environment, the installation will automatically start the agent and assign the hostname of the system as the nick name automatically. In such a case, you need to:

- On the snapshot / golden image / master VM, open the eg_nick.ini file in the <EG_AGENT_INSTALL_DIR>\agent\config directory.
- Check to see if the **Nick** parameter in that file is set to any value. If this parameter has no value, it implies that no nick name was set for the eG agent on that snapshot / golden image / master VM. On the other hand, if the **Nick** parameter has a value, it indicates that a nick name was set for the eG agent. In this case, make sure that you delete the eg_nick.ini file on the snapshot / golden image / master VM before you proceed further.

3.4.7 Configuring the eG Agent on Unix

After installing the eG agent and before beginning agent configuration, make sure that the <EG_AGENT_INSTALL_DIR> is added to the Anti-virus exclusion list. If not, then sometimes, the CPU usage on the agent host may increase.

If you have installed the eG agent by downloading the tar file and installation script from the eG web site and then manually running the installation script on the target host, then, post successful installation, you will have to run setup separately on the agent host to configure manager-agent communication. To do this, it is essential to login as the eG user. The licensing terms for eG Enterprise are mentioned in the file **/opt/egurkha/license_agreement**. It is mandatory that you read this before proceeding any further.

The steps involved in configuring the eG agent are the same for all Unix systems, and are listed below:

1. For configuring, type the following command at the command prompt.

   /opt/egurkha/bin/setup_agent

2. The following message will be displayed and the process seeks the user's confirmation.

```
The licensing terms for eG products are mentioned in the file
/opt/egurkha/license_agreement. PLEASE READ THIS FILE BEFORE
PROCEEDING FURTHER.
Please indicate if you accept the eG licensing terms y/n [n]:
```

3. After the configuration process verifies that the licensing terms are acceptable to the user, it attempts to configure the agent's operational environment with the details of the eG manager that the agent should communicate with. For this purpose, the configuration process prompts the user for the hostname (or IP address) and the port number of the eG manager. The hostname should be used if DNS is enabled in the target environment. Otherwise, the IP address should be used.

```
Setup of manager/agent communication path
Enter the hostname (or IP address) of the eG Manager:
Enter the port number of the eG Manager [7077]:
```

4. The configuration process then requires to know if the user needs an HTTP proxy for the eG manager - agent communication. If yes, the user has to provide the name of the proxy server followed by the port number of the proxy server. If further authentication is required, the user name and the corresponding password have to be provided.

```
Please indicate if you want to use a proxy for the eG Agent to communicate with the eG
Manager? y/n [n] :
```

   Note:

   - If the eG agent is configured to communicate with the eG manager via a proxy server, then, whenever the eG agent attempts to remotely monitor an application by connecting to it via HTTP/HTTPS, it may automatically use the proxy server to establish this connection; this in tun may cause problems while monitoring those applications. To avoid this, before configuring the eG agent-manager communication via a proxy, make sure that the agent will be able to connect to remote applications also via the same proxy.

5. Then, indicate whether you want to enable SSL for the eG agent.

```
The eG Agent can use HTTP or HTTP/SSL to communicate with the eG Manager. In order to
use HTTP/SSL, please make sure that the eG Manager has been configured to support SSL.
Do you want to configure the eG Agent to use SSL for communication with the eG
Manager? y/n [n] :
```

Entering **y** here will enable SSL support for the agent, and **n** will disable it.

6. If SSL support is enabled, then setup will request your confirmation to allow trusted certificates alone.

```
Do you want to allow trusted certificates only? y/n [n]:
```

Note:
Ensure that the manager IP/hostname provided when setting up the agent matches the IP/hostname provided when generating the certificate on the manager.

Enter **y** if the agent is expected to communicate only with a manager that has a trusted SSL certificate. If you enter **n**, the agent accepts any certificate provided by the manager at the time when the SSL connection is established. If you have chosen to allow trusted certificates alone, then, you need to indicate the trust relationship to the agent. Towards this end, follow the instructions detailed in the **Section 3.4.8** topic once agent installation completes.

Note:

While configuring an eG agent on AIX, setup will not prompt you to confirm whether you want the eG agent to allow trusted certificates alone.

7. The setup will now request you to indicate whether you wish to assign nick name(s) for the eG agent's host. Instead of remembering the IP address/ host name of a host, users can assign one or more nick names to the host and manage all applications on the host using the same.

```
Please indicate if you want to assign a nick name(s) for this host? y/n [n] :
```

To assign nick names, press **y**. Setup will then request you to specify the nick name(s) to be assigned to the host.

```
Please enter the nick name(s) to be used for this host:
```

While providing multiple nick names, ensure that they are separated by a ':'. Also, ensure that a nick name does not contain any white spaces, and that all nick names are in lower case.

8. Upon successful termination of the agent setup process, the following message is displayed:

```
The eG Agent has been configured successfully.
```

```
Please use the commands /opt/egurkha/bin/start_agent and
/opt/egurkha/bin/stop_agent to start and stop the agent.
To provide feedback and report errors, please contact support@eginnovations.com
```

3.4.8 Enabling the eG Agent to Allow Trusted Certificates

If you have configured the eG agent (during agent setup) to allow trusted SSL certificates alone, you need to follow the broad steps below to ensure the same:

- Extract the certificate from the **keystore** file and export it to a **certificate** file.
- Import the SSL certificate into the JRE of the eG agent

The steps in this regard have been discussed elaborately below topics.

- Section **3.4.8.1**
- Section **3.4.8.2**

3.4.8.1 Extracting the SSL Certificate to a Certificate File

To achieve this, do the following

1. Login to the eG manager.
2. Set the **JAVA_HOME** environment variable to point to the Java installation directory.
3. Go to the command prompt.
4. Execute the following command:

   cd $JAVA_HOME/bin

   keytool -export -alias ***egitlab1*** *-keystore* ***<filename>.keystore*** *–storepass* ***mykey*** *-keypass* ***mykey*** *-file* ***C:\tmp\eGCert.cer***

   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-alias** : the alias name of the certificate being extracted; **make sure that you provide the same alias name that you provided while generating the keystore file** (see Section **2.8.0.2** or Section **2.8.0.6** section). If you are extracting the SSL certificate from the default keystore that is bundled with the eG manager, then first determine the alias name using which the keystore file was created. For this, from the <EG_INSTALL_DIR>\java\jdk\bin directory, run the following command:

keytool –list –v –keystore egmanager.bin

This command will prompt for the keystore passphrase. Type eginnovations and press ***Enter****. This will provide the details of the default keystore. From these details, you can infer the* ***Aliasname****.*

- **-keypass** : the password used to protect the key that was generated; **make sure that you provide the same password that you provided while generating the keystore file** (see Section **2.8.0.2** or Section **2.8.0.6** section). Also, note that **-storepass** and **-keypass** should be the same. If you are extracting the SSL certificate from the default keystore that is bundled with the eG manager, then the **–storepass** and **–keypass** should be *eginnovations*.
- **-keystore** : Provide the name of the *keystore* file in which the key has been stored; **specify the same file name that you used to store the key** (see Section **2.8.0.2** or Section **2.8.0.6**section).
- **-file** : Specify the full path to and the name of the certificate file (**.cer**) to which the certificate has to be exported

5. Once the **keytool** command successfully executes, the certificate file will be created.
6. Finally, copy the certificate file from the eG manager to any location on the eG agent host.

3.4.8.2 Importing the SSL Certificate into the JRE of the eG Agent

To achieve this, do the following:

1. Login to the eG agent host.
2. Open the Shell prompt and set the path:

   PATH =/opt/egurkha/jre/bin:$PATH

3. Then, using the **keytool** command, import the manager certificate to the JRE of the eG agent. A sample command has been given below:

   keytool - import - file C:\tmp\eGCert.cer - alias egcert - keystore <EG_ INSTALL_ DIR>\jre\lib\security\cacerts

   The parameters expected by this command are:

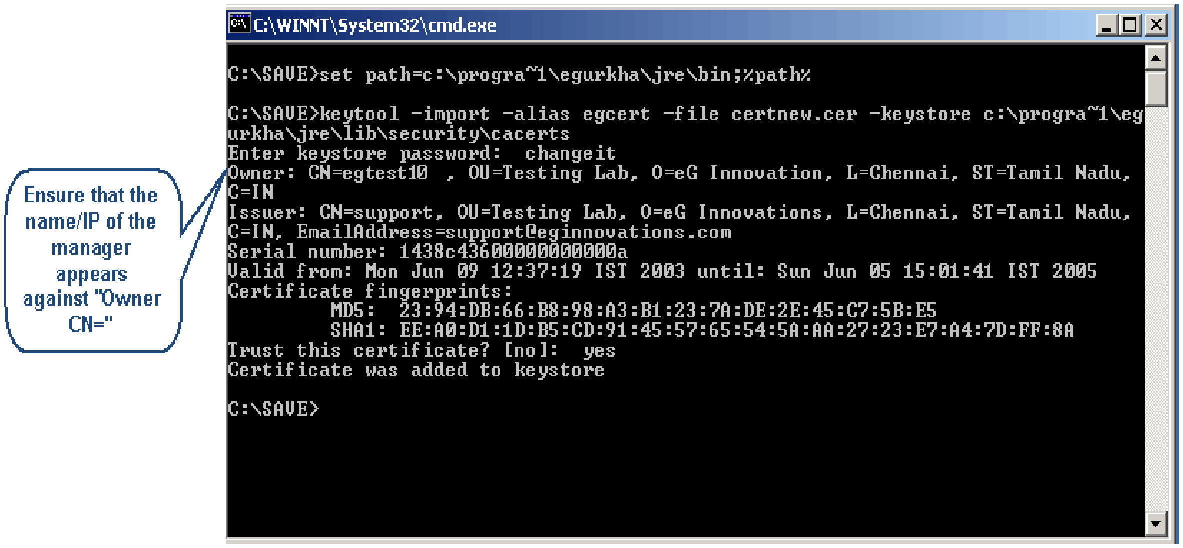
- **-alias** : an alias name for the certificate being imported; make sure that you provide the same alias name that you provided while generating the keystore file (see Section **2.8.0.2** or Section **2.8.0.6** section, depending upon whether the certificate is a self-signed certificate or a certificate obtained from a valid certificate authority). If you are extracting the SSL certificate from the default keystore that is bundled with the eG manager, then first determine the alias name using which the keystore file was created. For this, from the <EG_INSTALL_DIR>\java\jdk\bin directory, run the following command:

  keytool –list –v –keystore egmanager.bin

  This command will prompt for the keystore passphrase. Type *eginnovations* and press **Enter**. This will provide the details of the default keystore. From these details, you can infer the **Aliasname**.

- **-file** : the full path to the **.cer** file that was created in the Section **3.4.8.1** topic.
- **-keystore** : the keystore file that the JVM used by the agent checks for trusted certificates; specify the same file name that you used to store the key (see Section Section **2.8.0.2** or Section **2.8.0.6** of this document, depending upon whether the certificate is a self-signed certificate or a certificate obtained from a valid certificate authority). For the default certificate bundled with the eG manager, the **–keystore** should be *egmanager.bin*.This command, upon execution, will request for the keystore password. Provide the same keystore password you provided when generating the keystore file (see Section **2.8.0.2** section, as the case may be). For the default certificate bundled with the eG manager, the passwordshould be *eginnovations.*

4. Finally, the command will request your confirmation to make the imported certificate a trusted one. Enter **yes** to trust the certificate.
5. If the processing was successful, then a message stating that the *“Certificate was added to keystore”* will appear. Figure 3.113 depicts the processing explained above.



```
C:\SAVE>set path=c:\progra~1\egurkha\jre\bin;%path%

C:\SAVE>keytool -import -alias egcert -file certnew.cer -keystore c:\progra~1\eg
urkha\jre\lib\security\cacerts
Enter keystore password:  changeit
Owner: CN=egtest10  , OU=Testing Lab, O=eG Innovation, L=Chennai, ST=Tamil Nadu,
C=IN
Issuer: CN=support, OU=Testing Lab, O=eG Innovations, L=Chennai, ST=Tamil Nadu,
C=IN, EmailAddress=support@eginnovations.com
Serial number: 1438c4360000000000000a
Valid from: Mon Jun 09 12:37:19 IST 2003 until: Sun Jun 05 15:01:41 IST 2005
Certificate fingerprints:
         MD5:  23:94:DB:66:B8:98:A3:B1:23:7A:DE:2E:45:C7:5B:E5
         SHA1: EE:A0:D1:1D:B5:CD:91:45:57:65:54:5A:AA:27:23:E7:A4:7D:FF:8A
Trust this certificate? [no]:  yes
Certificate was added to keystore

C:\SAVE>
```

Ensure that the name/IP of the manager appears against "Owner CN="

Figure 3.113: The process of importing and trusting the manager certificate

6. Now, start the agent.

3.4.9 Starting the eG Agent

To start the agent, first, login as the eG user, and then, run the command **/opt/egurkha/bin/start_agent**. The following message would be displayed

```
Starting the eG agent. . .

The eG agent 5.1 has been started...

Please check the file: /opt/egurkha/agent/logs/error_log

for any errors while executing the agent.
```

The following error message would appear if the agent fails to start

```
The eG agent failed to start ...
```

This is probably because the eG manager's license does not permit this agent to communicate with it.

Please check the file: /opt/egurkha/agent/logs/error_log for details.

An eG agent may fail to start if:

- the eG manager cannot be contacted (or)
- there is a license mismatch

Note:

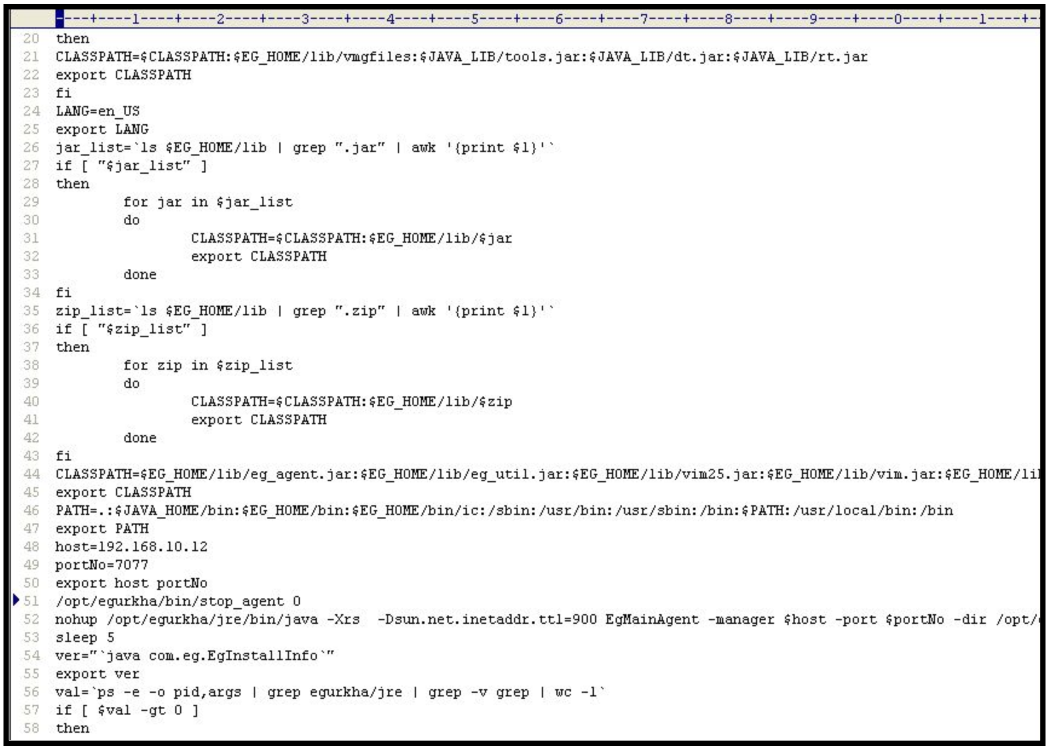
The following processes will run when the agent starts:

- A Java process that executes EgMainAgent - this is the core agent process
- A script named eGAgentMon that periodically monitors the agent and restarts it if the agent ever fails

Then, the eG administrative interface (described in the *Administering eG Enterprise* document) can be used to enable/disable authentication during manager/agent communication.

In Linux, AIX, and HPUX systems, error and output logging for the eG agent can be triggered by editing the **start_agent** script in the **/opt/egurkha/bin** directory. The steps involved in this process are discussed hereunder:

1. Open the **start_agent** file.
2. Edit the line that begins with **nohup /opt/egurkha/jre/bin/java–Xrs EgMainAgent . . .** (see Figure 3.114).

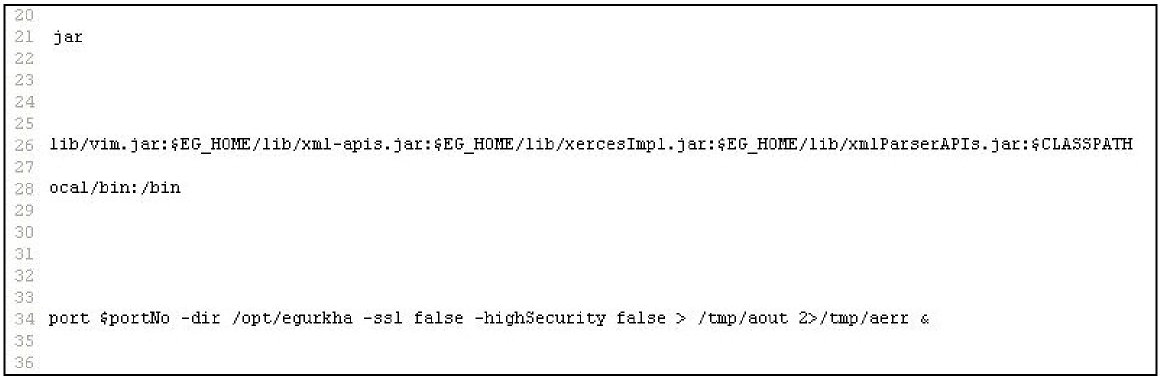


```
then
CLASSPATH=$CLASSPATH:$EG_HOME/lib/vmgfiles:$JAVA_LIB/tools.jar:$JAVA_LIB/dt.jar:$JAVA_LIB/rt.jar
export CLASSPATH
fi
LANG=en_US
export LANG
jar_list=`ls $EG_HOME/lib | grep ".jar" | awk '{print $1}'`
if [ "$jar_list" ]
then
        for jar in $jar_list
        do
                CLASSPATH=$CLASSPATH:$EG_HOME/lib/$jar
                export CLASSPATH
        done
fi
zip_list=`ls $EG_HOME/lib | grep ".zip" | awk '{print $1}'`
if [ "$zip_list" ]
then
        for zip in $zip_list
        do
                CLASSPATH=$CLASSPATH:$EG_HOME/lib/$zip
                export CLASSPATH
        done
fi
CLASSPATH=$EG_HOME/lib/eg_agent.jar:$EG_HOME/lib/eg_util.jar:$EG_HOME/lib/vim25.jar:$EG_HOME/lib/vim.jar:$EG_HOME/li
export CLASSPATH
PATH=.:$JAVA_HOME/bin:$EG_HOME/bin:$EG_HOME/bin/ic:/sbin:/usr/bin:/usr/sbin:/bin:$PATH:/usr/local/bin:/bin
export PATH
host=192.168.10.12
portNo=7077
export host portNo
/opt/egurkha/bin/stop_agent 0
nohup /opt/egurkha/jre/bin/java -Xrs  -Dsun.net.inetaddr.ttl=900 EgMainAgent -manager $host -port $portNo -dir /opt/
sleep 5
ver="`java com.eg.EgInstallInfo`"
export ver
val=`ps -e -o pid,args | grep egurkha/jre | grep -v grep | wc -l`
if [ $val -gt 0 ]
then
```

Figure 3.114: The start_agent script

3. At the end of the line indicated by Figure 3.114, you can find an entry that reads as follows: **. . . /dev/null 2>/dev/null**.

4. This entry is appended to the **nohup /opt/egurkha/jre/bin/java** line by default, and indicates that both output and error logging is not enabled for the eG agent in question, by default.
5. To enable output logging, replace the first occurrence of **/dev/null** in the line with the full path to an output log file (see Figure 3.115). Similarly, to enable error logging, replace the second occurrence of **/dev/null** with the full path to the error log file (see Figure 3.115).



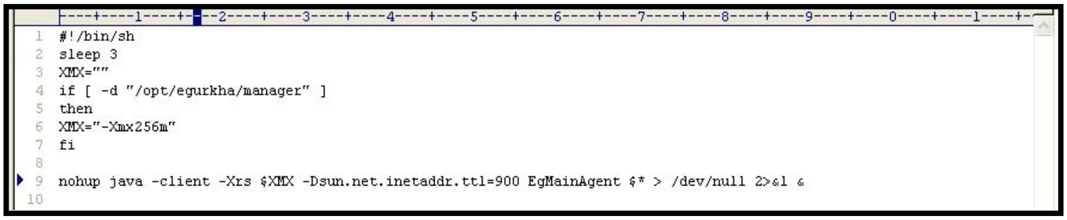
```

jar




lib/vim.jar:$EG_HOME/lib/xml-apis.jar:$EG_HOME/lib/xercesImpl.jar:$EG_HOME/lib/xmlParserAPIs.jar:$CLASSPATH

ocal/bin:/bin





port $portNo -dir /opt/egurkha -ssl false -highSecurity false > /tmp/aout 2>/tmp/aerr &


```

Figure 3.115: The edited start_agent script

6. Finally, save the **start_agent** script.
7. Restart the agent.

In Solaris environments, error and output logging for the eG agent can be triggered by editing the **starta** script in the **/opt/egurkha/bin** directory. The steps involved in this process are discussed hereunder:

1. Open the **starta** file.
2. Edit the line that begins with **nohup java –client -Xrs . . .** (see Figure 3.116).

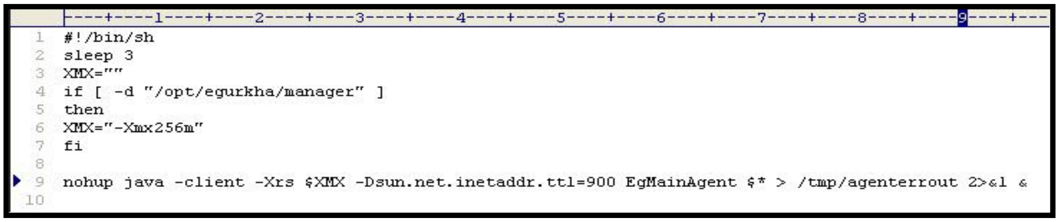


```
#!/bin/sh
sleep 3
XMX=""
if [ -d "/opt/egurkha/manager" ]
then
XMX="-Xmx256m"
fi

nohup java -client -Xrs $XMX -Dsun.net.inetaddr.ttl=900 EgMainAgent $* > /dev/null 2>&1 &

```

Figure 3.116: The starta script

3. At the end of the line indicated by Figure 3.116, you can find an entry that reads as follows: **. . . /dev/null 2>&1**.

4. This entry is appended to the **nohup java** line by default, and indicates that both output and error logging is not enabled for the eG agent in question, by default.
5. Unlike Linux, HPUX, and AIX agents, which can be configured with two separate log files for error and output logging respectively, the agent on Solaris can only be configured with a single log file; both errors and output will be captured by this log file only. Therefore, to enable error and output logging, replace the **/dev/null** entry in the **nohup** line with the full path to the log file (see Figure 3.117).



```
#!/bin/sh
sleep 3
XMX=""
if [ -d "/opt/egurkha/manager" ]
then
XMX="-Xmx256m"
fi

nohup java -client -Xrs $XMX -Dsun.net.inetaddr.ttl=900 EgMainAgent $* > /tmp/agenterrout 2>&1 &
```

Figure 3.117: The edited starta script

6. Finally, save the **starta** script.
7. Restart the agent.

Note:

Before attempting to administer the eG Enterprise system, ensure that *sysstat* package is installed on the component to be monitored (check for the existence of the *iostat* command on the target system). The DiskActivity Test will not function on Unix environments without the *sysstat* package.

3.4.10 Overheads of the eG Agent on Unix

The resource utilization of an eG agent is dependent on various factors including:

- the number of components that are being monitored by the eG agent;
- the specific component types to be monitored;
- the frequency of monitoring;
- whether the agent is monitoring applications in an agent-based or an agentless manner;

For an **internal** agent monitoring a single application on the server at a 5 minute frequency, the agent typically consumes 0.1-0.3% of CPU. Network traffic generated by the agent is about 0.05 – 0.2 kbps. The size of the agent on disk is about 1 GB. While a 32-bit eG agent will consume a heap memory of 64 MB on an average, the heap memory footprint of a 64-bit agent is 128 MB on an average. On an average, the eG agent will consume a heap memory of around 128 MB.

For an agent that monitors multiple applications on a server, or for an agent that monitors components in an agentless/external manner, the CPU, memory, and network bandwidth usage will be higher.

3.4.11 Increasing the Memory of the eG Agent

The eG agent runs as a Java process. The maximum heap memory that can be allocated to an eG agent on Unix is 256 MB. If an eG agent has been configured to monitor many components, then, you may have to allocate more heap memory to the eG agent. In such a case, follow the steps below for a Unix agent:

1. Login to the eG agent host.
2. Edit the **start_agent** script in the **/opt/egurkha/bin** directory.
3. Look for the entry *-Xmx* in the file. If you do not find it, then, insert an entry of the following format:

   Xmx<Memory_allocation_to_the _eG_agent>M

   For instance, if you want to allocate 2 GB (i.e., 2048 MB) of memory to the eG agent, your –Xmx specification should be as follows:

   Xmx2048M

   On the other hand, if you find the entry in the **start_agent** file, then simply alter the **<Memory_allocation_to_the _eG_agent>** to suit your specific needs.
4. Finally, save the file.

3.4.12 Uninstalling eG Enterprise

The process of uninstalling eG Enterprise varies depending on the operating system used. The steps to be executed to uninstall eG Enterprise are as follows:

1. First stop the execution of the manager using the command:

   /opt/egurkha/bin/stop_manager
2. Next, stop the execution of the agent using the command:

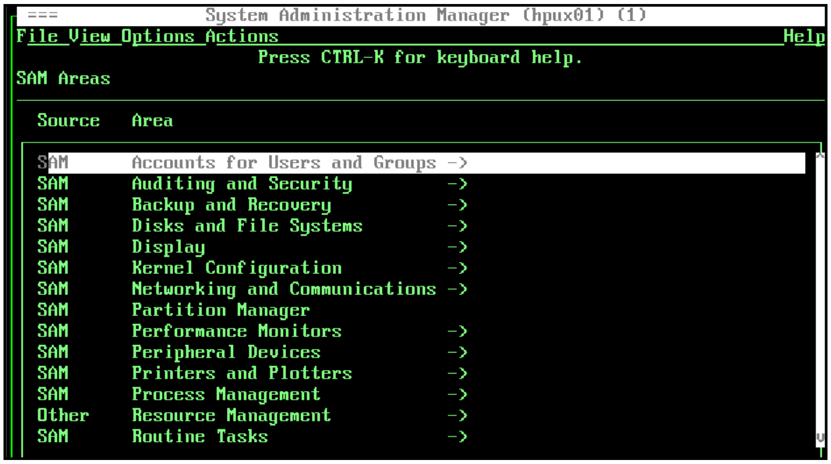
   /opt/egurkha/bin/stop_agent
3. Next, on Solaris, use the **pkgrm** command to uninstall the eGmanager and eGagent packages.

4. On Linux and AIX, the **/opt/egurkha** directory has to be manually removed to uninstall the eG Enterprise system.

5. On HP-UX, uninstall the eG agent following the steps given below:

- The eG agent can be uninstalled only by a super-user. Therefore, login as the super-user and run the command **sam**.

- Now, press the **Enter** key on the keyboard. A screen depicted by Figure 3.118 below appears next.

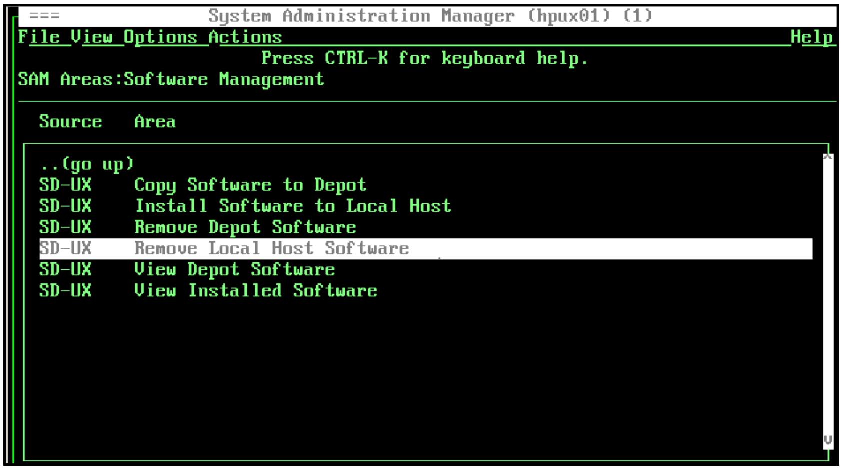


```
 ===              System Administration Manager (hpux01) (1)
File View Options Actions                                          Help
                       Press CTRL-K for keyboard help.
SAM Areas

  Source    Area

  SAM       Accounts for Users and Groups ->
  SAM       Auditing and Security         ->
  SAM       Backup and Recovery           ->
  SAM       Disks and File Systems        ->
  SAM       Display                       ->
  SAM       Kernel Configuration          ->
  SAM       Networking and Communications ->
  SAM       Partition Manager
  SAM       Performance Monitors          ->
  SAM       Peripheral Devices            ->
  SAM       Printers and Plotters         ->
  SAM       Process Management            ->
  Other     Resource Management           ->
  SAM       Routine Tasks                 ->
```

Figure 3.118: Selecting the Software Management option

- Using the down-arrow key on the key board, select the **SD-UX Software Management** option from Figure 3.118, and then press Enter.

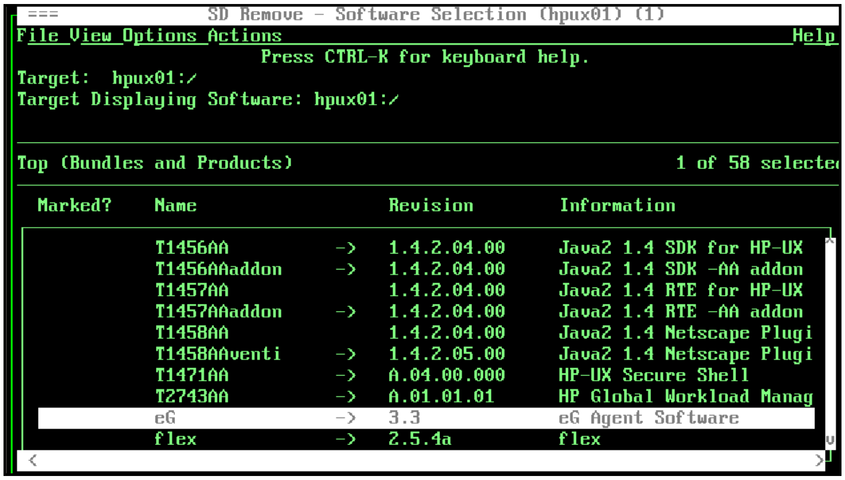
- Using the next screen (see Figure 3.119), choose to remove the eG agent software executing on the local host, by selecting the **Remove Local Host Software** option. To select this option, use the down-arrow key until the option is reached, and then press the **Enter** key.



```
 ===                System Administration Manager (hpux01) (1)
File View Options Actions                                        Help
                       Press CTRL-K for keyboard help.
SAM Areas:Software Management

  Source   Area

  ..(go up)
  SD-UX    Copy Software to Depot
  SD-UX    Install Software to Local Host
  SD-UX    Remove Depot Software
  SD-UX    Remove Local Host Software
  SD-UX    View Depot Software
  SD-UX    View Installed Software
```

Figure 3.119: Choosing to remove a software on the local host

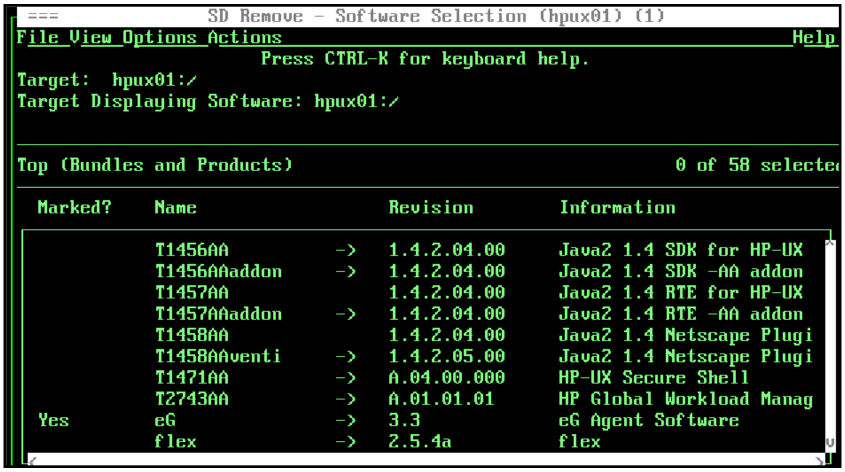
- From the screen that appears next, select the eG Agent software to be removed. To remove the selected eG agent software, first, mark it for removal by pressing the "**m**" key on the keyboard (see Figure 3.120).



```
 ===                SD Remove - Software Selection (hpux01) (1)
File View Options Actions                                        Help
                       Press CTRL-K for keyboard help.
Target:  hpux01:/
Target Displaying Software: hpux01:/

Top (Bundles and Products)                               1 of 58 selecte

  Marked?    Name                 Revision        Information

             T1456AA         ->   1.4.2.04.00     Java2 1.4 SDK for HP-UX
             T1456AAaddon    ->   1.4.2.04.00     Java2 1.4 SDK -AA addon
             T1457AA              1.4.2.04.00     Java2 1.4 RTE for HP-UX
             T1457AAaddon    ->   1.4.2.04.00     Java2 1.4 RTE -AA addon
             T1458AA              1.4.2.04.00     Java2 1.4 Netscape Plugi
             T1458AAventi    ->   1.4.2.05.00     Java2 1.4 Netscape Plugi
             T1471AA         ->   A.04.00.000     HP-UX Secure Shell
             T2743AA         ->   A.01.01.01      HP Global Workload Manag
             eG              ->   3.3             eG Agent Software
             flex            ->   2.5.4a          flex
```

Figure 3.120: Marking the eG agent software for deletion

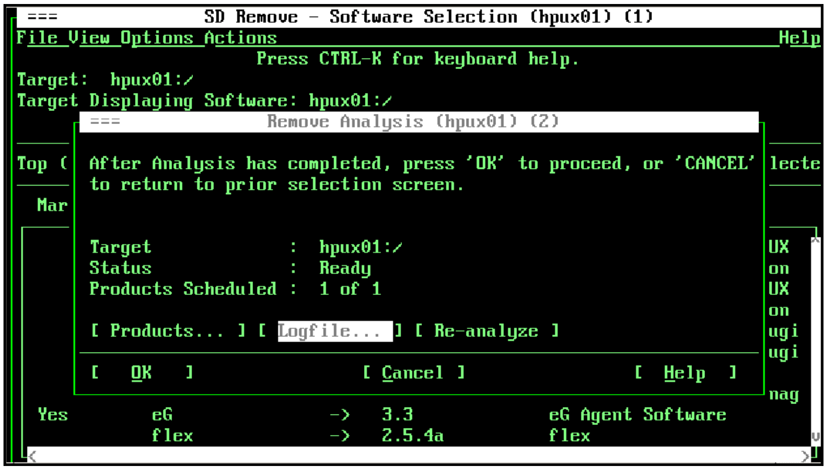
- Then, press the **Tab** key and choose *Actions* -> *Remove* as depicted by Figure 3.121 below.



```
===                 SD Remove - Software Selection (hpux01) (1)
File View Options Actions                                              Help
                       Press CTRL-K for keyboard help.
Target:  hpux01:/
Target Displaying Software: hpux01:/

Top (Bundles and Products)                                    0 of 58 selecte

  Marked?     Name                   Revision         Information

              T1456AA          ->    1.4.2.04.00      Java2 1.4 SDK for HP-UX
              T1456AAaddon     ->    1.4.2.04.00      Java2 1.4 SDK -AA addon
              T1457AA                1.4.2.04.00      Java2 1.4 RTE for HP-UX
              T1457AAaddon     ->    1.4.2.04.00      Java2 1.4 RTE -AA addon
              T1458AA                1.4.2.04.00      Java2 1.4 Netscape Plugi
              T1458AAventi     ->    1.4.2.05.00      Java2 1.4 Netscape Plugi
              T1471AA          ->    A.04.00.000      HP-UX Secure Shell
              T2743AA          ->    A.01.01.01       HP Global Workload Manag
  Yes         eG               ->    3.3              eG Agent Software
              flex             ->    2.5.4a           flex
```

Figure 3.121: Selecting the Remove option from the Actions menu

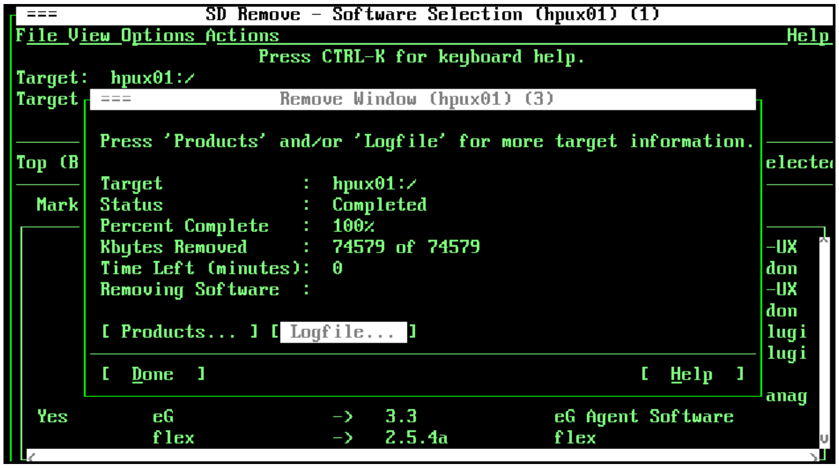
- Then, press the **Enter** key and wait until the **Status** of the remove analysis changes to **Ready** (see Figure 3.122). Then, using the **Tab** key, choose the **OK** button to confirm deletion of the selected eG software.



```
===                 SD Remove - Software Selection (hpux01) (1)
File View Options Actions                                             Help
                      Press CTRL-K for keyboard help.
Target:  hpux01:/
Target Displaying Software: hpux01:/
      ===                 Remove Analysis (hpux01) (2)

Top (  After Analysis has completed, press 'OK' to proceed, or 'CANCEL'  lecte
       to return to prior selection screen.
  Mar

       Target              :  hpux01:/                                  UX
       Status              :  Ready                                     on
       Products Scheduled  :  1 of 1                                    UX
                                                                        on
       [ Products... ] [ Logfile... ] [ Re-analyze ]                    ugi
                                                                        ugi
       [   OK   ]              [ Cancel ]              [  Help  ]
                                                                        nag
  Yes         eG               ->    3.3              eG Agent Software
              flex             ->    2.5.4a           flex
```

Figure 3.122: Confirming removal of the eG software by selecting the OK button

- Once the software is removed, status will become **Completed** (see Figure 3.123). Now, click the **Done** button, specified by an arrow in the figure.



```
 ===               SD Remove - Software Selection (hpux01) (1)
File View Options Actions                                              Help
                   Press CTRL-K for keyboard help.
Target:  hpux01:/
Target   ===                 Remove Window (hpux01) (3)

        Press 'Products' and/or 'Logfile' for more target information.
Top (B                                                                 electe
        Target             :  hpux01:/
  Mark  Status             :  Completed
        Percent Complete   :  100%
        Kbytes Removed     :  74579 of 74579                           -UX
        Time Left (minutes):  0                                        don
        Removing Software  :                                           -UX
                                                                       don
        [ Products... ] [ Logfile... ]                                 lugi
                                                                       lugi
        [  Done  ]                                       [  Help  ]
                                                                       anag
  Yes        eG                 ->   3.3          eG Agent Software
             flex               ->   2.5.4a       flex
```

Figure 3.123: Status changing to Completed

- Finally, exit the uninstall process using the menu sequence: *File -> Exit SAM*.

Note:

If an agent monitoring a web server is uninstalled, then the web adapter should be manually removed. To do so, open the **httpd.conf** file (in the <WEB_SERVER_HOME_DIR>/conf directory) of the web server, and comment the LoadModule egurkha_module entry and the AddModule mod_ egurkha entry.

3.5 Installing an eG Agent on the Manager System in a SaaS Deployment

By default, the eG agent on a manager system will operate as an external/remote agent for the target environment. In a SaaS deployment of eG Enterprise, follow the procedure discussed below to install an eG agent on a manager system:

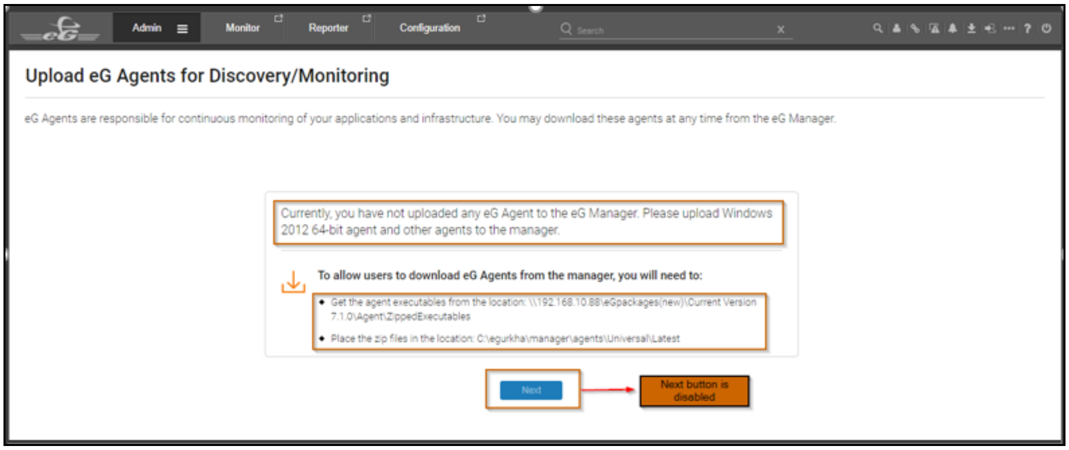
1. Soon after you install and configure the eG manager, login to the eG management console as the default user *admin* with password *admin*.

2. Figure 3.124 will then appear displaying a message stating that no agents have been uploaded to the manager yet. Follow the steps below to upload eG agent installables to the manager:

   - Login to the system hosting the eG manager.

   - From a browser, connect to the URL: https://www.eginnovations.com/eval712/AgentPackages

- In this location, you will find a set of zip files. Each zip file is an agent package that corresponds to every operating system on which an eG agent can be installed.
- Download the agent packages / zip files that correspond to the eG manager host.
- Copy the downloaded packages to the <EG_ MANAGER_ INSTALL_ DIR>\agents\Universal\Latest folder.



Upload eG Agents for Discovery/Monitoring

eG Agents are responsible for continuous monitoring of your applications and infrastructure. You may download these agents at any time from the eG Manager.

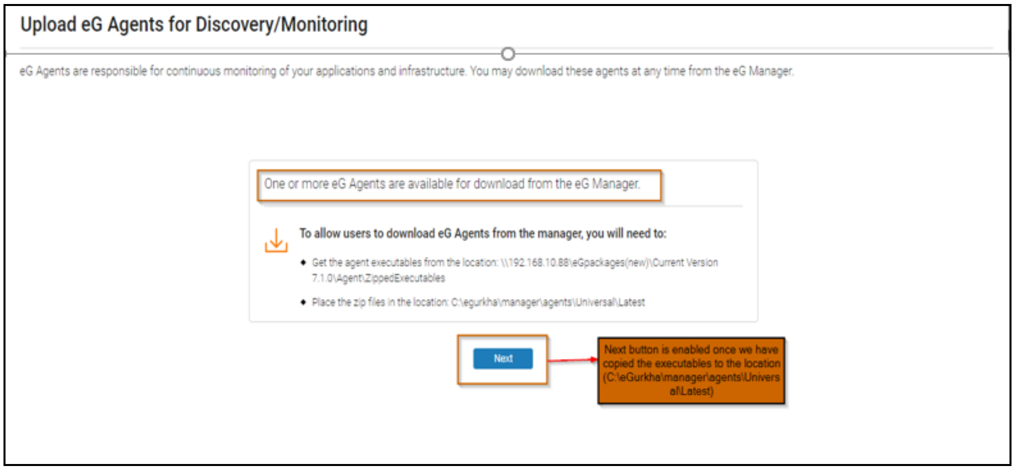
Currently, you have not uploaded any eG Agent to the eG Manager. Please upload Windows 2012 64-bit agent and other agents to the manager.

To allow users to download eG Agents from the manager, you will need to:

- Get the agent executables from the location: \\192.168.10.88\eGpackages(new)\Current Version 7.1.0\Agent\ZippedExecutables
- Place the zip files in the location: C:\egurkha\manager\agents\Universal\Latest

Figure 3.124: A message stating that no agents have been uploaded to the eG manager

3. Once the agents are uploaded to the manager, log back into the eG management console. Figure 3.125 will now appear. Click the **Next** button in Figure 3.125 to proceed.



Upload eG Agents for Discovery/Monitoring

eG Agents are responsible for continuous monitoring of your applications and infrastructure. You may download these agents at any time from the eG Manager.

One or more eG Agents are available for download from the eG Manager.

To allow users to download eG Agents from the manager, you will need to:

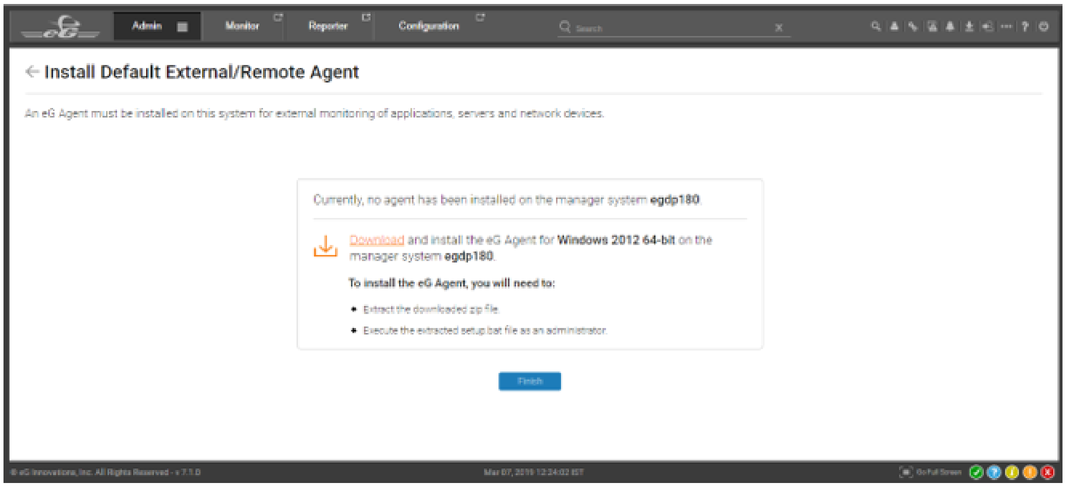
- Get the agent executables from the location: \\192.168.10.88\eGpackages(new)\Current Version 7.1.0\Agent\ZippedExecutables
- Place the zip files in the location: C:\egurkha\manager\agents\Universal\Latest

Next
Next button is enabled once we have copied the executables to the location (C:\eGurkha\manager\agents\Universal\Latest)

Figure 3.125: A message stating that one/more eG agents are available for download from the eG manager

4. Figure 3.126 will then appear. Using Figure 3.126, you can download the eG agent you want installed on the eG manager. This eG agent will automatically operate as an external/remote agent for the target environment. To download the eG agent installable, click the **Download** link

in Figure 3.126.



Install Default External/Remote Agent

An eG Agent must be installed on this system for external monitoring of applications, servers and network devices.

Currently, no agent has been installed on the manager system **egdp180**.

Download and install the eG Agent for **Windows 2012 64-bit** on the manager system **egdp180**.

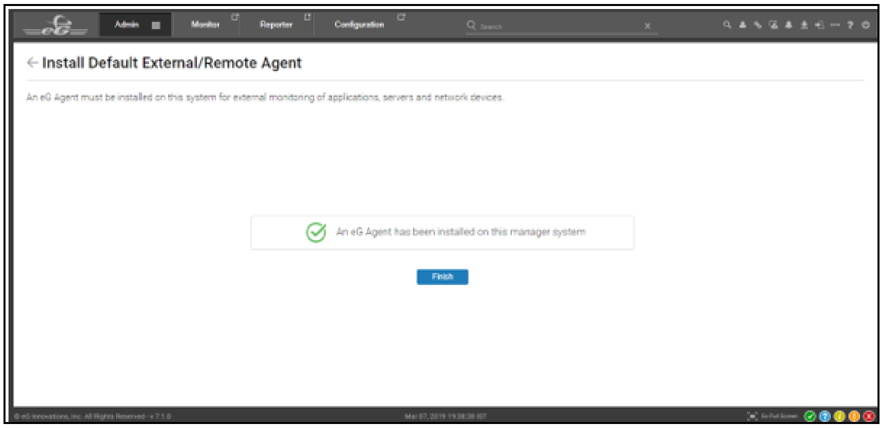
To install the eG Agent, you will need to:

- Extract the downloaded zip file.
- Execute the extracted setup.bat file as an administrator.

Finish
© eG Innovations, Inc. All Rights Reserved - v 7.1.0
Mar 07, 2019 12:24:02 IST
Go Full Screen

Figure 3.126: Downloading the eG agent installable

5. Then, using the downloaded installable, install the eG agent on the manager host. To know how to install an eG agent downloaded from the eG manager console on a Windows / Linux / Solaris / AIX / HP-UX host, follow the procedure discussed in the corresponding topics.
6. After successful installation, reboot the agent host.
7. If you then log back into the eG management console, you will view a message to this effect (see Figure 3.127).


Admin
Monitor
Reporter
Configuration
Search

Install Default External/Remote Agent

An eG Agent must be installed on this system for external monitoring of applications, servers and network devices.

An eG Agent has been installed on this manager system

Finish
© eG Innovations, Inc. All Rights Reserved - v 7.1.0
Mar 07, 2019 19:38:38 IST
Go Full Screen

Figure 3.127: A message confirming the successful installation of an eG agent on the manager host

3.6 eG Agent's JRE Variations

Typically, HotSpot JRE 1.6 and 1.8 are bundled as part of the eG agent installable for Linux (32-bit). 64-bit Linux agents on the other hand are bundled with OpenJRE 12 and HotSpot JRE 1.7. To ensure backward compatibility with older versions of Linux , HotSpot JRE 1.6 is set as the default in 32-bit Linux agents, and HotSpot JRE 1.7 is set as the default in 64-bit Linux agents. Eventually, the eG agent will only use that JRE which is supported by the Linux kernel. For example, if the Linux kernel (32-bit) on which the agent is installed supports HotSpot JRE 1.8, then the agent will use the HotSpot JRE 1.8 that it is bundled with. On the other hand, if the Linux kernel does not support the HotSpot JRE 1.8, then the eG agent uses JRE 1.6 only.

The eG agent for Solaris AMD environments is bundled with HotSpot JRE 1.5 and 1.8 , with JRE 1.5 being the default. The eG agent for Solaris SPARC environments on the other hand is bundled with HotSpot JRE 1.6 and 1.8, which JRE 1.6 being the default.

The eG agent for AIX is bundled with IBM JRE 1.7 and 1.8, with JRE 1.7 being the default.

The eG agent for HP-UX (PA-RISC and Itanium) is bundled with HotSpot JRE 1.7.

While the eG agent for 32-bit Windows systems/servers is bundled with HotSpot JRE 1.8, the eG agent for 64-bit Windows targets is bundled with OpenJRE 12.

The table below discusses this clearly.

Operating System	HotSpot JRE 1.5	HotSpot JRE 1.6	HotSpot JRE 1.7	HotSpot JRE 1.8	IBM JRE1.7	IBM JRE 1.8	OpenJRE 12
Linux (32-bit)		**X (default)**		**X**			
Linux (64-bit)			**X (default)**				**X**
Solaris AMD	**X (default)**			**X**			
Solaris SPARC		**X (default)**		**X**			
AIX					**X (default)**	**X**	
HP-UX			**X**				
Windows (32-bit)				**X**			
Windows (64-bit)							**X**

4.1 Troubleshooting the eG Agent Installation

The following sections highlight the common problems you may encounter when installing, configuring, or starting an eG agent and discuss how to resolve them.

- Section **4.1.1**
- Section **4.1.2**

4.1.1 Installing the eG Agent

The eG agent failed to install properly. What could be wrong?

Please check for the following:

a. Did you accept the license agreement?

b. Do you have the pre-requisites

- An operating system version that eG supports
- The right service pack and option pack (for Windows environments)

4.1.2 Starting the eG Agent

1. **The eG agent was installed successfully, but it does not seem to be reporting any measures. What could be wrong?**

    a. Make sure that the IP address or the hostname of the manager specified during the agent install is correct.

    b. Please check to see if the eGurkhaAgent service (on Windows) or the EgMainAgent process (on Unix) is running. If the agent service/process is not running, the main reason is probably because the Java environment is not set properly.

    c. If the agent is running but is not reporting measures, possible reasons for this are:

    - The manager may not be accessible from the agent. Please check to see if any test from the agent is reporting measures. If no test is reporting measures, it is possible that the agent is not able to communicate with the manager. In this case, check the directory <EG_HOME_DIR>/agent/data. If there are many files in this directory, the main reason for this could be that the manager is either down or is not accessible from the host where the agent is installed.

- Another reason why the agent may not be reporting measures to the manager could be that no applications running on the host where the agent is installed are in the managed list of the eG manager. Please check the agent error log to confirm if this is the case.
- A third reason for the agent/manager communication to fail could be if the manager is configured to authenticate all agents reporting to it, and the agent is communicating via a Network Address Translator or firewall. In this case, the manager will not be able to authenticate the agent. To enable manager/agent communication, turn the authentication option off for manager/agent communication.
- Some antivirus software may stop the eG agent from executing any Visual Basic scripts on Windows. This can cause the agent to stop running. Please check the antivirus software's documentation to determine how it can be configured to allow the Visual Basic scripts in the eG directory to execute.

2. **The eG agent on a server used to work. Suddenly, it has stopped working. What could be wrong?**

   This problem can also occur if you have uninstalled the Java environment that you had specified when installing the eG agent. Even an upgrade of the java environment or changing the java installation directories can cause problems. You will need to edit the <EG_ HOME_ DIR>/bin/start_agent script on Unix to restart the manager. On Windows, reinstall Java in the same location.

3. **Are there log files that I should look at to figure out what problems are happening with my eG installation?**

   Yes, to detect problems with the eG manager, please look at the error_log file in the <EG_ HOME_DIR>/manager/logs directory. Likewise, to detect problems with the eG agent, please look at the **error_log** file in the "<EG_HOME_DIR>//agent/logs directory.

Chapter 5: Manually Installing / Uninstalling the Auto-restart Feature for the eG Agent / Manager

To manually install/uninstall the auto-restart feature for the eG agent / manager, do the following:

1. Move to the **/opt/egurkha/bin** directory and run the command, **auto_restart <argument1> <argument2>**, where **<argument1>** could be either of the following:

   - **install:** Enter **install** if you wish to install the auto-restart feature
   - **uninstall**: Type **uninstall** if you wish to uninstall the auto-restart feature
   - **<argument2>** could hold either of the following values:
   - **manager**: Enter **manager** to ensure that the manager restarts on system reboot
   - **agent**: Enter **agent** if the agent is to be restarted on system reboot

2. If none of the above arguments are provided, or, an incorrect / invalid argument is provided, then the following message will appear:

   ```
   Usage /opt/egurkha/bin/auto_restart [ install | uninstall ] [ manager | agent ]
   ```

   Now, specify the correct argument and proceed with the corresponding process.

3. Only a super user has the permission to execute the **auto_restart** script. Therefore, if the current user is not the super user, then soon after the following message is displayed, the install / uninstall process will be terminated:

   Current user ‘john’ does not have permission to execute this script

   Only super user can execute this script!

4. On the other hand, if the current user is the super user, then the script will begin installing / uninstalling the auto-restart feature. Upon successful installation of the auto-restart feature for an agent, you will see the following message:

   Successfully installed the auto-restart feature for the eG agent!

   Upon successful installation of the auto-restart feature for a manager, you will see the following message:

   Successfully installed the auto-restart feature for the eG manager!

Similarly, upon successfully uninstalling the auto-restart feature for an agent, you will see the following message:

Successfully uninstalled the auto-restart feature for the eG agent!

In the same manner, once the installation of the auto-restart feature for a manager becomes successful, the following message will appear:

Successfully uninstalled the auto-restart feature for the eG manager!

Chapter 6: Configuring eG Enterprise to Work in NATed Environments

It is straightforward to deploy the eG manager and agents for monitoring an Intranet where all the managed systems are in the same IP address range, and there are no firewalls/address translators between the managed devices/servers. In many large environments, there may be multiple demilitarized zones, with firewalls between them. Furthermore, the monitored network can span multiple geographical locations and can be connected via Virtual Private Networks. The devices/servers in each location can be in a different, often private, IP address range. This section covers how the eG manager and agents have to be configured to handle such environments.

There are various scenarios to be considered, depending on whether the manager and agents reside in network address translated environments.

- Section **6.1**
- Section **6.2**
- Section **6.3**
- Section **6.4**

6.1 Manager behind a NAT

Consider the case where the eG manager and agents are in a private Intranet (see Figure 4.1). All the agents can be configured to communicate with the manager using its private IP address. In this case, if external access from the Internet is required for the eG manager, network address translation can be setup, so the eG manager can be accessed using a public IP address from the Internet. In the example in Figure 5.1, the manager is installed on a private address - 10.5.20.12. The agents are installed on private addresses 10.5.20.4, 10.5.20.11, 10.5.20.19. The manager is accessible from the Internet via a public address - 209.15.165.127. In this case, users inside the Intranet (eg., User A) can use the URL http://10.5.20.12 to connect to the manager, while users on the Internet (eg., User B) must use the URL *http://209.15.165.127/* to connect to the manager (see Figure 6.1).

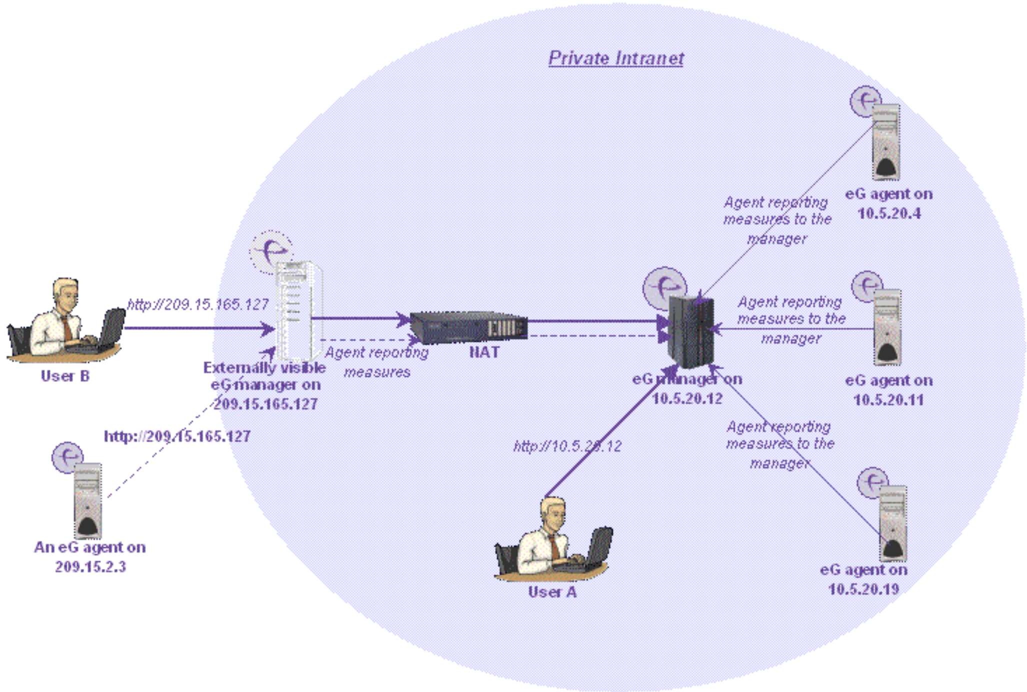


Figure 6.1: Manager behind a NAT

6.2 Agent on a Public IP

Suppose an agent with a public IP address, say 209.15.2.3 (see Figure 6.1), has to communicate with the eG manager. In this case, when installing the agent, the externally visible IP address of the manager (i.e., 209.15.165.127) has to be specified as the manager's IP address (see Figure 6.1). Only then can the agent communicate with the manager. The dashed lines (--) in Figure 6.1 represent the flow of information from the eG agent on 209.15.2.3 to the eG manager on 10.5.20.12. In this case, the server/applications on 209.15.2.3 must be managed via the eG admin interface for the manager to respond to the agent.

6.3 Agent behind a NAT

Yet another scenario involving NATed environments is when the system on which the agent is installed is also behind a network address translator (see Figure 6.2). Suppose that the agent is being installed on a server with a private IP address 192.168.10.7, and that this agent has to be configured to communicate with the manager on 10.5.20.12 (which is accessible over the Internet as 209.15.165.127). Suppose that the private IP 192.168.10.7 is translated into the public IP address 209.15.2.3 via a NAT (see Figure 6.2).

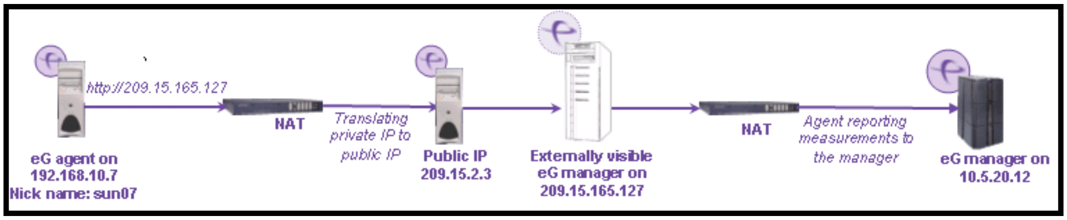

http://209.15.165.127
NAT
Translating private IP to public IP
eG agent on 192.168.10.7 Nick name: sun07
Public IP 209.15.2.3
Externally visible eG manager on 209.15.165.127
NAT
Agent reporting measurements to the manager
eG manager on 10.5.20.12

Figure 6.2: Agent behind a NAT

In this case:

- When installing the agent, the address of the manager to which the agent must communicate has to be specified as its public IP - i.e., 209.15.165.127.
- On the manager side, the “authentication” setting in the Agents->Settings->Communication Menu has to be set to “Off”. This is because the private IP address 192.168.10.7 is not accessible to the eG manager (which is actually running on a different Intranet with IP 10.5.20.12). Hence, the manager cannot check the validity of the agent’s IP address directly.
- When managing the server via the eG admin interface, the server’s IP address must be specified as 192.168.10.7. To see why this is the case, consider how the agent/manager communication works. When the agent connects to the manager, it presents its identity - IP address, nick names, hostname, etc. The manager determines the tests that must be executed by the agent based on its identity and passes this information back to the agent. In this case, the NATed public IP of the agent system (209.15.2.3) is NOT known to the agent (as this is not explicitly configured on the agent system). Hence, servers/applications on the target system must be managed using the private IP address (i.e., 192.168.10.7).

Although the above scenario has been described in the context of a NATed environment, the same steps above apply if the agent is communicating to the manager using a proxy server as well.

6.4 Managing Agents in Multiple Private Networks

In some cases (especially in managed service provider - MSP environments), a single manager may be used to manage multiple private networks. The same private IP address could be used by different servers in the different networks. For example, server Sa in the first network and server Sb in the second network could both have the same private IP address 192.168.10.7. Different applications could be running on these servers. The eG architecture provides an elegant solution to allow these servers to be managed using a single manager. This solution involves configuring the eG manager to identify agents using their nick names and not their IP addresses. The steps in this regard are as follows:

1. First, add both the servers Sa and Sb via the eG admin interface with the same IP address but different nicknames (e.g., Sa and Sb as in Figure 6.3).

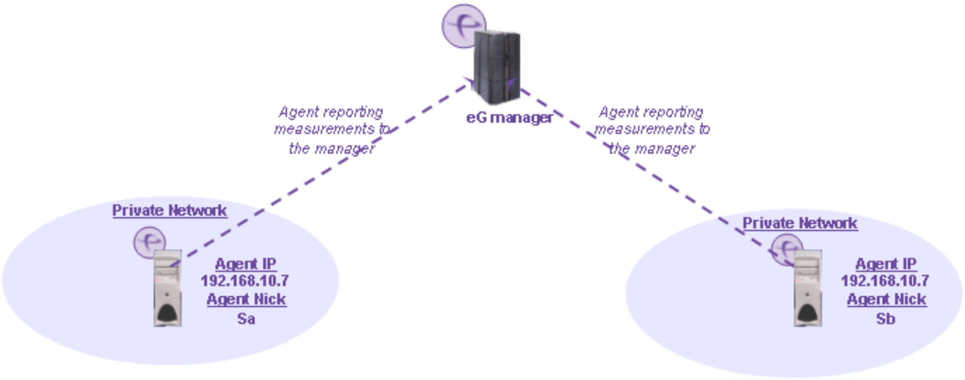


Figure 6.3: Managing agents in multiple private networks

2. Next, understand how the eG manager in your environment is presently determining the identity of the eG agents – using the IP address of the eG agents, or their nick name? For this, check the status of the **Verify if agent is reporting from configured IP** parameter in the **MANAGER SETTINGS** page (Configure -> Settings menu sequence) in the eG administrative interface. If this flag is set to **No**, it indicates that the eG manager is identifying the eG agents using their nick names and not their IP addresses. Since this is the desired setting, following step 1 alone would suffice to ensure that both *Sa* and *Sb* communicate with the eG manager.

   On the other hand, if this flag is set to **Yes** in your eG manager installation, it indicates that your eG manager is currently identifying the eG agents using their IP address only. In such environments typically, many eG agents may not have been configured with nick names at all at the time of installation! In such a situation, if you set this flag to **No**, then agents without nick names will stop working! To avoid this, before proceeding any further, you must make sure that every eG agent installed in your environment is assigned a unique nick name! Since manual nick assignment can be cumbersome, the eG Enterprise system provides the following alternative:

3. Edit the **eg_tests.ini** file in the <EG_INSTALL_DIR>\manager\config directory.
4. Set the **UpdateNicks** parameter in the **[AGENT_SETTINGS]** section of the file to **Yes**.
5. Then, save the file.

   Setting **UpdateNicks** to **Yes** ensures that every eG agent in the environment, which has no nick assigned to it, is automatically assigned the nick name that is specified in the eG admin interface for the application that is managed using that agent's IP address. For instance, if no nick name has been assigned to the eG agent on host 192.168.10.10, and a *Windows server* has been managed on this host with the nick name *win10* using the eG admin interface, then, this nick name will be automatically mapped to the eG agent on the IP address, 192.168.10.10.

Note:

- If you have already assigned nick names to one/more agents in your environment, then setting **UpdateNicks** to **Yes** will not change the original nick assignments of those agents.
- If **UpdateNicks** is set to **Yes**, then, for this setting to take effect, you need to enable auto-upgrade for all eG agents for which nicks are to be automatically assigned.
- By default, it will take **1 day** for the eG manager to update all eG agents with nick names. To override this default setting, do the following:
  - Follow the Agents -> Upgrade -> Enable/Disable menu sequence in the eG admin interface.
  - Select the **Upgrade Settings** option from the **AGENTS – UPGRADE** page that appears next. Alternatively, you can also follow the menu sequence, *Agents -> Upgrade -> Settings*, to access this page.
  - Then, from the **How often agents should check for Auto Upgrade package** list box, select the time interval at which you want the eG agents to be updated with nicks.
  - If you want the updates to occur within the next 15 minutes, then, select the **Upgrade now** option from the **AGENTS – UPGRADE** page, pick the agents for which nicks are to be auto-assigned from the **AUTO UPGRADEABLE AGENTS** list, and click the **Enable** button therein.

6. Once this is done, set the **Verify if agent is reporting from configured IP** parameter in the **MANAGER SETTINGS** page (Configure -> Settings menu sequence) in the eG administrative interface to **No**.

Since the eG manager and agents have now been configured to use the nick name as the key to identify an agent/server, servers with the same IP address can be easily distinguished and managed by an eG manager.

Chapter 7: Backing up and Restoring eG Enterprise

The procedure involved in backing up and restoring eG Enterprise on Windows and Unix environments is detailed in the following topics.

- Section **7.1**
- Section **7.2**
- Section **7.3**
- Section **7.4**

7.1 Backing up and Restoring the eG Manager on Unix Environments (Linux and Solaris)

To backup and restore the eG manager on Unix environments, do the following:

1. Tar the **/opt/eGurkha** directory and save it in a convenient location.
2. To restore the eG manager to the same host from which the backup was taken, untar the **eGurkha** directory to the **/opt** directory.
3. If you restore the eG manager to a different host, first, untar the **eGurkha** directory to the **/opt** directory, and then, check whether the IP/host name of the new host is different from the old manager host. If so, run the **reset_ manager** and **reset_ agent** scripts from the **/opt/egurkha/bin** directory, and change the IP/host name of the eG manager to that of the new host. Also, replace the old eG manager license with a new license generated for the new IP address/hostname.
4. After restoring, check whether the **/opt/egurkha/manager/tomcat/webapps/final/WEB-INF/lib** is a soft link to **/opt/egurkha/lib**. To perform this check, execute the following command from the command prompt:

   ls -alt /opt/egurkha/manager/tomcat/webapps/final/WEB-INF/

5. If the result of this command includes the following statement, then it indicates that the soft link exists.

   lib -> /opt/egurkha/lib

6. If not, first, remove the directory **/opt/egurkha/manager/tomcat/webapps/final/WEB-INF/lib**.

7. Next, create a soft link using the following command:

   ```
   ln -s /opt/egurkha/manager/tomcat/webapps/final/WEB-INF/lib /opt/egurkha/lib
   ```

8. Finally, restart the eG manager.

7.2 Backing up and Restoring the eG Manager on Windows Environments

To back up and restore the eG manager on Windows, do the following:

1. Login to the eG manager host.
2. Copy the **eGurkha** directory to a convenient location.
3. If you want to restore the eG mananger to the same host from which its backup was taken, follow the steps below:

   a. If you already have a fully operational manager on the target host and you simply want to revert to the backed up version of the eG manager, then, simply replace the **eGurkha** directory on the target host with the backed up **eGurkha** directory, and then restart the eG manager.

   b. On the other hand, if you want to completely scrap the existing manager installation and replace it with the backed up version, then, follow the steps below:

   - Uninstall the existing eG manager.
   - Next, install the eG manager with the same specifications as the old manager; for instance, if the old manager was installed using Tomcat and not IIS, make sure the new manager also uses Tomcat. Similarly, install the new manager in the same directory as the old manager. **However, during installation, make sure that you do not provide the name of the database used by the old manager. Instead, provide the name of a new ‘dummy’ database for use as the eG backend.**
   - Replace the **eGurkha** directory of the new manager with the old eG manager.
   - Finally, start the eG manager.

4. If you want to restore the eG manager to a different host (i.e., a host with a different IP address/hostname from that of the backed up manager), then, do the following:

   a. If you have a fully operational manager on the target host and you simply want to revert to the backed up version of the eG manager, then, to restore the backed up version, simply replace the **eGurkha** directory on the target host with the backed up **eGurkha** directory, and then restart the eG manager.

b. On the other hand, if you want to completely scrap the existing manager installation and replace it with the backed up version, then, follow the steps below:

- Uninstall the existing eG manager.
- Next, install the eG manager with the same specifications as the backed up manager; for instance, if the backed up manager was installed using Tomcat and not IIS, make sure the new manager also uses Tomcat. Similarly, install the new manager in the same directory as that of the backed up manager. **However, during installation, make sure that you do not provide the name of the database used by the backed up manager. Instead, provide the name of a new 'dummy' database for use as the eG backend.**
- Replace the **eGurkha** directory of the new manager with that of the manager in backup.
- Next, run the **changeManagerSettings.bat** and **changeAgentSettings.bat** files from the <EG_INSTALL_DIR>\lib directory to change the IP address/host name of the eG manager and agent.
- Replace the old eG manager license with a new license generated for the new IP address/hostname.
- Finally, start the eG manager.

7.3 Backing up and Restoring the eG Database

eG uses MS SQL and Oracle databases to store its persistent data. The best practices for backing up and restoring the eG database are the ones recommended by the database vendor themselves. These documents can be downloaded from *http://www.microsoft.com/* or *http://www.oracle.com/*. The exact URLs will vary depending upon the type and version being used, and can be easily found using the **Search** options given in the sites.

7.4 Mandatory steps

- If the database is in a different box, and only the manager setup is to be restored to the same box from which it was backed up, then follow steps detailed in Section **7.1** topic and Section **7.2** topic, depending upon the operating system of the eG manager.
- If the database alone is to be restored, then follow procedure explained in Section **7.3** topic only
- If both have to be restored, then follow the steps provided in the Section **7.1** topic through Section

7.3 topic.

- Restart the system after this process before attempting to start the manager and/or the agent

Chapter 8: Conclusions

eG Enterprise has been specially designed keeping in mind the unique requirements of IT infrastructures. For more information on the eG family of products, please visit our web site at www.eginnovations.com.

This document has described the installation and configuration, of eG Enterprise. For more details regarding the eG architecture, how to use eG Enterprise, and details of the metrics collected by the eG agents, please refer to the following documents:

- A Virtual, Private Monitoring Solution for Multi-Domain IT Infrastructures
- The eG User Manual
- The eG Measurements Manual
- The eG Quick Reference Guide

We recognize that the success of any product depends on its ability to address real customer needs, and are eager to hear from you regarding requests for enhancements to the products, suggestions for modifications to the product, and feedback regarding what works and what does not. Please provide all your inputs as well as any bug reports via email to mailto:support@eginnovations.com.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.